Band 17 / 2016

Networked Insecurity – Hybrid Threats in the 21st Century

Anton Dengg and Michael Schurian (Eds.)

Schriftenreihe der
Landesverteidigungsakademie

www.bundesheer.at

SCHUTZ und HILFE

Schriftenreihe der Landesverteidigungsakademie

Anton Dengg, Michael Schurian (Eds.)

Networked Insecurity – Hybrid Threats in the 21st Century

17/2016
Vienna, June 2016

Imprint:

Copyright, Production, Publisher:
Republic of Austria / Federal Ministry of Defence and Sports
Rossauer Lände 1
1090 Vienna, Austria

Edited by:
National Defence Academy
Institute for Peace Support and Conflict Management
Stiftgasse 2a
1070 Vienna, Austria

Schriftenreihe der Landesverteidigungsakademie

June 2016
ISBN 978-3-903121-01-0

Printing:
HDruckZ-ASt Stift 16-xxxx
Stiftgasse 2a
1070 Wien

Translation by Georgette Hauzenberger and Peter Cox, for the
Austrian Armed Forces Language Institute

Special thanks are due to all those who contributed to the creation of this publication.

“To fight and conquer in all our battles is not supreme excellence;

rather, supreme excellence consists in breaking the enemy's resistance without fighting.”

Sun Tsu

Table of Contents

Foreword

The military, but ultimately non-violent taking of the Crimean peninsula by Russian special forces has demonstrated a novel threat phenomenon that was indeed theoretically conceivable in this form and yet seemed unrealisable politically. Here it is less about the individual components of “Operation Crimea” and more about their specific composition in defiance of the stipulations of international law and particular reliance on both old and new mass media. The resulting propaganda war, which continues to this day, makes it difficult for those involved and for observers to form a clear overview of what is actually going on or indeed of the causes and effects of events.

Many experts see Russia’s behaviour towards the Ukraine as confirming the hypothesis of hybrid warfare, which extends beyond direct and indirect military action also to include many other measures (including CyberWar), with a view to having an effect on the opponent and forcing his hand. Nor does this seem to be a new idea, given that the Chinese military theoretician Sun Tsu rated “victory without fighting” as the best strategy. Yet all of this falls short of covering the full bandwidth of risks, dangers and threats completely in today’s world with the means and possibilities available. To a certain extent, the associated profiles now manifesting themselves amount to a new form of “enclosure” of war, because both the aggressor and his target, as well as the actual objectives, can remain in the dark. Humanitarian international law and other international regulations may have no influence or be ignored, whilst the true extent of an “attack with modern means” on a state and its ability to function may only become recognisable at a very late stage and abruptly. Anton Dengg and the co-authors of this volume have dealt intensively with the topic of hybrid power projection in the context of a project. In this they progress beyond the narrow and indeed militarily dominated model of hybrid warfare to lay out a concept that endeavours to cover the full spectrum of threats. In doing this, they also accomplish pioneering work in the area of terminology, in that they define significant, relevant phenomena and point out that not every hacker attack constitutes a threat to a state, but rather that a strategic threshold, which must be defined by every state, has to be exceeded.

It is evident from the contributions and country studies that a certain awareness of the problems arising from hybrid threats does indeed exist, and yet that perceptions and methods of resolution at a national level apparently tend to be diffuse or one-dimensional. The intention of the work presented here is therefore to make a contribution towards creating awareness, defining the problem and anticipating potential protective and countermeasures at a strategic level. Potentially particularly helpful in this regard is the graphic developed by Anton Dengg and Michael Schurian, which illustrates the spectra of threat potential. It should indeed also be seen as a prompt for forward-looking reflection.

Walter Feichtinger

Director, IFK

Abstract

Societies grow ever more connected in practically all spheres of life; not least due to the technological achievements. Alongside positive effects, negative ones also appear – systems become more prone to failure. Thus the image of threats also changes and is influenced by a growing number of factors.

In international publications[1] different governmental options of choice in contemporary combat operations are dealt with. The notion of Hybrid Warfare has been coined.

This book takes a much broader approach and describes potentially applicable possibilities of a state to exert power beyond mere combat operations. As an example, the current Ukraine conflict is appropriate because it is not fought with conventional – military – means, but rather with a variety of different instruments of power projection. From this variety of options to exert influence over another state's capability to take decisions arise specific images of threats. Technological achievements and their offensive possibilities amplify the options of states to apply hybrid methods. The "worst case scenario" for the target state is a hostile advancement on different levels.

How, when and by whom either soft or hard power is projected in the present or the future lies at the core of this publication. The security policies of two reference states are examined with regard to their preparedness for hybrid threats.

An integral part of this book is the highlighting of options for action to deal with hybrid threats.

Examples taken from current tension- and conflict regions ultimately underpin the theoretical remarks on "hybrid threats". The illustrations serve to visualise complex interdependencies.

[1] See, e.g. Frank G. Hoffman: Hybrid Warfare and Challenges. In: JFQ, issue 52, 1st quarter 2009. <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-52.pdf>, accessed on 25/10/2015.

1. Introduction and Theory

Conflict scenarios are subject to continuous change. Technological achievements make a substantial contribution to this change. The characteristics of power change with the advent of new technologies and their applications. Actors can use these to bring power and force to bear by means of a variety of methods. These can be expected to include "resource-conserving" approaches, ahead of military options. Priority is given to a change in the balance of power achieved with no resistance if possible – victory without battle. The consequence is modified threat situations. Yet perceptions of threat depend on subjective, selective criteria and are interpreted in a variety of ways. The challenge for a target state lies in recognising such an unconventional "attack" and implementing appropriate countermeasures.

1.1 Reflections on the Term “Strategic Threat”

Thomas Pankratz

The term “strategic threat” is, without doubt, one of the core terms in discussions of strategy and security policy. It is therefore all the more remarkable that, in contrast to “threat”, no summaries of this term are to be found in the relevant lexica or handbooks. A number of thoughts are assembled below with a view to defining this term. The starting point is the phenomenon threat, with the subsequent argumentation guided by the central elements of strategy, in particular the strategic objectives of the state. Implicit in this approach is that the argumentation is not founded on the threats themselves but rather from the perspective of the actor under threat. These considerations should not be seen as conclusive but rather, indeed primarily, as prompts for further thought and reflection about a frequently used and yet scarcely more closely questioned term.

A central element of strategic thinking[2] is, alongside the formulation of objectives and the means[i3] by which these objectives should be achieved, the analysis of the so-called strategically relevant environment.[4] Within this are located not only the objectives but also possible resources and methods, as well as other actors and their objectives and means. Thus the strategically relevant environment includes not only challenges but also potential threats. Ultimately as a consequence, strategic thinking is about positioning oneself in this strategically relevant environment and influencing it.

Threats can be presented in two fundamental ways. In one case, specific phenomena are named as threats, as in the European Security Strategy of 2003 or in the Austrian Security Strategy of 2013 for example.

[2] Strategic thinking can be understood as goal- and success-oriented calculation aimed at weighing up objectives, means and environment as elements.

[3] In this approach, means include both methods and resources (instruments).

[4] Strategically relevant environment indicates here that subset of the entire environment arising from concentration on the basis of relevance apparent to the actor involved.

In this approach, in most cases there is no explicit explanation of why these phenomena constitute a threat. The explanation is treated as known and follows by implication. In the other case there is active questioning of how and by what means something manifests itself as a threat. This point is treated in greater detail below.

Fundamentally a threat can be understood as the endangerment of the security[5] of an actor[ii][6] by another actor[7]. Applying finer differentiation in an ideal-typical manner, several dimensions are plausible:

- Perception of a threat at the same time as an actual threat is present;
- Perception of a threat at the same time as an actual threat is present;
- Perception of a threat in the absence of an actual threat;
- No perception of a threat when a threat is present.

The extent to which other actors[8] now actually do constitute a threat for another actor depends on a variety of factors, which are reflected in three dimensions. One dimension is the capability and potential (multiple potentials) of one actor actually to endanger another. The second dimension is the intention to do so too. From this it can be inferred that, if one of these dimensions is zero, the first actor does not, indeed cannot[9], present any objective threat to the other[10].

[5] Here security is taken to include all societal and political aspects.

[6] Individual, group, community, state, community of states.

[7] This endangerment can arise from another actor or a phenomenon such as the environment for example. The threats discussed here are those originating from actors.

[8] This can be one or many actors. To some extent these can be named, i.e. there is knowledge of who is involved; yet to some extent they cannot definitely be named.

[9] This relates only to this interaction. In contrast, there may well be endangerment for other actors.

[10] Thus, for example, if state A threatens state B with “nuclear annihilation”, i.e. it has the intent to do this or asserts this intent, even though it lacks the capability, no end-

One can identify a third dimension of endangerment of one actor by another in the event that the latter possesses particular potential to endanger the former, albeit not through corresponding, conscious intent, yet nevertheless through some behaviour that has the unintended effect of endangering the former actor.[11]

Similar considerations apply to the potential of threatened actors. For the latter it is not solely the potentials or intents of other actors that are important here, but rather primarily the capability to recognise them and indicate them too in an appropriate manner. In this interpretation, a whole set of partly conscious and partly unconscious factors[12] play a role, which can be collected together under the term "strategic culture". This means that the perception, i.e. the analysis of the strategically relevant environment, should be seen as a subjectively constructivist act. This implies that the interpretation of the environment is not to be seen as a static moment but rather as something that can and will change for the relevant actor, subject to internal and external influences, with the result that threats will be interpreted differently at different points in time. Furthermore, these differences in interpretation lead to different actors interpreting this environment differently and, as a consequence, interpreting the behaviour of other actors variously as threatening. However, the strategic culture sets not only the interpretation of the environment but also whether, how and to what extent the actor is able and wishes to react to it. Yet this is not solely a question of the means or ability and will to muster that reaction but also a question of the formulation of objectives.

angerment of state B actually applies in the given situation. In a reversal of this for example, a state allied to other states may have the potential to attack each of those states but, as a consequence of the alliance, there is no intent, so no endangerment arises for the allied states.

[11] Thus, for example, through behaviour with respect to third parties as a result of an accident or the like.

[12] E.g. experience of history, geo(political) factors, attitudes and stances of the political elite and population, characteristics of the political system.

Thus, by way of an intermediate result, it is possible to state that at least two actors are required for a threat situation, whereby at least one of them feels or is indeed actually threatened in terms of their security as a result of the intentions and potential of another actor.

The perceived threat can, but does not have to correspond with reality. The reverse is also true. A present threat can, but does not have to be perceived or recognised as such by an actor.

From these considerations one can progress to what can be understood to constitute a "strategic threat". This has to be seen in close relation to the strategic objectives of an actor, in our case the state.

It is fundamentally possible to filter out two dimensions of a state's strategic objectives, which can be subdivided into objectives of power and design. They are closely aligned, albeit power objectives take chronological priority ahead of design objectives. Power objectives relate to one's own position in the system environment, i.e. in particular, one's position relative to other actors alongside one's capabilities and capacity to pursue one's own interests in relation to others. Design objectives are ideas as to how and in what manner the environment can and should be structured to one's own advantage. Thus the interests and values of the corresponding actor are also implicated. If one now transposes these considerations onto the state, it is possible to deduce the following:

The fundamental pre-requisite for positioning with respect to other actors is the secure existence of the state. Thus the top strategic power objective is to be seen as the continuation of the state (its secure existence), where "state" is interpreted here primarily according to principles of international law as an entity composed of the three elements: state population, state territory and state government.

To be seen in close association with this is the protection of sovereignty with respect both to the exterior and interior, thus requiring this to be subsumed under the dimension of design goals. This sovereignty can be seen as executive authority and prerogative of interpretation over the arrangement of the domestic sociopolitical system and of the values lying behind it. Whilst the former dimension is to be seen as independent of the sociopolitical system of the state, the second dimension is indeed dependent on this first dimension and yet variable. This can mean for example that, for western-oriented states, the democratically constituted, liberal pluralistic rule of law, which is oriented towards the fundamental needs and rights of the individual, lies at the focus of those political values deserving protection[13] whilst in contrast, for dictatorially aligned systems, it is the maintenance of absolute power by the political elite and/or unconditional implementation of their own ideology.

Following on from the discussion of the term 'threat', it can now be stated that strategic threats are those threats that either threaten the secure existence of the state system and/or stand in opposition to supreme authority over the arrangement of the sociopolitical system.

These arguments might appear clear at first sight. But applying somewhat finer differentiation to these arguments yields several points worthy of discussion. Thus it can be argued, for example, that possible threats, which are directed towards the three central elements of the state, are to be understood as fundamentally strategic threats. However, it is also possible to argue that a specific scale of threat must be presented to one or all elements in order to endanger the secure existence of the state as such; i.e. only once a specific threshold were exceeded would one speak of a strategic threat. Yet it seems to be difficult to nominate this scale either qualitatively or quantitatively.[14] Ultimately it is up to political leaders to assess and indeed rate this scale. Decisive in this process will not only be the capability of the elite to assess and rate but also their readiness, i.e. their will to do this.

[13] Regarding Austria's sociopolitical objectives, see for example Federal Chancellery of Austria: Austrian security strategy. Security in a new decade – Shaping security. Vienna 2013, p. 9. <www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf>, accessed on 26/10/2015.

[14] Excluding for example the case where a state is occupied by another actor, the population as a whole is threatened by unconventional systems or the government is terminated.

A similar argument applies to the second dimension, that of prerogative of interpretation and sovereignty. Here again all threats arranged in opposition to the actor's own values, interests and ultimate objectives could be seen as strategic threats. But it is also possible to argue as above that a specific threshold level of threat must exist for it to be termed a strategic threat.

An essential point here is that it is first of all necessary appropriately to formulate these values and objectives and also to nominate them as "high priority state objectives". Here again it is up to the political decision-makers to evaluate and assess this. A decisive aspect that contrasts with dictatorially aligned systems is that, in western systems, responsibility for this evaluation and assessment will be shared by at least a majority of those with political responsibility (and thus also the opposition) and, in particular, the people.[15]

It is possible to state in summary that not every potential threat constitutes a strategic threat in itself and that there is no "typical" strategic threat. However, it is possible generally to conclude that "strategic threats" can be seen as those endangering the secure existence of the state. Given that this strategic objective of the state can be essentially defined, the threat to it is more self-evident, immediate and also comprehensible. Nevertheless there is room for interpretation which also applies to threats that endanger the sociopolitical objectives derived from values and interests, and can therefore be described as strategic threats. But in this dimension it seems that the room for interpretation is greater, given that values and interests and thus threats to them are more indirect.

Ultimately the political elite carries responsibility, namely (the responsibility) for formulating the strategic objectives of the state. In democratically oriented systems, this should and must take place to the benefit of the population; also so that these objectives, along with the values on which they are based, are communicated appropriately to the population. Fur-

[15] But this also means that the population must not only know but also be conscious of the values and interests, and therefore also the strategic objectives, of the state.

thermore responsibility should be taken for evaluating and assessing the strategically relevant environment appropriately and in an open manner. Furthermore, responsibility must also be adopted for taking action to enable defence against possible threats, particularly those directed against the strategic objectives of the state. The formulation of strategic objectives without providing appropriate means cannot be described either as success-oriented or enduring.

In democratically oriented states it is therefore common, not only from an academical standpoint but also particularly from citizens' point of view, to demand of those with political responsibility the capability, the will and indeed the courage to think and consequently act strategically. This is politicians' primal task.

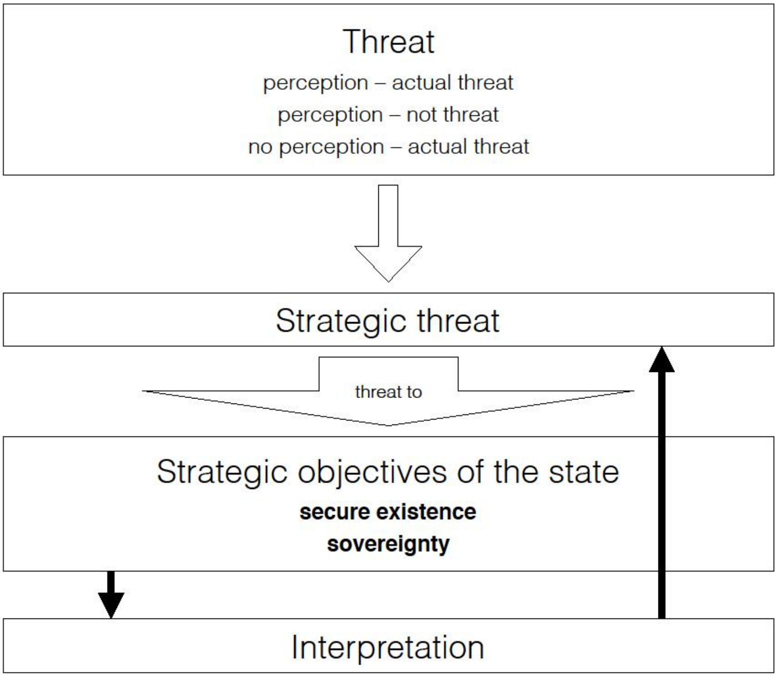


Figure 1: Strategic threat
Thomas Pankratz

1.2 On the Concept of Hybrid Threats

Anton Dengg
Michael N. Schurian

1.2.1 Introduction

Up until the end of the 20th century, conflicts could be described relatively simply: a state or alliance of states applied its instruments of power (largely military) against another state. Aggression was directed towards a clearly identified enemy. In the Cold War, two ideologically opposed power blocs confronted one another, each attempting to dominate the other in a military arms race. As a result of new weapons systems (e.g. intercontinental missiles and long-range bombers), strategic considerations and military orientations changed. Through so-called proxy wars, attempts were made to gain and extend political influence. A variety of means and methods were applied to this end. Regional actors were supported in their conflicts with a variety of instruments by "pact representatives". Propaganda activities were a significant factor in the staging of "good versus evil" in the media. Here, conflicts were largely symmetric (state against state, armament against armament). With the disintegration of the Warsaw Pact countries, the bipolar world order was dissolved and, along with it, a clear and relatively predictable theatre of conflict.

The subsequent development of new technologies, particularly information and communication technologies along with social networks, provided states with more space in which to act in order to achieve power projection against other states in many forms and ways. Playing a particular role here is not only the factor of time but rather and primarily, as evident in examples of cyber attacks, the concealed use of state power projection. The primary objective is not to allow oneself to be recognised as an aggressor but rather to achieve the objective of influencing the other state in one's own interest. This can leave a positive international image unblemished, and/or one opens up the possibility of shifting blame for an aggressive act onto another state. Such activities can be observed particularly in the cyber area. "[The quick and unpredictable nature of these attacks makes it almost impossible to consider the origin of adversaries and their motives in our own preparatory action.]"[16], confirm German security experts. The experts continue: "[The possibility of denying cyber attacks after the fact has already become a strategic element in a new type of computer-based conflict even between states.]"[17]. The armed conflict between Georgia and Russia prevailing since 2008 shows evidence of similar hybrid power projection whilst also making use of cyberspace.

Events taking place in the current Ukraine conflict expose an additional application of hybrid methods by an armed group with no identifiable state allegiance. This form of power projection in particular can be expected to attract an increasing number of imitators in future. The Ukraine conflict makes it clear that the capability and intent for power projection by hybrid means could well emerge as a trend.

Hybrid methods can be localised not only in the case of power projection by states but also terrorist organisations. With its innovative tactics and methods, the kind of terrorism prevailing over the last decade, which is not dependent on state support[18], defies even great powers. Western allies do indeed strive to find concepts for solutions, yet effective counter-strategies for containing global terrorism have not yet been developed. With their ghastly acts broadcast via the Internet, religious fanatics continue to define the image of the war. The many years of international intervention in crises, as for example in Afghanistan and Iraq, demonstrate future challenges in the development of usable, long-term solutions against hybrid means and methods.

[16] Federal Ministry of Defence – The Federal Minister: Defence Policy Guidelines. (27/05/2011). <http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY3NmY2ODMyNmU2YjM0N2EyMDIwMjAyMDIw/Defence%20Policy%20Guidelines%20(27.05.11).pdf>, accessed on 28/10/2015, p. 2; Translation from the German original quotation.

[17] Ibid, p. 2.; Translation from the German original quotation.

[18] Cf. Bauer, Alain: Hybridization of Conflicts. In: PRISM 4, 4/2014. <http://cco.dodlive.mil/files/2014/04/Hybridization_of_Conflicts.pdf>, accessed on 08/12/2015, p. 57.

To date, security policy expertise tended to be directed towards conventional warfare and corresponding counter-strategies. The examples presented make the multi-layered nature of power projection possibilities readily apparent, leading to discussions among experts about hybrid threats. Against a background of worldwide networking and cross-border effectiveness of both ecological and economic risks, many states find themselves exposed to a novel form of threat. Defence against the latter can no longer be achieved solely by means of conventional military force. It is precisely in this context that the project of "The Institute for Peace Support and Conflict Management" of the National Defence Academy (IFK/LVAk) is brought to bear, seeking to encourage awareness of this topic.

1.2.2 Methodology

The basis for this work was the [Strategies of hybrid power projection exemplified by the USA, Russia, China and India][19] project carried out from 2011-2012 at the IFK. This gave rise to the follow-on project [Hybrid potential threats and resultant security policy deductions for small states][20].

To define the concept of "small state", use was made of the distinguishing characteristics employed by Jeanne A.K. Hey, who differentiates between three categories of small state:

a) ["micro-states with fewer than a million inhabitants (e.g. in the Caribbean and Indian Ocean),
b) industrialised European small states (e.g. Belgium, The Netherlands, Switzerland and Austria), [...], along with
c) under-developed small states in the Third World (e.g. in Africa, Asia and Latin America) [...]"[21].

[19] Translation of the original German title.

[20] Translation of the original German title.

[21] Hey, Jeanne A.K.: Refining Our Understanding of Small State Foreign Policy. In: Hey, Jeanne A.K. (Ed.): Small States in World Politics. Explaining Foreign Policy Behavior. Boulder, Colorado 2003, p. 185195. Translation from the German original quotation.

For further treatment within the project, the category "industrialised European small states" was selected. In a subsequent stage of work, the states of Slovakia and Sweden were filtered out. On the one hand, the reason for this selection was that these states were similar to Austria in terms of structure, size of armed forces and engagement in international affairs, thus being suitable for quantitative comparison. On the other hand, they are distinct in being members of various alliances (UNO, NATO, etc.), which explains potentially differing national approaches to defence against hybrid threats. The deductions drawn serve as a contribution to constructive security policy discussions.

Serving as the theoretical basis for the project is Joseph Nye's soft and hard power model. According to Nye, a state "can compel others to advance its interests in three main ways: through coercion, payment, or attraction".[22] In the project, using an empirical/analytical approach, the security strategies of Slovakia and Sweden were investigated with regard to actual references to "hybrid threats".

In order to gain an overview of the topic, the project management relied on Internet research, discussions with experts and workshops. A variety of security policy strategies and studies were analysed with regard to the concept of "hybrid threats". Initial results showed multiple references to "hybrid warfare" but that scarcely any findings on hybrid threats existed. Principally in focus were theoretical considerations as well as potential constellations of actors and their means and methods, so that, in the event that hybridity was not addressed as a topic, indirect reference could be made to the presence of hybrid threats.

Initial analyses of areas of crisis and conflict, as well as various scenarios relevant to security, showed that the concept of "hybrid warfare" is insufficiently inclusive. After all, a change in a state's political direction is not necessarily conditional on warfare – the sensitive destabilisation of the economy or society is sufficient.

[22] Nye, Joseph S. Jr.: Putin's Rules of Attraction (12/12/2014). <http://www.project-syndicate.org/commentary/putin-soft-power-declining-by-joseph-s--nye-2014-12>, accessed on 06/11/2015. Translation from the German original quotation.

This can take place without any apparent use of military force. For example, highly complex computer viruses, requiring a great deal of effort to produce, have been deployed in order to influence the activities of states, as proven by the *Stuxnet* computer virus. The deliberate influencing of state interests by non-military means demonstrates not only this new variant of power projection but also certain states' intention to deploy such forms of projection. The importance of state cyber-power has been illustrated by Edward Snowden's revelations regarding National Security Agency (NSA) surveillance practices. Snowden was also aware that "[... he had increased the power of the state through his work...]"[23], concluded Laura Poitras, U.S. journalist and film-maker.

Worthy of note as a further example of indirect, non-military intervention are the measures of support in the form of military training activities provided by British elite forces[24] to rebels in Syria. "[Already more than 300 rebels in Iraq have completed training at a camp on the Syrian border. This training is led by ex-members of the SAS (Special Air Service), a special forces division of the British army]"[25], according to a report in "Spiegel Online" in 2012. Through such actions, states/governments influence not only events in conflict areas. They also exert an influence on the actions of the affected states. All of the activities described in the examples are therefore to be rated as being part of exercising hybrid power.

In the course of various discussions with experts and workshops, the need for a definition of "hybrid threat" became evident. To this end, the IFK developed a working definition, which was discussed with experts from a variety of interdisciplinary areas in a workshop.

[23] Seibel, Alexandra: Die ganze Existenz aufs Spiel setzen [Betting your entire existence]. Interview with U.S. journalist and film-maker Laura Poitras who, together with Glenn Grenwald, reporter at the Guardian, met Edward Snowden in Hong Kong in June 2013. In: Kurier, 29/12/2014, p. 21. Translation from the German original quotation.

[24] Salloum, Raniah: Britische Elite-Kämpfer bilden Rebellen aus [British elite soldiers train rebels]. In: Spiegel Online, 23/07/2012. <http://www.spiegel.de/politik/ausland/syriens-rebellen-werden-angeblich-im-ausland-trainiert-a-845923-druck.html>, accessed on 07/11/2015.

[25] Ibid; Translation from the German original quotation.

Ultimately a smaller group of experts finalised the working definition stated in the chapter 'The Concept of "Hybrid Threat"' (chapter 1.2.5).

In order to reduce the complexity of "hybrid threats", various illustrations and overviews were prepared, with the aim of clarifying both the concept of hybrid threats and any potential interdependencies. There is a further attempt at complexity reduction developed in the form of the tabulated depiction[26] of "offensive" actors and their offensive means on the one hand and corresponding "defensive" actors with the necessary defensive means on the other.

Ultimately, individual experts analysed security policy strategies and reports for the presence of hybrid threats and for content judged to correspond with them, according to prescribed criteria. Finally, examples of cases of hybrid power projection that had already taken place at a variety of levels made up the concluding part of the project, with a view to illustrating the theoretical approach.

1.2.3 Objective of the Project

Going into depth on the topic of "hybrid threats" makes clear its scarce appearance in research into security policy. Consequently the IFK set itself the goal of investigating the "hybrid threat" phenomenon, examining it on a scientific basis and ultimately moving to the aspect of public awareness. Decisive here is not merely the knowledge of such threats but particularly knowing the necessary counter-strategies. The objective targeted by the project was to analyse the security policy concepts of selected small states with regard to their assessment of prevailing threats and develop deductions as a consequence. At the focus of the project, amongst other aspects, was the question as to the extent to which potential hybrid threats at the whole-of-nation level are registered in the reference states (Slovakia and Sweden). Furthermore, international security organisations like the North Atlantic Treaty Organization (NATO)

[26] Developed by Bachora/Dengg/Schurian; see Figure 3.

for example, were analysed in order to determine what strategies and concepts they have available to counter hybrid threats.

Finally there was concentrated attention on the question of perceived interdependencies between participation in international crisis and conflict management (ICCM) and the associated risks of hybrid threats for the sending state. Here the focus was on the question as to the national consequences in the context of whole-of-nation security provision.

Ultimately the findings and conclusions, particularly those relating to perceived threats and possible protection and defence measures, yielded inferences for small states. The resulting experience and *lessons learned* should serve as references to inform Austrian security policy. This aligns with the partial strategy of the Austrian Ministry of National Defence and Sport issued in 2014, which states that, in future, "[conflicts in the European region will increasingly be conducted using hybrid methods]"[27].

1.2.4 General Observations on Perceived Threats

The thought that actors in conflict, whether state or non-state, would employ every possible means and method to achieve their objectives is certainly not new. Clausewitz had already determined that every era must deal with its own concept of war.[28] The waging of war as a cultural phenomenon always reflects civilisation and is tied into the state of technology of the corresponding era and society. To this day, nothing appears to have changed.

What are new, with regard to present day threats, are the changed circumstances in which states and their armed forces find themselves at the beginning of the 21st century: globalisation and internationalisation

[27] BMLVS: Partial strategy defence policy, p. 5. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf>, accessed on 08/12/2015 Translation from the German original quotation.

[28] Clausewitz, Carl von: Vom Kriege [On War]. Eighth book, third chapter. B. Reclam 1994 (1832), p. 312.

challenge territorially defined concepts such as sovereignty and national defence.

A global population explosion, accompanied by an equally exponential escalation in requirements to be satisfied and resources to be consumed, is forcing economies into competition over ever scarcer raw materials, amplified by the technology revolution. Information, opinions and capital circulate worldwide with practically no delay. Networked global media and the possibility of permanent communication by means of ICT technology (therefore also the potential to influence, whether deliberately or inadvertently), enable international comparison of differing living environments and standards of living, thus also differing "forms of freedom", which each respective society offers to, or withholds from its population. The result of this comparison, alongside other causes and motivations, is the drive for migration flows, particularly to Europe.

Societies, markets, the individual especially, all seek to network to an ever increasing degree. As a result, states are both more powerful and more vulnerable. Consequently the security and stability of states, the wellbeing of societies and the welfare of individuals depend on the functional efficiency of complex, coupled systems. Obvious examples are the power supply grid or cashless electronic payment. If these coupled systems become functionally compromised, this has a negative effect on states, markets and societies. This begs the question as to potential types of exercise of influence upon actors. How will conflict be conducted in future? What threats confront us in a complex, networked world?

One may assume that enemy hybrid power projection measures, as illustrated in the IFK model (see Figure 2 "Potential hybrid threats and strategies" below), would provoke hybrid countermeasures made evident by corresponding strategies. Here it is necessary to note that defensive countermeasures can also be applied in reverse and as offensive strategies.

One finding from the strategy and threat analyses is that the various states' security experts often envisage similar scenarios of threats in their security policy deliberations. Reviewing the security strategies of large states and alliances of states, e.g. the EU, shows clear correspondence with regard to security policy challenges. This can indicate two things: either those states are reacting independently to similar, real threats scenarios or they align with the threats scenarios of large states and make corresponding deductions for their own area (see Figure 2). Albeit this yields two challenges for small states:

a) on the one hand they would have to prepare to defend against the (hybrid) threat scenarios analysed by large states; and
b) on the other, develop strategies against the potential (hybrid) offensive strategies of large states (as well as those of non-state actors).

Categories of the exercising of power, like politics, economy, ecology, cyber, culture, media and armed forces, whether on the ground, at sea, in the air or in space, all have a significant role to play here. Technological developments in particular increasingly enable non-state actors too (like conglomerates for example) to influence states by exercising hybrid power either in partial or indeed all categories. Worthy of emphasis here are potential influences on critical infrastructure.

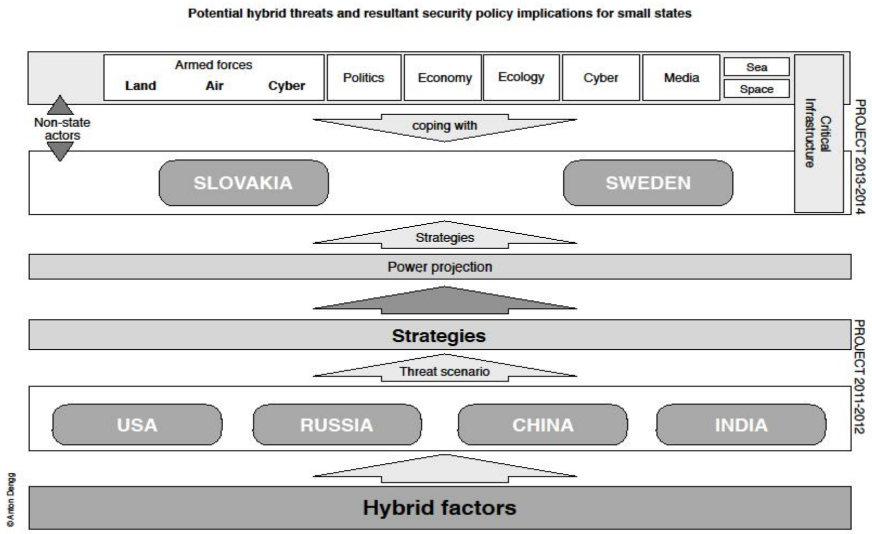


Figure 2: Potential hybrid threats and strategies
Anton Dengg

One may assume that small states primarily refer to large states' perceived threats. Only this can explain the fact that they too are practically identical in terms of their analyses of threats and strategies. Nevertheless one must take account of the fact that, in times of increasing political and economic globalisation, small states must orient themselves towards global realities of security policy and so have the similarities in threat analyses explained to them. The complexity of this situation highlights, notwithstanding the many advantages that globalisation confers, dangers and threats for states and societies too. With increasing multiple layering of infrastructure, both dependency and vulnerability grow. As a result, the security of societies is endangered just as much as that of each individual. The state as sovereign of legitimised instruments of power therefore has to apply protective measures. Yet how should/must a state react? Which countermeasures to deploy when?

1.2.5 The Concept of "Hybrid Threat"

For a long time, people have been seeking answers to the challenges of "new" or "asymmetric wars". The aim of employing the term "hybrid threat" to introduce a new category into the research debate now requires explanation. Where is this term being discussed and what if any new findings can be gained in consequence? Do resultant countermeasures arise?

Fundamentally of note is that there is no consistent single definition of the term "hybrid threats". In the Anglo-American domain there is ever more reference to the term *hybrid warfare*. This involves engaging in combat using both conventional military and unconventional elements using corresponding means and methods (e.g. with non-military forces, guerrillas, terrorists and criminal tactics).

The definition of "threat" in the *Wörterbuch Sicherheitspolitik* is:

> "[… the perception of existential endangerment of a state, federation of states or alliance as a result of the policy of another state, federation of states, or those dan-

> gers, usually asserted through superior means of military power, which are brought to bear on their security, sovereignty or integrity ...]"[29].

Here this threat might only be the subjective assessment of a latent endangerment of state security. Whether the threat actually becomes real depends on the capabilities and intentions of the opponent. Only at the point of capability, which is linked to an intent to harm, is a real threat presented. Here the intent can change abruptly, as the build-up of appropriate options requires the provision of resources and, in particular, a certain lead time. To summarise: a threat is composed of capability and will together, of capability and intent. Whilst capacity build-up occupies a certain amount of time and can be observed, the identification of an intent to harm is much more difficult.

Politics can move abruptly with the unforeseen consequence that a strategic partner can become and actual threat. This could be observed in the case of the Ukraine conflict, which surprised the European Union (EU).

The term "hybridity" comes from biology, albeit originally from agriculture. There the term indicates the result of mixing two previously separate systems. However, the German dictionary *Duden* defines "hybrid" as a mixture of two or more components. An example from the animal world is the mule, a cross between a horse and a donkey, which is bred so as to emphasise significant advantages of each respective animal. A new "product" had arisen. Combining two or more originally independent elements allows something new to emerge here. Here the new relates not only to the internal composition but also has a decisive effect on its environment. For the conception of a "hybrid threat" this means that forms of threat recognised to date come to be combined in new ways. Ultimately the new configuration of existing conflict phenomena and forms of threat extends the threat spectrum.

[29] Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald; Schreiner/Karl H. and Bruzek, Oliver: Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000, p. 38. Translation from the German original quotation.

It can therefore be stated that hybrid threats constitute a synthesis of conflict scenarios long regarded as isolated. There is not the hybrid threat as such, but rather different threats that arise from diverging variations of alternating combinations, thereby giving rise to alternating effects and lines of attack. Hybrid threats should anyway be considered in the plural. As a consequence, methods of resolution, protective and defensive mechanisms need to be developed with corresponding multiplicity.

Conceptually, hybrid threats are composed of several elements of conventional perceived threats. The military form of implementation (h*ybrid warfare*) is therefore to be regarded as only a subset of the hybrid threat spectrum. In an article on hybrid warfare, Hoffmann refers to the National Defense Strategy (NDS) 2005, according to which hybrid warfare constitutes a mixture of traditional, irregular, terrorist and disruptive threats.[30]

The concept of hybrid threats extends beyond that of *hybrid warfare*, given that it also takes non-military means into account. In conceptual terms, this perceived threat represents a reaction to the increasingly diffuse nature of conflicts since the collapse of East-West confrontation. Hoffmann writes:

> “[…] our greatest challenge in the future will come not from a state that selects one approach, but from states or groups that select from the whole menu of tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography and aims.”[31]

Thus hybrid threats are characterised by the use of both conventional and irregular tactics, by decentralised planning and execution, the presence of non-state actors and application of high technology. The combination of different tactics and methods leads to a “division of labour” between state entities and non-state groupings along with the establishment of novel, innovative associations, which are in a position to carry out all activities.

[30] Hoffman, Frank G.: Hybrid Warfare and Challenges. In: JFQ, issue 52, 1st quarter 2009, p. 35. <http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf>, accessed on 21/11/2015.

[31] Hoffmann, Frank G.: Hybrid Threats. Reconceptualizing the Evolving character of Modern Conflict. In: Strategic Forum, 240/2009, p. 5.

In 2010, the United States Government Accountability Office (GAO) in Washington looked into hybrid warfare tactics that are highly likely to be used by current and future adversaries. According to this, U.S. troops will be confronted by threats like:

> “[...] non-state and state-sponsored adversaries, including computer network and satellite attacks; portable surface-to-air missiles; improvised explosive devices; information and media manipulation; and chemical, biological, radiological, nuclear, and high-yield explosive devices”[32]

Notwithstanding this finding, the Department of Defense (DoD) has no official definition of a hybrid threat and “... has no plans to do so because DOD does not consider it a new form of warfare.”[33] Indeed several U.S. experts from politics and the military go on to affirm that they do not use the term “hybrid warfare” in their doctrines for these ever more complex conflicts.[34]

In the GAO paper mentioned above, a working definition of “hybrid threat” produced by the Joint Irregular Warfare Center is mentioned by way of example. Here “hybrid threat” is characterised as:

> “An adversary that simultaneously and adaptively employs some fused combination of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors.”[35]

In 2011, the U.S. Army defined the term “hybrid threat” in their “Opera-

[32] GAO, United States Government Accountability Office: Subject: Hybrid Warfare. GAO101036R Hybrid Warfare. Washington, DC 10709/2010, p. 1. <http://www.gao.gov/new.items/d101036r.pdf>, accessed on 21/11/2015.

[33] Ibid, p. 2.

[34] Ibid, p. 2.

[35] Working definition derived by U.S. Joint Forces Command, Joint Irregular Warfare Center, 20082009. In: GAO, United States Government Accountability Office: Subject: Hybrid Warfare. GAO101036R Hybrid Warfare. Washington, DC 10/09/2010, Enclosures, p. 18. <http://www.gao.gov/new.items/d101036r.pdf>, accessed on 21/11/2015.

tions Doctrine". It is taken to mean: "The diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects."[36] Even though the GAO's proposed definition is not dissimilar to the IFK working definition, it appears that, particularly in that of the U.S. Army, hybrid threats are seen more as military hostilities in the U.S. context.

A further potential approach to attempting a European definition was delivered by the European Council on Security and Defence in 2013:

> "The world as a whole faces increased volatility, complexity and uncertainty. A multipolar and interconnected international system is changing the nature of power. The distinction between internal and external security is breaking down. Complex layers of governance and new patterns of interdependence empower new players and give rise to new challenges. "[37]

From the variety of definitions given above, it is possible to see why it was necessary to develop a working definition of "hybrid threat", which was acceptable for all participating experts and generally comprehensible, at the start of the project. In the course of the research project, the following working definition was ultimately developed:

"A hybrid threat is a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as being multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests."[38]

[36] U.S. Army: Field Manual 30 Operations C1. GPO, Washington, DC February 2011, p. 1ff. In: MAJ Brian P. Fleming, United States Army: The Hybrid Threat Concept. Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. Report. 17/05/2011, p. 2. <https://www.hsdl.org/?view&did=700828>, accessed on 21/11/2015.

[37] High Representative/Head of the EDA on the Common Security and Defence Policy: Preparing the December 2013 European Council on Security and Defence. Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy. Brussels 15/10/2013. <http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf>, accessed on 21/11/2015.

[38] Working definition developed by The Institute for Peace Support and Conflict Ma-

To this working definition should be added that threat activities must exceed a strategic threshold in order to count as a hybrid threat. This comes to apply if the hostile activity substantially limits the attacked state's freedom to act or decide. The form this limitation takes may differ from case to case and, depending on its effects, may be interpreted differently by each state.

What remains is the question of identifying a strategic threshold. One approach would be: this is exceeded if at least two sectors are affected by hybrid threats and accordingly at least two ministries are involved in defending against them.

From what has been stated so far it is evident that, in its approach to a working definition, the IFK interprets the term "hybrid threats" more comprehensively and in greater detail than is to be found in other attempts at defining the term.

Looking across the broad range of international publications, "hybrid threats", as interpreted by the IFK, are scarcely discussed. As mentioned, there is treatment of the topic of hybrid warfare which, in the view of the authors of this work, is more limited to hard power (namely combat with weapons and ordnance). Initial indications (NATO is working on "hybrid threats" for example) allow for a change of mind among experts to be recognised, in which there is an increasing trend to move beyond *hybrid warfare*. Differences in the definition tend to result more from different interpretations of "war". Is smart power "war"? What is the threshold beyond which hard power might be termed "war"? Or: what scale of terrorist activity must prevail for a "war on terror" to be declared?

Given that the term war is disputed, no more detailed description will be attempted here. However it has been determined that the designation

nagement of the National Defence Academy (Dengg/Feichtinger/Schurian) on the basis of: Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald/Schreiner, Karl H. and Bruzek, Oliver. Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000.

“war” only becomes permissible once a conflict involving substantial force of arms is waged between at least two states. Thus the designation of “war” does not apply in the case of a hybrid threat, because of the deployment of many kinds of power projection including some that involve no use of physical force.

In 2011 the NATO Allied Command Transformation (NATO ACT) brought together around 100 experts drawn from both the private sector and specialists from NATO and ran a one-week multiple scenario experiment with the theme “Countering Hybrid Threats”. Striking here is the evident change in direction from *hybrid warfare* to “hybrid threats”. This NATO simulation makes clear a broader interpretive approach from this point on. NATO describes terrorism, migration, piracy, corruption, ethnic conflicts as parts of hybrid threat. In an orchestration of diplomacy, political interaction, humanitarian aid, social pressure, economic development and a skilful media campaign, alongside the deployment of armed forces, the organisation sees a hybrid threat as “[...] those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives”.[39] Thus the approach to a working definition of “hybrid threat” taken by the IFK aligns closely with that of NATO. A press release of June 2015 proves that NATO has not stopped dealing with hybrid threats. In a common statement the Ministers of Defense of the member states express their determination to resolutely confront the new threats. „We have set the key elements for an effective response to hybrid threats.”[40]- In January 2016 NATO General Secretary Jens Stoltenberg informed the public among others about effective NATO measures to combat hybrid warfare: „To combat hybrid warfare, we are improving our intelligence and early warn-

[39] Miklaucic, Michael: NATO Countering the Hybrid Threat. <http://www.act.nato.int/nato-countering-the-hybrid-threat>, accessed on 08/12/2015.

[40] Ministerial Meeting, Meeting of NATO Ministers of Defence, Brussels, Belgium, 24-25 June 2015; Press Release (2015) 094 of 25 June 2015; Last updated: 25 Jun. 2015 13:11: Statement by NATO Defence Ministers, Item 7; http://nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en; queried on 01.02.2016

ing."[41]– In February 2016 a report in a German newspaper underlined Stoltenberg's words with an information from higher NATO circles that 28 minsters of the alliance are being confronted with a hybrid situation.[42]–

It is a very interesting fact that the European Union is also concerned about the hybrid threat which is reflected in a statement of the "European Agenda on Security". It says: "[…] threats such as those posed by cyberterrorism and hybrid threats could increase in the years to come."[43]

It is a very interesting fact that in 2015 the European Union has already been concerned about the hybrid threat which is reflected in a statement of the "European Agenda on Security". It says: "[…], threats such as those posed by cyberterrorism and hybrid threats could increase in the years to come."[44]

Moreover, on April 6, 2016 the European Commission adopted a "Joint Framework on countering hybrid threats"[45] that is to be seen as a rigorous response to the increasing hybrid threat.

[41] NATO: Press conference by the NATO Secretary General Jens Stoltenberg at the launch of his Annual Report for 2015, 28. Jan. 2016; http://www.nato.int/cps/en/natohq/opinions_127496.htm; queried on 02.02.2016.

[42] Bolzen, Stefanie; Schiltz, Christoph B.: Nato simuliert in geheimer Aktion Angriff aus dem Osten. Die Welt online 31.01.2016 [Nato simulates attacks from the East in a secret mission. The world online 31.01.2016]; http://www.welt.de/politik/ausland/article151674938/Nato-simuliert-in-geheimer-Aktion-Angriff-aus-dem-Osten.html; queried on 01. Februar 2016.

[43] European Commission: The European Agenda on Security. COM(2015) 185 final, of 28.04.2015, S. 15; <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_de.pdf>, accessed on 24/03/2016.

[44] European Commission: The European Agenda on Security. COM(2015) 185 final, of 28.04.2015, p. 13; <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_de.pdf>; accessed on 24/03/2016.

[45] European Commission: Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. A European Union response. Brussels, 6.4.2016, JOIN(2016) 18 final.

1.2.6 Enforcement of interests as the aim of a hybrid threat

For Clausewitz, war is "[... therefore an act of violence to compel our opponent to fulfil our will]"[46]. Thus war is the enforcement of interests. On the other hand, however, not every type of interest enforcement has to be war.

By using the instruments from his "toolbox" of hybrid "weapons" in a concerted manner, an actor can seek to enforce and secure his interests. A hybrid approach with non-military means against a targeted state might take place rather if a direct (military) confrontation seems less rewarding or could damage the actor's international reputation. The actual enforcement of interests, the weakening of the adversary, can also be achieved by using other means and methods (than military).

To distinguish a hybrid *threat* from other broad policy approaches, it is necessary to have criteria that, through an analysis, allow for a differentiation of the coordinated use of instruments from different areas of threats by its harmful and its beneficial impacts.

Such a differentiating feature is the stabilising impact through a multi-dimensional approach. For example Austria's involvement in Bosnia-Herzegovina (BiH) is a policy of multi-dimensional enforcement of interests, affecting the targeted country's (BiH) security sector[47], judicial system[48] and economy[49]. However, the intention is not the implementation of

[46] Clausewitz, Carl von: Vom Kriege (On War). In: Von Clausewitz, Sun Tzu: Vom Kriege und die Kunst des Krieges [On War and the Art of War]. Meisterwerke der Strategie [Masterpieces of Strategy]. Edited by: MaxiBucks. 1. Edition, 2011; iBooks Store; vertical format p. 22. Translation from the German original quotation.

[47] Cf. Kugelweis, Pierre: Universität Graz und Streitkräfte blicken gemeinsam auf Bosnien-Herzegowina [The University of Graz and the Armed forces jointly look at Bosnia-Herzegovina]. In: Der Soldat [The Soldier], 23/2010, 01/12/2010. <http://www.dersoldat.at/universitaet-graz-und-streitkraefte-blicken-gemeinsam-aufbosnien-herzegowina?PHPSESSID=66m5qg8qftiuu6kuj0tdh2f7g6>, accessed on 08/12/2015.

[48] Ibid.

a hybrid threat, but to contribute in "[... assisting the Balkan state on its way towards a peaceful and democratic future]"[50]. A hybrid threat with the same broad approach would rather aim at the contrary: internal destabilisation, disintegration, public fear and disturbance, economic volatility and diplomatic isolation to enforce one's own interests. A hybrid threat must therefore be designated as a type of negative use of force.

1.2.7 Force

Force is closely linked to the term power, from which a threat (often perceived subjectively) can be deduced. The term force is a daily companion in the world of news. Newspaper articles show the use of the term force, such as: the force of the militias; fuel rods are dragged out by force; journalists are exposed to force; reports on forceful incidents; clerical force; somebody is being blackmailed under the threat of force. The term "force" is therefore often used in different contexts.

Force is

> "[... in the broader sense of politics a collective term for efforts by individual or collective actors that are aimed at manipulating and shaping public policy concerns, under threat of or the use of physical or psychological coercion against health and life or through hidden violence (»structural violence«).]"[51]

For Clausewitz physical force is the means to submit the enemy to our will. Specialist literature distinguishes between different kinds of force: *physical*,

[49] Federal Ministry for Europe, Integration and Foreign Affairs, Republic of Austria: Außen- und Europapolitischer Bericht (Foreign and European Policy Report) 2013; p. 87; <http://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Publikationen/AEPB/Aussen_und_Europapolitischer_Bericht_2013.pdf>, accessed on 19/01/2015.

[50] Austrian Armed Forces: Bundesheer in Bosnien [Armed Forces in Bosnia]. <http://www.bundesheer.at/ausle/eufor/index.shtml>, accessed on 08/12/2015. Translation from the German original quotation.

[51] Schmidt, Manfred G. Wolfgang: Wörterbuch zur Politik [Political Glossary]. Stuttgart 1995, p. 367. Translation from the German original quotation.

psychological, *institutional*, *structural* and *cultural* or *symbolic* force[52]. According to Bonacker and Imbusch, *physical force* has the aim of impairing, injuring or killing other persons, while *psychological force* is based on words, images, symbols, intimidation and fear.[53] *Institutional force*, however, aims at relations of dependency and submission[54], comparable to soft power. "[The prototype of institutional force in the modern era is the claim for sovereignty and obedience posed by the state towards the individual.]"[55] Within this context, force is used by the state's security institutions. Bonacker and Imbusch include Galtung's term of *structural violence* in their categorisation, which shall be mentioned for the sake of completeness. Violence is immanent and omnipresent within a society's social structure. Broadly speaking, it is a form of social "injustice"[56].

Bonacker and Imbusch also use Galtung's concept of *cultural violence*. This includes those aspects of culture "[... that can be used to justify or legitimate direct, illegitimate, institutional or structural violence]"[57]. In the case

[52] Cf. Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden [key terms of peace and conflict research: conflict, force, war, peace]. In: Imbusch, Peter/Zoll, Ralf (Eds.): Friedens- und Konfliktforschung. Eine Einführung [peace and conflict research, an introduction]. Wiesbaden 2006, p. 86.

[53] Ibid, p. 86f.

[54] Ibid, p. 87.

[55] Waldmann, Peter: Politik und Gewalt [politics and force]. In: Nohlen, Dieter/Schultze, Rainer-Olaf (Eds.): Politische Theorien [political theories], Munich 1995, p. 431. Quoted from: Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden [key terms of peace and conflict research: conflict, force, war, peace]. In: Imbusch, Peter/Zoll, Ralf (Eds.): Friedens- und Konfliktforschung. Eine Einführung [peace and conflict research, an introduction]. Wiesbaden 2006, p. 87. Translation from the German original quotation.

[56] Galtung, Johann: Gewalt, Frieden, Friedensforschung (violence, peace and peace research). In: Senghaas, Dieter (Eds.), Kritische Friedensforschung [critical peace research], Frankfurt am Main 1971, p. 62. Quoted from: Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden [key terms of peace and conflict research: conflict, force, war, peace]. In: Imbusch, Peter/Zoll, Ralf (Eds.): Friedens- und Konfliktforschung. Eine Einführung [peace and conflict research, an introduction]. Wiesbaden 2006, p. 88.

[57] Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktfor-

of *symbolic violence*, violence is understood as a verbal or cultural means of expression[58]. This includes e.g. insult, discrediting, humiliation or defamation. Although Bonacker/Imbusch refer to people, this type of force is not discussed with regard to a society or an ethnic, religious or other community. The difference from *psychological violence* is in fact its purpose. While *psychological violence* is aimed at intimidation and fear, in *symbolic violence* the degradation of the counterpart plays a crucial role.

The use of force can therefore pursue two kinds of objectives. Either force is used to achieve power or to stay in power. This leads to the term *Power*.

1.2.8 Power

The US citizen Robert Kagan characterises power as "[... the ability to get others to do what you want and prevent them from doing what you don't want.]"[59]. For this, the use of force is not always necessary. The exercising of power, particularly with the use of means other than military, namely by hybrid methods, is reflected in the United States of America's (USA) security strategy: "While the use of force is sometimes necessary, we will exhaust other options before war whenever we can, and carefully weigh the costs and risks of action against the costs and risks of inaction."[60]

Joseph Nye defines power as the ability to influence the behaviour of others to one's advantage.[61] According to Nye, power can be exercised, if one

schung: Konflikt, Gewalt, Krieg, Frieden [key terms of peace and conflict research: conflict, force, war, peace]. In: Imbusch, Peter/Zoll, Ralf (Eds.): Friedens- und Konfliktforschung. Eine Einführung [peace and conflict research, an introduction]. Wiesbaden 2006, p. 89. Translation from the German original quotation.

[58] Ibid, p. 89.

[59] Kagan, Robert: Die Demokratie und ihre Feinde. Wer gestaltet die neue Weltordnung? (The return of History and the End of Dreams) Munich 2008, p. 20. Translation from the German original quotation.

[60] President of the United States: National Security Strategy. Washington May 2010, p. 22. <http://nssarchive.us/NSSR/2010.pdf>, accessed on 08/12/2015.

[61] Cf. Nye, Joseph p. Jr.: Soft Power. The Means to Success in World Politics. PublicAffairs 2004, p. 2.

is in possession of capabilities and resources to exercise appropriate influence.[62] Thus a threat can only originate from those actors who, besides willingness, also hold the means necessary to exercise power. According to Nye, power can, as already mentioned, be exercised through two areas: through hard and soft power. Subsequently, Nye ads a third one that represents a mixture between the ones mentioned: smart power. Nye describes hard power as an inducement/threat tactic ("carrots and sticks"[63]), while soft power can be described as the persuasion to strive after values considered as ideal. Soft power has been used successfully when the arguments used can convince an actor to support them, which is reflected in Robert Kagan's definition. Nye states that soft power is based on cultural and political ideals, such as foreign policy, if it is considered legitimate. Smart power, on the other hand, is "[...] the ability to combine hard and soft power into a successful strategy."[64]

1.2.9 Hybrid warfare versus warfare so far

So how does a hybrid threat exceed the previously perceived threats? If the concept is not to vanish in unsubstantial conceptual confusion, hybridity as a distinctive feature must consequently stand out from other perceived threats Therefore hybrid threats have to be differentiated from other conflict scenarios, such as conventional, total and asymmetric war.

(1) Hybrid threats versus conventional war

Conventional war is "[... collective organised force involving the state]"[65], particularly fighting in an "open" battle against another state's armed forc-

[62] Ibid, p. 3.

[63] Ibid, p. 5.

[64] Nye, Joseph S. Jr.: Smart Power. The Blog. <http://www.huffingtonpost.com/josephnye/smart-power_b_74725.html>, accessed on 08/12/2015.

[65] Cf. Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- and Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden [key terms of peace and conflict research: conflict, force, war, peace]. In: Imbusch, Peter/Zoll, Ralf (Eds.): Friedens- und Konfliktforschung. Eine Einführung [peace and conflict research, an introduction]. Wiesbaden 2006, p. 107ff. Translation from the German original quotation.

es. Use of violence as a substantial characteristic of wars lies within the synonym "armed conflicts".

A hybrid threat does not necessarily include force of arms. It can appear without the use of physical force, but it has to include a combination of non-violent practices to be considered as a hybrid threat.

(2) Hybrid threats versus total war

In a case of total war, all means are used, under the control of a centralised administration and a rigid organisation that aims to maximise military capabilities. The largest possible number of people are mobilised to participate in the war, as soldiers on the one hand and as part of the production of weapons and supplies on the other. The main purpose of total war is the deployment of maximum military force to defeat the adversary or to eliminate him physically. The aim of total war is victory, which is achieved by eliminating the adversary. It absolutizes itself as being distinct from its political purpose and is at risk of gaining a fatal momentum of its own. In total war, the "[grammar of the war replaces the logic of politics]"[66]. Military supremacy stands opposite political impotence.

Hybrid threats are in this respect similar to total war, as multiple instruments (economics, public and published opinion, legislation, etc.) are being used to harm the adversary. Conflict actors, planning on carrying out a controversy in a hybrid manner, run the risk of letting the conflict escalate through counter reaction (e.g. through multiplier effects[67]), thereby becoming intensified.

Contrary to total war, hybrid threats are not aimed at the complete elimina-

[66] Hofmeister, Heimo: Theorie des Terrorkrieges [theory of terrorist war]. In Gustenau, Gustav (Ed.): Zur Theorie des Terrorismus [on the theory of terrorism] (4/02). Vienna 2002, p. 10. Translation from the German original quotation.

[67] For further explanations see below in this section.

tion of the adversary and the destruction of vital structures. Instead, hybrid threats are to be classified as overextension strategies on various levels in multiple spheres that collectively lead to a multiple institutional breakdown.

(3) Hybrid threats versus asymmetric war

Symmetric wars (also named "Westphalian wars") are armed conflicts between two homogenous violent actors. In this case, two violent actors face each other who are both equal, or symmetric, regarding their legal status, the training of their armed forces, the technologies used and the tactics applied. One characteristic of the symmetry is the exercising of military operations that are limited to a certain profession, with its members being considered as combatants.

Asymmetric wars, on the other hand, are characterised by a deceleration of conflict dynamics, heterogeneity of actors and normative inequality[68]. Asymmetric warfare is characterised by diverse groups of actors, ranging from conventional armed forces, through paramilitary volunteer forces and private military service providers to organised criminal terrorists acting across borders. The distinction between combatant and non-combatant and between frontline and hinterland becomes blurry.

Hybrid threats can overlap partially with asymmetric warfare. A violent actor acting asymmetrically might use several other means in an interconnected manner on different levels (i.e. hybrid) against a targeted country, to compensate for his (e.g.) military inferiority.

The initiator of such a threat will direct his attacks against areas in which there is a significant imbalance of power and resources in his favour (similar to military tactics). He will conduct operations in physical and virtual areas in which the desired impact is achieved with the minimal use of resources. Technological superiority is a pillar of this asymmetric warfare.

[68] Explanation: While a state's armed forces are bound by international humanitarian law, non-state combatants might hardly feel committed to it.

1.2.10 Hybrid threat factors

There are many and varied possibilities of influencing a state. They increase with the complexity of processes and technological progress. Hybridity is not a new phenomenon. New challenges arise from contemporary technologies and modern communication strategies, affiliated to global interconnectedness. The latter enables the actor to use a previously unknown variety of means and methods to influence a counterpart.

Besides the positive aspects for societies that new technologies involve (e.g. in cyber areas through interdisciplinary interconnectedness), there are also negative interdependencies emerging. The breakdown and therefore the lack of certain areas of technology show e.g. the dependency and ultimately the vulnerability of our infrastructure. With a systems failure, consequences arise in an avalanche-like manner, with sometimes dramatic impacts. The currently much-cited *black out* in the electricity industry is seen as the best example of this. The special characteristic in this case: a wide-ranging blackout is not necessarily the result of a technological defect. It can also have a man-made cause, e.g. through a technical "error" in the equipment. The specific in this case is that the saboteur's physical presence is not bound to the location of the attack, as attacks can be made from a distance, through cyberspace. Attacks planned well in advance, with synchronized procedures including a similar approach as used in the case of the *Stuxnet*[69] malware, being conceivable. Comparable incidents cannot be excluded for all information technology (IT)-based infrastructure.

Globalisation makes responsible action mandatory, especially in security policy issues. In this context, contributions to providing national and international crisis and conflict management (ICCM) represent a crucial element. This is intended not only to provide security in conflict zones but also further to reduce backlash on one's own state and ideally completely to

[69] *Stuxnet* was a computer worm targeted at highly specialised industrial facilities in critical infrastructure. See: Karnouskos, Stamatis: Stuxnet Worm Impact on Industrial Cyber-Physical System Security. SAP Research, Germany. <http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf>, accessed on 08/12/2015.

prevent them. Here the largest challenge is the growing number of protagonists besides means and methods. This is illustrated by the conflicts in Syria or eastern Ukraine. Regular security forces face a growing number of combatants from non-state actors, such as radical religious groups, diverse ethnic militias, guerrillas, mercenaries and ideologically convinced supporters and members of the opposite state's armed forces without corresponding labelling. In such cases there can be no talk of a monopoly on the use of force. Instead it has to be regarded as an "oligopoly on the use of force"[47] and further even as a "oligopoly on the use of force"[70]. A German newspaper described these circumstances in June 2014:

> "[NATO is particularly alarmed by Russia's newly developed "subversion strategy".[71] To date it is internally named "hybrid warfare". According to NATO analyses, Moscow's new military tactics consist of infiltrating certain areas with military experts, called "little green men" in NATO parlance, who advise and instigate insurgents and train them in the use of military equipment.]"[72]

The article cites a high-ranked NATO officer saying "[They destabilise, without firing one conventional shot themselves]"[73].

As a consequence, a type of psychological warfare is being established that is paired with supporting measures as e.g.: military training and instruction, provision of materials, propaganda support by the media and/or the "provision" of subversive forces. This method is indeed common and has already been used by Western powers in similar ways. In this context for example Gert Sommer reported in a book article: "[Officially the war in

[70] Oligopoly on the use of force has to be understood in contraposition to the term monopoly on the use of force. "Security" is basically ensured by the state whereas, especially in crisis regions, various groups often assert to their clientele that they provide their security.

[71] Schiltz, Christoph B.: Die Nato zittert vor Russlands neuer Strategie. [NATO is afraid of Russia's new strategy] In: Die Welt, 25/06/2014. <http://www.welt.de/politik/ausland/article129431400/Die-Nato-zittertvor-Russlands-neuer-Strategie.html>, accessed on 08/12/2015. Translation from the German original quotation.

[72] Ibid Translation from the German original quotation.

[73] Ibid Translation from the German original quotation.

Libya began two days after the United Nations' (UNO) Resolution 1973 (17/03/2011). But the direct prearrangements for the war apparently began earlier.]"[74] Sommer refers to a report by the British newspaper Sunday Mirror of March 23rd 2011, according to which "Hundreds of British soldiers have been operating with rebel groups inside Libya for three weeks"[75].

This method therefore constitutes a new kind of quality, since voluntary combatants are being organised by another state, which is however denied officially. Hence a clear distinction between ally and enemy, or between combatant and non-combatant, becomes indistinct.

This distinction becomes even more difficult to draw in the case of cyber attacks. The challenge here lies not only in locating the origin of the attacks territorially but also in ascribing them to a determined actor. If the source of the attack can actually be traced back, the question still arises, whether this actor is in fact the initiator of this activity. Or is another actor just building on the latter's infrastructure? This complicates the analytical work of security experts as well as appropriate counter reactions. Specifically in the case of cyber issues, the question arises as to the level at which states are obliged to provide their own defence in order to count as reliable partners.

[74] Sommer, Gert: Der Libyen Krieg: Reflektionen zu Gaddafi und anderen Beteiligten [the war in Libya: reflections on Gaddafi and other participants]. In: Becker, Johannes M./Daxner, Michael und Sommer, Gert (Eds.): Der Libyen Krieg. Das Öl und die "Verantwortung zu schützen" [the war in Libya: oil and the "responsibility to protect"]. In: Schriftenreihe zur Konfliktforschung [series on conflict research], Volume 26. Berlin 2013, p. 206. Translation from the German original quotation.

[75] The Mirror: Crack SAS troops hunt Gaddafi weapons inside Libya. 20/03/2011. <http://www.mirror.co.uk/news/uk-news/crack-sas-troops-hunt-gaddafi-117405>, accessed on 08/12/2015. In: Sommer, Gert: Der Libyen Krieg: Reflektionen zu Gaddafi und anderen Beteiligten [the war in Libya: reflections on Gaddafi and other participants]. In: Becker, Johannes M./Daxner, Michael und Sommer, Gert (Eds.): Der Libyen Krieg. Das Öl und die "Verantwortung zu schützen" [the war in Libya: oil and the responsibility to protect"]. In: Schriftenreihe zur Konfliktforschung [series on conflict research], Volume 26. Berlin 2013, p. 206.

If an actor's cyber attacks are executed from one state's territory against another state, this raises the question as to whether there is a need for future regulation, according to which the state, from whose territory the attack originates, has to be held accountable due to its insufficient protective measures.

Similar challenges emerge with social networks such as Facebook and Twitter. They are currently an important component in the transfer of information (state of knowledge) about a crisis region. The extensive access possibilities to various social media by almost any user also present the opportunity for propaganda. Media reports on corporations paying for a positive depiction in online forums[76] provide an insight into the corresponding possibilities. Furthermore, enormous challenges arise in the moral and legal perspective, like: is there a deliberate launch of information through social media to call for political actions by states? Must/should states influence social networks to counteract appropriately? Are states responsible and therefore accountable for the instrumentalised spreading of radical propaganda and false reports through servers located on their state-territory? The growing number of tablet computers and smartphones significantly increases the corresponding legal challenges and could particularly influence intra-state conflicts. The Heidelberg Institute for International Conflict Research's Conflict Barometer shows 414 conflicts[77], for the observation period 2013, of which 337 were classified as so-called "intrastate conflicts" and only 77 were "interstate conflicts". Could future cyber possibilities intensify these conflicts or increase their number?

[76] ÖBB, ÖVP und Bank Austria zahlten für positive Internet-Forenbeiträge [ÖBB, ÖVP and Bank Austria paid for positive posts in Internet forums]. In: Die Presse Online. 06/11/2014. <http://diepresse.com/home/techscience/internet/4587699/OBB-und-Bank-Austria-zahlten-fur-positive-InternetForenbeitraege>, accessed on 08/12/2015.

[77] Heidelberg Institute for International Conflict Research (HIIK): Conflict Barometer 2013. February 2014. <http://hiik.de/de/downloads/data/downloads_2013/ConflictBarometer2013.pdf>, accessed on 08/12/2015.

1.2.11 General reflections on "Hybrid threat potentials and the resulting security policy deductions for small states"

The new information age offers a wide range of exceptional perspectives that were considered simply impossible a few years ago. The rapid proliferation of smartphones and all their technical capabilities, e.g. Global Positioning System (GPS) tracking, saving and sending of films and pictures or information, enable worldwide provision of information by every user with scarcely any delay. One example is the U.S. special operation in May 2011 to capture Osama Bin Laden, at which the helicopter operation in Abbottabad Pakistan had been put online by a Twitter user in real time[78] – although initially not making a connection to Al-Qaeda or Osama Bin Laden.

Further examples are posted casualty figures or calls for perseverance. "Spiegel Online" reported on Syrian opposition groups, writing on Twitter about more than 650 fatalities, due to the use of chemical weapons.[79] Since information like this can be hardly verified in this rapid media age, it can lead to political misinterpretation and a state's overreaction.

A further challenge appears through similar reports: The verifiability of an Internet report's substance resulting, given the corresponding intention, in a threat.

Another analogous threat, located in the hybrid area, appears from publishing alleged misconduct of the state's security actors. This was the case

[78] See: Osama bin Laden killed: Pakistani man live tweets deadly raid. In: The Telegraph, 02/05/2011. <http://www.telegraph.co.uk/technology/twitter/8487686/Osama-bin-Laden-killed-Pakistani-man-live-tweets-deadly-raid.html>, accessed on 08/12/2015.

[79] Reuter, Christian: Bürgerkrieg in Syrien: Aktivisten werfen Assad Giftgaseinsatz mit Hunderten Toten vor [civil war in Syria: activists accuse Assad of using toxic gas with hundreds dead]. In: Spiegel Online, 21/08/2013. <http://www.spiegel.de/politik/ausland/aktivisten-in-syrien-neuer-giftgasangriff-von-assads-armee-a-917699.html>, accessed on 08/12/2015.

when personal data about the protagonists were spread, including data about their family members.

The purpose of these activities (the data were published in listed form) can be regarded as prompting lynch law or vigilantism or to expose the acting persons. One example is the use of pepper spray by a policeman during the so-called Occupy protests in New York.[80] This policeman's personal data were spread on the Internet by the *Anonymous* group. He was accused of having used the irritant against a peaceful protestor. In a similar manner, *Anonymous* published personal data (name, address, dates of birth) of 25,000 Austrian public officials of the Ministry of the Interior through a Twitter account in 2011.[81] In general the possibility cannot be excluded that pressure may be applied to security forces/security ministries and politicians during a hybrid power projection through media tools.

One further aspect in current and future hybrid threat scenarios is the constantly simpler broadcasting of digitised and "classified" information to non-authorised persons or institutions. The publication of classified information through Wikileaks or by the US citizen Edward Snowden in early 2013 demonstrate the extent to which, in the current IT world, individuals in lower and middle levels of command can get access to broad, classified knowledge and also use it accordingly. Such publications can, if orchestrated with other hybrid tactics, have eminent, security policy related impacts on a state.

Within the EU, methods of soft- and hard power are apparently also used to enforce political objectives, wittingly or unwittingly. When Swit-

[80] McVeigh, Karen: Occupy Wall Street activists name officer over pepper spray incident. In: The Guardian, 26/09/2011 26.09.2011.<http://www.theguardian.com/world/2011/sep/26/occupy-wall-street-police-named>, accessed on 08/12/2015.

[81] Proschofsky, Andreas: Anonymous veröffentlicht Daten von Polizisten [Anonymous publishes policemen's data]. In: Der Standard Online, 26/09/2011. <http://derstandard.at/1317018455940/Pwnyzei-Anonymous-veroeffentlicht-Daten-von-Polizisten>, accessed on 08/12/2015.

zerland did not extend its free movement of persons to Croatia, the EU reacted in February 2014 and terminated Switzerland’s access to the EU research programme “Horizon 2020” as well as to the student exchange programme Erasmus.[82]

The examples stated show that, for corresponding countermeasures within the whole spectrum of hybrid threats, special methods are necessary in order not to fall behind tactically, operatively or strategically.

1.2.12 Actors, level of ambition and methods for hybrid threats

In this section the individual elements of the definition of hybrid threat receive more detailed treatment.

(1) Endangerment of a state or an alliance of states

The methods of a hybrid threat are aimed at damaging substantial treasures of a state. These include not only territorial integrity and political sovereignty but also functioning commercial activity, social peace and public order.

Territorial integrity relates to respect for state territory and extends beyond physical living space. State territory includes land, stretches of water, offshore areas and airspace. As yet unresolved is whether and to what extent cyberspace, the fifth space, should be calculated into state territory. Can an aggressor actually violate a state’s virtual cyberspace and thereby its territorial integrity? Political sovereignty can be interpreted as the political community’s freedom to make decisions and express its wishes. So, for example, are disruptions of elections or referendums through the dissemination of false information aimed at influencing the results of elections to be seen as attacks on public freedom to express its wishes and consequently on political sovereignty (propaganda battle)?

[82] [Students and researchers demand participation in EU programmes]. In: Online Tagesanzeiger, 04/03/2014. <http://www.tagesanzeiger.ch/wissen/bildung/Studentenund-Forscher-fordern-Beteiligung-an-EUProgrammen/31353020/print.html>, accessed on 08/12/2015.

Similarly the build-up and support of armed opposition or local secessionist movements should be rated as endangerment of the state.

But just what are the scale and intensity of such threats? Not every threatening gesture is relevant in terms of security policy. *Ergo* it is necessary for a *strategic threshold* of threat presentation to be exceeded. This can only pertain if a state is substantially limited in terms of its freedom to act or decide. The assumption is that such intensive threats against substantial national treasure exceed a single state ministry's capacity to react, thereby raising the demand for cooperation.

(2) Who is the actor presenting a hybrid threat?

Fundamentally a hybrid threat can be presented by either a state or non-state actor. Examples of the latter include both terrorist organisations and conglomerates operating trans-nationally. In such a case, the actor must exhibit both the corresponding capacity (capabilities, resources, knowledge, objective element) and intention (policy, components of will, subjective element) for such a deliberate move. This allows a hybrid threat to be delimited to just one actor and to be isolated from other sources of risk such as climate change, ageing, state fragility, migration.

As laid out at the beginning, the deployment of a hybrid threat requires a combination of two components: on the one hand, the capability and, on the other, the will to deploy particular means and methods. If one of these components is missing, no hybrid threat is presented. Thus a state can indeed build up the capabilities and organisational prerequisites (resources, personnel, finance, mechanisms of cooperation, decision rules etc.) but, if the intent to deploy such capability against another state is absent, there can be no discussion of a "threat". On the other hand, a state might pursue the intent to deploy coordinated means against another state but, if it lacks the corresponding capability, there is once again no hybrid threat present (yet). Depending on the corresponding actor, the level of intent will be evaluated as "wishful thinking" or as a definite stage of preparation. In this context, one must include companies and non-state actors with appropriate potential power. It would be conceivable for private companies to pursue their own interests in terms of power whilst, on the other hand, receiving political objectives from the state.

The overview prepared by the project team and shown below serves as a simplified visualisation of offensive and defensive actors involved in hybrid threats and the corresponding means and methods employed. Ranged against such threats are potential defensive forces active within the state.

It must be born in mind here that, in the case of hybrid threats, several protagonists can present themselves in different guises and, as mentioned at the beginning of this work regarding the working definition, at least two governmental actors must be involved on the defensive side for it to be possible to talk of a hybrid threat. It must be mentioned that this overview should not be seen as a completed description of actors but rather serves solely as an aid to the analysis of a hybrid threats.

Hybrid Threats

	Hybrid Threats Offensive actors	Offensive means and methods (examples)	Objects of threats	Defensive and preventive means and methods (examples)	Defensive actors	
					national	international
	Simultaneous, systematic, targeted combination		SPACE, scale		Simultaneous, systematic, targeted combination	
HARD POWER	STATE POWER • Land-, air-, naval-, space- and special forces • Police, special forces • Intelligence • Justice	Military Operations NBC weapons Putsch* Surveillance, control, order, investigation, , arrest, custody Reconnaissance/espionage, manipulation, sabotage Penal prosecution, sentencing, punishment	STATE Individual Society	Military operations, defence, PsyOps, Security measures, control, establishment of order, investigation, custody Gathering of information, analysis, assessment, protection Penal prosecution, sentencing, punishment	STATE POWER • Ministry of defence (armed forces, counter-intelligence) • Ministry of the interior (police, special forces) • Intelligence • Judiciary, prison service	NATO Interpol Europol Eurojust UN EU
	CYBER POWER • Hackers, freaks** • Organised crime (phishing), • State institutions	Data surveillance, data manipulation, sabotage	STATE Society Economy	Legislation Special software Training of experts Training	CYBER POWER • State security services • Ministry of infrastructure • Ministry of science • Ministry of education • IT firms	Interpol Europol EU
	PRIVATIZED POWER • Organized crime. (mafia, people smugglers, &) • Mercenaries, private military- & security firms • Militias (warlords) • Pirates	Illegal trade, corruption Sabotage, attacks, killings, capture, taking hostages , extortion	STATE Individual Economy	Surveillance, control, investigation, detention, custody, analysis, assessment Military operations Police measures Information policy	Ministry of the interior Ministry of defence Federal chancellery Media	Interpol Europol NATO EU
	PEOPLE'S POWER • Extremists (pol./rel./ethn.) • Insurgents, revolutionaries • Rebels, malcontents, impoverished, marginalised, socially disadvantaged persons,	Incitement, demonstrations, violent unrest, Uprising, revolution rebellion, riot Social media	STATE Society Individual	Education, insemination of values Legislation, control, surveillance, detention Social policy, integration	Ministry of the interior (Ministry of defence) Ministry of social affairs Ministry of education, NGOs, Civil society	OSCE EU Churches NGOs
	TERRORIST POWER • Terrorists • Terror organisations/ -groups (pol./rel./ethn.)	Attacks, killings Weapons of mass destruction NBC weapons Corruption	STATE Individual Society Economy	Observation, Military operations, Penal prosecution, Development Freezing of funds	Ministry of the interior Ministry of defence Judiciary Ministry of foreign affairs Financial market authority Ministry of health	NATO EU

Figure 3: Overview of actors

Michael Schurian, based on an idea of *Rastislav Báchora*.

* Putsch: [act of force, mostly by small groups, with the primary aim of deposing a government and taking over power.] translated from Wörterbuch Sicherheitspolitik mit Stichworten zur Bundeswehr, 4th completely revised edition; Hamburg, Berlin, Bonn; Mittler (2000).

SOFT POWER	REAL ECONOMIC POWER • Firms; conglomerates • States	Price setting, tightening of resources, cessation of supply, boycott,	COMMERCE (Energy market, …) STATE Society Individual	Legislation Supervision	Ministry of economics Ministry of agriculture National bank	IWF World Bank EU
	FINANCIAL POWER • Firms, conglomerates Financial services • Sovereign wealth funds**	Financial manipulation, speculation, corruption	COMMERCE (Financial market, energy market…) STATE Society Individual	Legislation Supervision	Ministry of finance (Federal financing agency) National bank Financial market authority	IWF World Bank EU
	DIPLOMATIC POWER • States • International organisations	Alliances resolution, threats, sanctions (punitive tariffs, tightening of resources, boycott, embargo	STATE SOCIETY	Bargaining, treaties, alliances, retorsion, Insemination of values Development cooperation	Ministry of the exterior	UN EU
	CIVIL POWER • International organisations • Non-governmental organisations (NGOs) • Law firms	Protests Demonstrations	STATE SOCIETY	Insemination of values Development cooperation	Ministry of the exterior	International organisations EU, OSCE
	SCIENTIFIC & TECHNOLOGICAL POWER • States • Conglomerates, businesses	Research into new technologies	STATE Society Commerce	Research into new technologies	Ministry of science Ministry of education Research institutes Research & development departments of conglomerates	EU Think tanks
	MEDIA POWER • States • NGOs • PR agencies • Global media concerns	Campaigns (information & disinformation) Manipulation Propaganda Mobilisation Hoax***, viral campaigns	STATE Individual Society	Reporting Education Critical research Insemination of values	Media companies Ministry of science Ministry of education Think tanks NGOs	Media concerns Think tanks NGOS

** Sovereign wealth fund: national funds in which governments invest capital for a variety of purposes (including strategic objectives).

*** Hoax: false information disseminated via email, social networks or other media.

(3) *What constitutes an actor's potential?*

An actor's potential arises from the sum of all of his capabilities, resources and social connections. A hybrid threat is presented through the deployment of this potential in a combined application of widely differing means and methods. To be included as means are firstly, but not exclusively, those of state power: the armed forces and intelligence services, in order to become active beyond state borders, and police forces and the judiciary, in order to proceed against citizens of the state targeted for hostility who are present on home territory. Given the global nature of information and communication networks, a cyber-attack should be rated as a potential offensive act.

Also projecting beyond borders is the aspect of the economy which, thanks to globalisation, has led to a greater diversity of products and increased mutual benefits, albeit accompanied by a greater level of dependency. Necessary to consider in this context is, for example, the security of supply of energy. Many states are dependent on imports of fossil fuels from politically unstable regions or the strategic purchase of scarce resources (e.g. "rare earths"). At regular intervals, conflicts over natural gas supply flare up between Russia and the Ukraine, forever leading to political tensions between the two countries.[83]

Speculation on domestic currency presents a possible way of influencing the economy of a state. There is a similar phenomenon with regard to genetically modified seed. For example, Greenpeace accuses the U.S. conglomerate Monsanto of promoting dependency through the latter's genetically modified and sterile seed. The problem is that, to date, farmers retained some of the harvested grain to sew again the next year. This is no longer possible with seeds from genetically modified crops grown the preceding year as they are no longer suitable for planting. Thus farmers are forced to buy more seed.[84] The possibility cannot be exclud-

[83] Cf. Mangott, Gerhard: Russia, Ukraine und die Gasversorgung der EU. 12/09/2014. <http://www.gerhard-mangott.at/?p=3598>, accessed on 08/12/2015.

[84] Greenpeace: Steriles Saatgut als Geldquelle. 21/02/2006. <http://www.green

ed that such practices are also utilised for the purpose of state power projection.

Regarding the potential capabilities and resources of an actor, the following twelve dimensions of force and power apply, consequently constituting a state's array of instruments of foreign policy:

Military power

This involves particularly the deployment of armies and special forces. Military power can be applied both "overtly" and "covertly". In future, covert operations in particular might be expected to gain yet more importance in connection with hybrid threats. In the Cold War this involved a phenomenon barely noticed by the public. It was said of the "Spetsnaz" forces (Russian special forces) that, in the event of potential conflict, they would have exerted covert military influence. But there are also comparable examples from more recent history in the west. For example, at the beginning of 2011 in its online edition, the British "Mirror" stated: "Hundreds of British SAS soldiers have been operating with rebel groups inside Libya for three weeks."[85] USA armed forces are known to have had similar intentions. Thus relevant U.S. literature refers to "covert operations", "black operations" or "clandestine operations". In the USA, a "clandestine operation" is defined as an

> "[...] operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities."[86]

peace.de/themen/landwirtschaft/gentechnik/steriles-saatgut-alsgeldquelle>, accessed on 08/12/2015.

[85] Crack SAS troops hunt Gaddafi weapons inside Libya. In: The Mirror, 20/03/2011. <http://www.mirror.co.uk/news/uk-news/crack-sas-troops-hunt-gaddafi-117405>, accessed on 08/12/2015.

[86] Department of Defense: Dictionary of Military and Associated Terms. Joint Publicati-

In the language of the Central Intelligence Agency (CIA), a “clandestine operation” is seen as a “[...] mission, with negative particulars, not attributable to the organization carrying it out”[87]

Judicial challenges arising in connection with the concepts of combatant and non-combatant will not be discussed further here however. Nevertheless it is worth pointing out that the “blurriness” currently evident when observing the armed forces in eastern Ukraine for example, could become an established method of influencing a country’s political processes in future.

Political and judicial power

Legislation and consequently the judicial apparatus could be employed so as to disadvantage another state, its economy and citizens (laws affecting rights, retrospective dispossession without recompense, detention etc.). The improper enforcement of laws on individuals or companies and potential exertion of political influence on laws in another state has led some writers to talk of “lawfare”, a blend of *law* and *warfare*.[88]

Power exerted by intelligence services

Alongside the collection of intelligence and information, intelligence services can be used for the manipulation of information, propaganda and sabotage. For example, referring to documents from Edward Snowden, the “Frankfurter Allgemeine” commented in June 2014: “[The British GCHQ

on 0102. 08/11/2010, p. 56. <http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf>, accessed on 08/12/2015.

[87] Smith, Thomas W.: Encyclopedia of the Central Intelligence Agency. New York 2001, p. 31. <http://books.google.at/books?id=1Jc9wBsImOIC&printsec=frontcover&dq=encyclopedia+of+the+central+intelligence+agency&hl=de&sa=X&ei=SXkyVIiUD6P9ywObuYDQAQ&ved=0CCAQ6AEwAA#v=snippet&q=%22black%20operation%22&f=false>, accessed on 06/10/2014.

[88] Cf.. <http://www.thelawfareproject.org/what-is-lawfare.html>, accessed on 08/12/2015.

[Government Communications Headquarters] intelligence service possesses a wide range of facilities for influencing online surveys and forging web content and email sender addresses.]"[89] As to whether western intelligence services actually employ such manipulative measures is a matter of speculation.

Cyber power

Cyber attacks can be deployed in a variety of forms, e.g. by means of viruses, identity theft (phishing), data interception and manipulation, suppression of web services, alteration of website content etc. Here once again attention is drawn to the example of the British intelligence service GCHQ's theoretical potential, using appropriate software, to influence Internet traffic, remove content from video websites etc. (see above).

Privatized power

Private military and security firms, paramilitary volunteer forces and militia, along with pirates and criminal organisations, do indeed pursue independent objectives, though they may seek a strategic partnership with the offensive actor to both sides' advantage. Whilst permanent instability and thus a weak state are more advantageous for organised crime (OC) and warlords when it comes to turning a profit, an aggressive neighbouring state could take advantage of instability caused by OC in order further to weaken the state under attack in line with the objectives of the aggressor.

People power

Belonging to this group are, in particular, armed insurgents, political or religious extremists, any mobilised mass of malcontents and marginalised

[89] Britischer Geheimdienst kann Internet manipulieren [British secret service can manipulate the Internet]. In: Frankfurter Allgemeine Zeitung, 14/07/2014. <http://www.faz.net/aktuell/politik/weitere-snowdenenthuellungen-britischer-geheimdienst-kann-internet-manipulieren-13046387.html>, accessed on 08/12/2015. Translation from the German original quotation.

minorities, who act almost as a "fifth column" to realise the interests of an offensive actor. Successful exploitation of this People power by an actor in another country can serve as an important tool for inciting the population. Thus, for example, a private company, organised in such a way as to imitate the Belgrade-based "Canvas" organisation, could offer courses and training on "strategic nonviolent conflicts"[90]. Reliance on a similar set of objectives as those of "Canvas" is plausible:

> "[...] rather to spread the word of "people power" to the world than to achieve victories against one dictator or another. Our next big mission should obviously be to explain to the world what a powerful tool nonviolent struggle is when it comes to achieving freedom, democracy and human rights."[91]

A German daily paper described one of the heads of Canvas, the Serbian Srña Popovič, as someone who pursued "revolution as business"[92]. If these objectives at Canvas are perhaps noble, then the possibility cannot be excluded that similar companies might pursue less altruistic objectives in order to facilitate them as a method of hybrid threat in the form of "covert operations".

Terrorist power

Terror attacks or spectacular acts of sabotage, which give rise to a large number of civilian victims having deliberately targeted them, are aimed at minimising society's resolve to resist. Here a state can passively support terrorist organisations in that it does not actually actively encourage terrorist activities but also does not prevent them – or actively support them.

[90] CANVAS: Who we are. <http://canvasopedia.org/about-us/>, accessed on 28/11/2015.

[91] Ibid.

[92] Scheffer, Ulrike: Der Serbe Srdja Popovic betreibt Revolution als Business. In: Tagesspiegel, 14/03/2011. <http://www.tagesspiegel.de/politik/widerstandsguru-derserbe-srdja-popovic-betreibt-revolution-als-business/3946482.html>, accessed on 08/12/2015.

Diplomatic power

A state actor can make use of diplomatic resources by, for example, unsettling existing alliances and increasingly isolating the target state from the international community. The EU approach in the case of Switzerland has already been mentioned. Even though comprehensible motives feature in the foreground here, similar procedures are plausible in the case of hybrid threats from states.

Real economic power

Interruption of supply of raw materials and fuels (gas), the purchase of strategic resources, land grabbing, control over transportation routes can all be seen as forms of real economic power projection. But an influence on society is also significantly facilitated by the area of e-commerce in particular. Financial transaction systems, wholesalers and the associated stock of customer data possess a previously unimaginable power projection potential for weakening a state's commercial position. Examples include online concerns like Amazon or the Chinese counterpart Alibaba. The latter has now grown larger than Amazon and eBay combined and operates at a remarkable level of profit.[93]

Financial power

Trade barriers, influencing exchange rates, inducing targeted indebtedness of other countries and the strategic application of sovereign wealth funds, are examples of means of application of economic influence on adversaries. Media reports from April 2013 reveal preceding attempts at electronically controlled, brief influence on financial markets. The U.S. news agency Associated Press (AP) reported the dissemination of false information via Twitter asserting that the U.S. President had been wounded in an explosion at the White House. More than 1.9 million people are said to have followed the AP reports on Twitter.

[93] Alibaba: After the Float. In: The Economist, 06/09/2014, p. 60.

The result was that, as a result of this news, the US S&P 500 stock exchange index fell by 0.8 percent in three minutes, implying a loss in value of 136.5 million US dollars.[94] Whilst the effects did indeed only last a short time (the exchange recovered quickly), nevertheless it became apparent what could be achieved in the financial sector with the aid of social media. Here some kind of criminal background can represent but one motive. Scenarios of strategic power politics are equally plausible. Thus additional, similarly refined methods in the area of financial speculation, aimed at damaging, destabilising or rendering a state compliant, are not improbable.

Scientific and technological power

Even though a "brain drain" may not be deliberately harnessed for the purpose of applying a hybrid threat, the former has taken place for decades. This involves academics with a bright future in research and development being recruited from abroad, often described in the media as a "brain drain". The migration of these experts confers twin advantages on the state responsible for their move. On the one hand, assuming it is deliberate, a state loses its (future) elite whilst, on the other, the initiator creates a technological advantage for itself too, given that the migrant experts generate knowledge for their "new" state. Furthermore, this would give rise to additional economic disadvantages for the states that lose "emigrated" patents.

The area of scientific power has another aspect: it is often only finance from abroad that enables the initiation of research projects. An example would be U.S.-financed research projects in Austria. Tim Lawrence[95] gave information about U.S. research investments in an interview in an

[94] [FBI investigates regarding tweet about explosion in the White House. In: Die Presse Online, 24/04/2013. <http://diepresse.com/home/politik/aussenpolitik/1393224/FBI-ermittelt-wegen-Tweet-uber-Explosion-im-Weissen-Haus> accessed on 08/12/2015.

[95] Tim Lawrence is commander of the Air Force Research Laboratory and heads the European Office of Aerospace Research & Development (EOARD) located there.

Austrian daily paper. According to this, in 2013 the USA cooperated on a variety of research projects with 30 countries worldwide.[96]

Since the article in the "Wiener Zeitung", over the last five years Austrian projects financed by the U.S. military have grown to almost nine million euros.[97] If a similar actor were to make such investments for the purpose of hybrid threats, the theoretical possibility might arise of those research subsidies being terminated, thereby substantially disrupting the success of the research projects. An additional benefit arising from financing research results is the possibility of examining the research findings of other states.

Worthy of mention in this context is the theoretical influence exerted by the pharmaceuticals industry on the public health service. It would be possible to exercise some control over opinion formers and healthcare institutions via networks active worldwide. Small states, particularly those in poorer regions of the world having urgent need of medicines, are often dependent to a large extent on the pharma industry of other states.[98] A tailored interpretation of health statistics or the effectiveness of medicines, combined with a desire for greater profit margins, could be harnessed both by conglomerates and by states, assuming the intention is there, to create panic. The population's demand for healthcare on the one hand, combined with the pharma industry's self interest on the other, could in certain circumstances provide additional fertile ground for the social destabilisation of a state.[99]

Media power

Liberal democracies with pluralistic societies thrive on the free exchange of ideas. Aiding this, media fulfil the function of reporting and contribute to opinion formation. Influencing and controlling the multi-medial "configu-

[96] Figl, Bettina: Mehr als Brustkrebsforschung [more than breast cancer research]. In: Wiener Zeitung, 31/07/2014, p. 7.

[97] Ibid, p. 7.

[98] Observations by Amin/Brica/Feuchter, participants in the GALG, 15-19/09/2014.

[99] Observations by Margreiter/Jancuska, participants in the GALG, 15-19/09/2014.

ration" of society is a central factor of power with which, well away from any force of arms, influence can be exerted on states and societies. The deployment of media power is directed towards public and published opinion, whether in the cyber domain, in social networks or by means of mass-media coverage in the form of words, sound, still or moving images (in music and lifestyle as well). Thus actors often make use of media, as for example currently in the case of the Islamist terror organisation "Islamic State".

The significance of conflicts is not based exclusively on real events but also on their symbolic construction, interpretation, collective perception and contextualisation within the dynamics of differing models through which to explain the world. What is perceived becomes the truth. Here media form the bridge between reality on the one hand and collectives/individuals on the other.

A completely different form of exercising power in the media domain is demonstrated by the interruption of a state's main channels of communication, similar to the case in Syria. In mid-2012, "Spiegel Online" reported that "[Arab satellites had stifled transmissions from the regime-aligned broadcaster Addounia]"[100].

An additional aspect within the spectrum of media power reveals its presence in the possibility to control announcements of information. Again "Spiegel Online" reported in 2012 that, according to a report by the Syrian ministry of information, western secret services were "[… hacking the state TV channel and replacing the official programme with false reports]."[101]

Environment

The environmental factor is gaining increased importance in security policy analyses. Rising global levels of environmental pollution and climate change

[100] Salloum, Ranniah: Offensive an der Twitter-Front. In: Spiegel Online, 24/07/2012. <http://www.spiegel.de/politik/ausland/buergerkrieg-in-syrien-offensive-an-dertwitter-front-a-845895-druck.html>, accessed on 08/12/2015. Translation from the German original quotation.

[101] Ibid; Translation from the German original quotation.

exert a direct influence on living conditions and resource availability. Exercising power by intervention or non-intervention in a nation's environmental interests, for example in the form of demands for environmental legislation or revision of the coverage of energy demand (e.g. demands for the closure of oil, coal or nuclear power stations etc.), can lead to societal effects.

Complexity

All of the capabilities and resources mentioned above, once assembled into a single illustration, yield the following Figure:

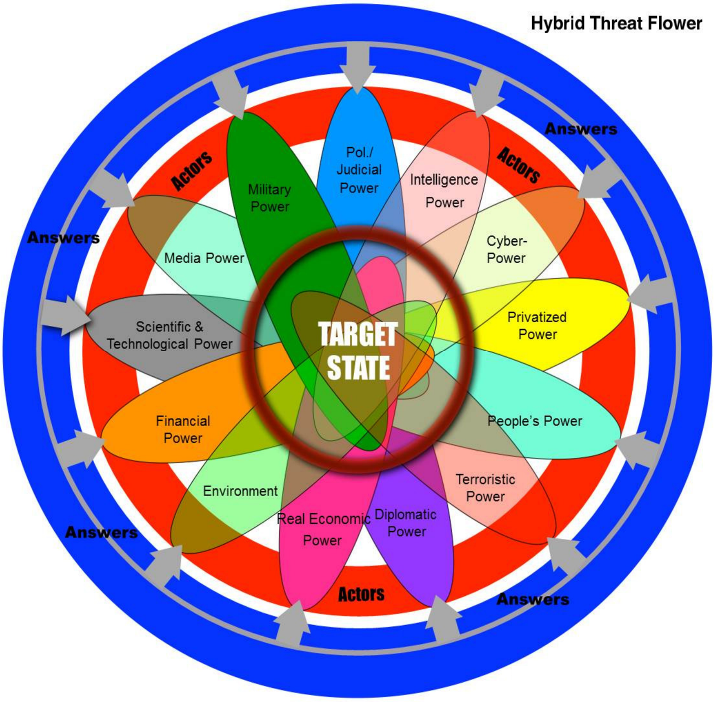


Figure 4: Spectra of potential threats
Anton Dengg, Michael Schurian

In Figure 4 the offensive actor, who initiates the hybrid threat, is represented by the red, outer ring. The defensive actor or target state is represented by the inner, small, red ring. These two rings are linked by twelve variously coloured ellipses. The latter symbolise the respective capabilities, dimensions for action and externally effective instruments of the actors. The offensive actor can select from this spectrum whichever means in whichever combination will achieve the most severe effect on the target state. From the combination of highly diverse activities against the adversary's various weak points, synergy effects can accrue, which encompass both the physical and psychological dimensions of the conflict. Aspects worthy of particular note in Figure 4 are the overlapping, coloured segments. These show that every segment, when coordinated with at least one other element, can/must prevail for a hybrid threat to arise. It is necessary to emphasise that Figure 4 illustrates only some possibilities of hybrid threats and can be extended practically without limit.[102] The blue ring represents the hybrid defensive response in the form of an all-encompassing, national security approach.

Figure 5 illustrates the complexity of the effects of varius exercises of violence and power against a state.

[102] This will be the subject of future research.

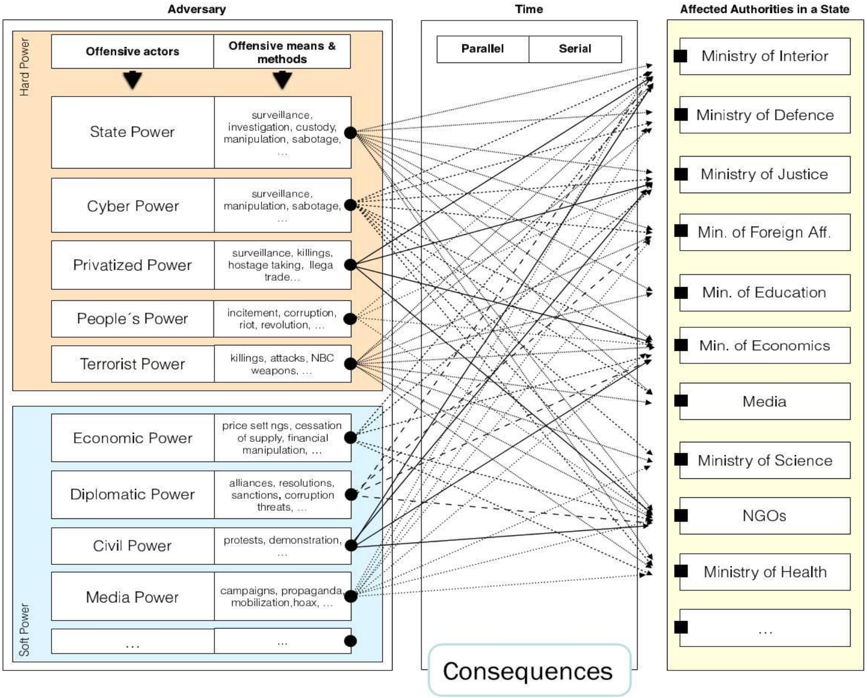

Adversary
Time
Affected Authorities in a State
Hard Power
Offensive actors
Offensive means & methods
Parallel
Serial
State Power
surveillance, investigation, custody, manipulation, sabotage, …
Cyber Power
surveillance, manipulation, sabotage, …
Privatized Power
surveillance, killings, hostage taking, llega trade…
People´s Power
incitement, corruption, riot, revolution, …
Terrorist Power
killings, attacks, NBC weapons, …
Economic Power
price sett ngs, cessation of supply, financial manipulation, …
Diplomatic Power
alliances, resolutions, sanctions, corruption threats, …
Civil Power
protests, demonstration, …
Media Power
campaigns, propaganda, mobilization,hoax, …
…
…
Soft Power
Consequences
Ministry of Interior
Ministry of Defence
Ministry of Justice
Min. of Foreign Aff.
Min. of Education
Min. of Economics
Media
Ministry of Science
NGOs
Ministry of Health
…

Figure 5: Complexity of the effects of varius exercises
Anton Dengg, Michael

(4) How can a hybrid threat be deployed?

A hybrid threat is a combined, coordinated, concerted, systematic coaction of several activities against and to the disadvantage of a state. Several actions (at least two) affect the target state. This not only increases the effectiveness but also hampers defence. The actions may involve coercion, pressure and force or equally use the means of propaganda or embargos.

Because a hybrid threat works on several levels, one can speak of a multidimensional process. Dimensions that have a particularly strong influence are those of politics and of the law, the military, the economy, ecology, society and culture, technology, science and the media.

The manner in which a hybrid process can actually unfold depends on the condition of the target state. An industrialised nation is more dependent on energy, resources and a functioning economy. In contrast, a threshold state with weak national institutions and internal asymmetries of power is more susceptible to corruption and uprisings. Cyber-attacks on a country that has IT infrastructure with scarcely nationwide coverage hold little promise of success. Yet in a highly technological country, such an attack can have fatal consequences on (financial) business and public order.

Here the threat potential can be applied either directly or indirectly. Direct attacks can be launched by domestic units, whilst indirect ones may be handled by proxies. The misuse of a foreign policy instrument should be seen as an indirect attack.

By way of example, the primary function of business is not to threaten but rather to serve the provision of people’s material needs, production of goods and delivery of services as well as the allocation of resources.[103]

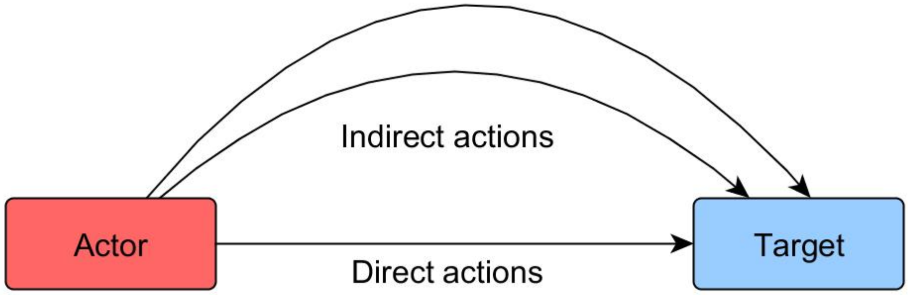


Figure 6: Direct and indirect actions against a target
Michael Schurian

[103] Business competition *per se* does not constitute a security threat, but it can be used to that end.

If one evaluates the deployment of state power as a direct action against a target whilst also seeing an indirect action through economic or media-related measures for example, the result is given schematically in the following Figure (Figure 7), which summarises an actor's potential via direct and indirect routes:

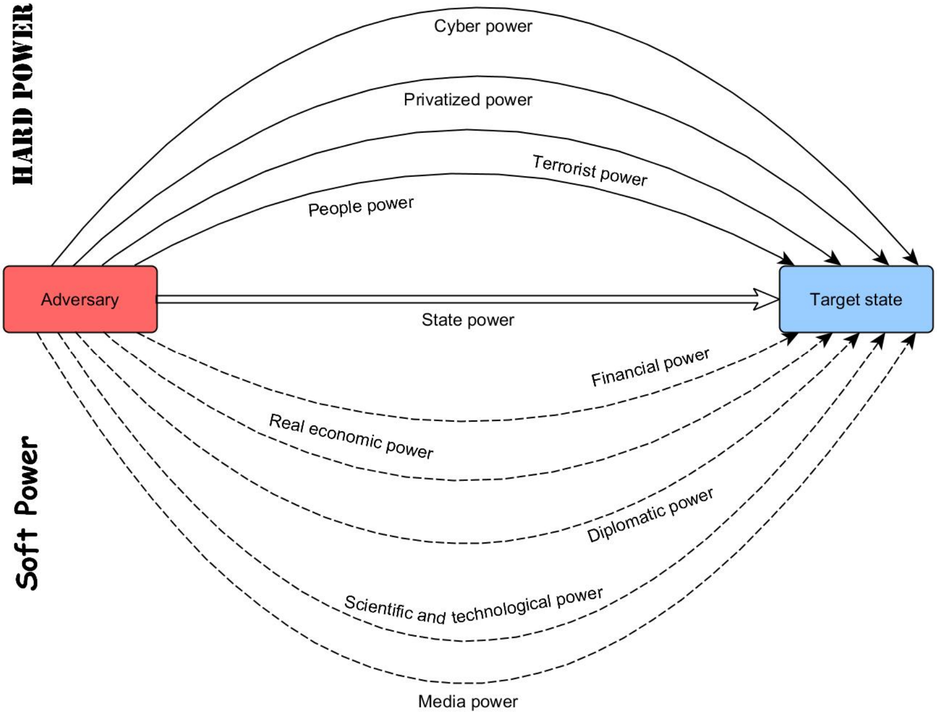


Figure 7: Direct and indirect actor potential.
Michael Schurian

(5) The targeted application of potential threat

The threat activities must be appropriate for the purpose of limiting the target state's freedom to make decisions and directing its behaviour to the advantage of the actor of the threats. Taken in isolation, the individual operations might appear to have no (or merely an arbitrary) relationship, given that there are no intersection points immediately apparent. Thus, for example, a naval exercise taking place off the coast of a country might seem, at first sight, to have nothing to do with demonstrations in the government district of the capital city. Only more precise analysis could reveal the two events as being power projection of a single actor.

(6) Multidimensionality

The multi-dimensional deployment of capabilities and resources for the purpose of conducting conflict forms the core element of hybrid threat. Alongside direct attacks on the adversary's armed forces, the strategy of hybrid threat also targets the economic, infrastructural, social and other prerequisites of the target state and its allies. In such a multi-dimensional process of conducting conflict (see also section (5) on targeted application) the question arises as to the accuracy of hybrid threats. Theoretically the assumption would be that not all effects would be foreseeable and that the pattern of reactions of the target state under attack would be difficult to predict. The aggressor is confronted with counterintuitive consequences. Unintended effects on collateral persons or property (e.g. civilians, allies, domestic export business, etc.) are capable of injecting unforeseen impetus to the dynamics of conflict. Such sources of impetus – even if they are unforeseen and surprising – can be used in turn with other spectra of hybrid threat for further attacks, assuming sufficient flexibility of the actor.

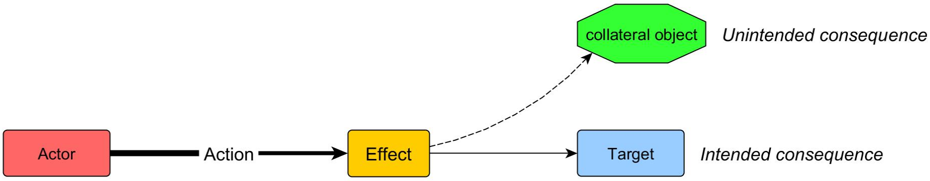


Figure 8: Intended and unintended consequences
Michael Schurian

As well as unintended consequences, a set of effects can arise, which were neither predictable nor estimable *ex ante*. A terrorist attack is aimed directly at civilians and indirectly at their state. But an attack also has effects on the economy (loss of tourism, loss of profit and thus reduced tax revenue, insecurity on financial exchanges), on the legal system (demands for stricter security legislation, acceptance of restrictions on individual freedom) and on public sentiment (identification with perpetrators) etc. These additional reactions have lateral effects on the conflict – they can intensify the effects or project them into other areas of life. Thus a terrorist attack can trigger hybrid effects which, in turn, require hybrid counter-reactions.

If the effects are amplified, one can term this a multiplier effect. Consistent with fulfilment of its original task of reporting, coverage in the media amplifies perpetrators' presence in the media. This can lead to commercial losses and thus to reduced tax revenue for example, in turn having reduced state spending as a consequence. Sanctions against supplier businesses (uranium mining, transportation and nuclear waste disposal) can bring pressure to bear on other sectors (power-generation). For this reason, the media and journalism have the enormous significance. Consequently, responsible journalistic research directed towards objective reporting can be regarded as an important strategy against hybrid threats.

There is justifiable fear that such multiplications of the initial attack trigger a certain level of automatic reaction which, through chain reactions, can ignite a widespread conflagration. As a result of the interdependence between affected systems (politics-economy-social-ecology-military), one may expect non-linear consequences, which exceed the direction and magnitude of thrust of the initial hybrid attack.

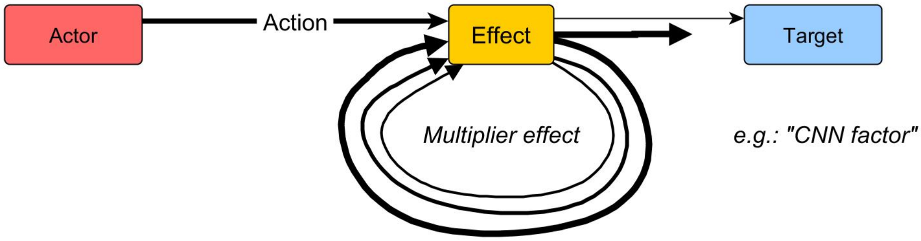


Figure 9: Multiplier effect
Michael Schurian

Whilst it is possible for multiplier effects against the target state to arise as a consequence of the connectivity between interdependent systems, a contrary effect is also possible. The consequences of a hybrid attack could equally hit the actor himself (feedback effect) and have the effect of an "own goal". Such feedback effects against the initiator are not surprising, because both the actor and the target are linked.

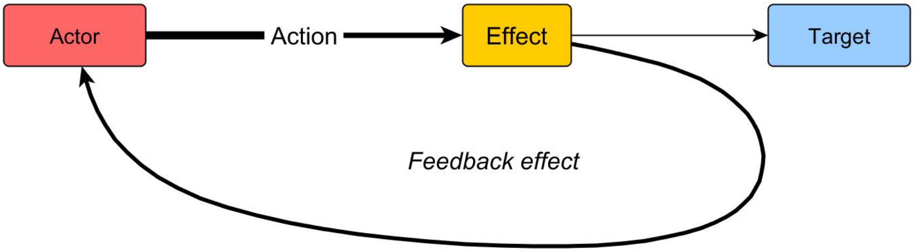
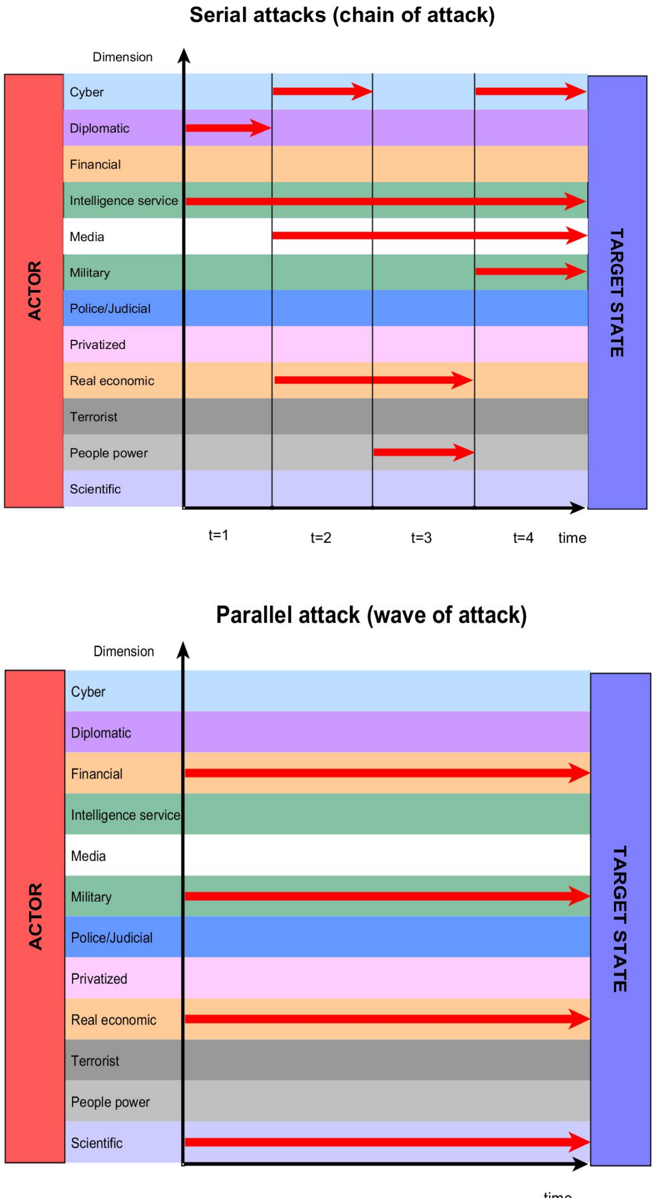


Figure 10: Feeback effect
Michael Schurian

A hybrid threat's success also depends on whether an actor takes account of all possible feedback effects in his plans, can prepare himself and consequently hold his position. Uncertainties over the scale, line of attack or timing of such effects is decisive for the development of effective resilience concepts.

(7) Coordination of timing

In terms of coordinating timing, both parallel and serial waves of attack are plausible. *Parallel attacks* are multiple, simultaneous operations. They are applied against an adversary through a brief, amassed process*. Serial attacks* are a chain of operations applied at staggered points in time. They are appropriate for use as instruments of attrition in order, for example, to achieve success in negotiations during breaks in hostilities, to evaluate one's strategy and possibly adapt it. A series of attacks, each on a scale below the threshold of perception, also helps the aggressor to remain concealed.


Serial attacks (chain of attack)

Parallel attack (wave of attack)

Figure 11: Waves and chains of hybrid attack
Michael Schurian

In the light of the force-space-time calculation, this means: hybrid waves of attack bring a variety of forces to bear simultaneously in a variety of spaces. Hybrid chains of attack distribute various kinds of force on several levels over different intervals of time. Because of the massive possibilities of parallel hybrid approaches, the latter represent a worst-case-scenario. An actor's ultimate choice between parallel or serial attacks is highly likely to depend on the size and capabilities of the target state.

1.2.13 Summary

Hybrid threats are fundamentally nothing new. But, as a result of global networking processes and new media-related possibilities, particularly social networks in cyberspace, they are acquiring new dynamics and significance. The growing complexity of our infrastructure, which has now permeated throughout our society's systems, is becoming ever more vulnerable because of its increasing reliance on technology. Worthy of emphasis is the enormous increase in dependency on technical products which, in turn, creates new potential forms of state power (as well as for non-state actors). Particular challenges result in cyberspace, because there is scarcely any guarantee of identifying the aggressor. This means that it is often impossible to spot who the "originator" of attacks is, or even the actual "wielder of power". If the supposed originator is spotted, the challenge then arises of substantiating accusations of the commitment of offence and proving that the suspect party is the "perpetrator". The country from which a cyber attack originates is not necessarily also the originator of the attack. Any weaknesses present in the cyberspace within a state could have been exploited by aggressors.

A multi-dimensional approach aids the concealment of objectives. In this case, the aggressor does not have to be placed in the situation of presenting himself in public as the originator of such power projection; what counts is achieving the objective and purpose of his activity[104]. What is important to understanding the strategy of a hybrid threat is that an actor coordinates his

[104] The example of events surrounding the *Stuxnet* virus makes this clear.

measures in a targeted, multi-dimensional and chronologically defined relationship and acts as a kind of “mastermind”.

An aggressor can threaten a target state in either a serial or parallel modality in a multiple (hybrid) manner. The desired effect does not always work as planned on the target state under attack. Such unintended consequences can deliver unanticipated impetus to the dynamics of conflict, in turn requiring great flexibility on the part of the aggressor. Decisive in the context of state security is the exceeding of a strategic threshold in the target state.

Taking advantage of natural disasters along with subsequent application of additional hybrid power projection can lead to greater destabilisation of the structure of a state to the advantage of the aggressor. Such capability to react depends critically on the aggressor’s flexibility, preparedness and capability to project his power.

Current examples (such as the Ukraine crisis from 2014 at the latest) illustrate the challenge of hybrid threats (either from state or non-state actors) to western society. Here both legal and moral aspects have a great role. Examples show that states are already making use of hybrid methods to exercise power. It is therefore necessary to generate countermeasures.

It is important not to evaluate hybrid threats as conflict scenarios viewed in isolation. There is no such thing as *the* hybrid threat, because it consists of diverging variations of alternating combinations and therefore generates effects and lines of attack in alternation. Consequently methods of resolution, mechanisms of protection and of defence must also be developed with a corresponding level of diversity.

The important challenge for states lies in their recognising hybrid power projections directed against them across their entire bandwidth and initiating appropriate, concerted countermeasures.

1.3 Hybrid Threat Potential in the Light of Networking and Systemic Thinking

Herbert Saurugg

Since the end of the Cold War 25 years ago, threats and scenarios we perceive have changed considerably. From a relatively straightforward bipolar world, we have moved to highly complex, very dynamic and increasingly turbulent times today. Experts call this VUCA - volatility, uncertainty, complexity and ambiguity. These developments concern basically all realms of life. At the same time our well-tried paradigms have hardly changed at all. But will that suffice to be able to deal with the new challenges we are facing?

One essential driver for change was the exponentially increasing proliferation of information technology (IT, computers, IT solutions, and, most of all technological networking, especially the Internet), basic technologies of the 5th Kondratiev wave. They describe economic developments in a period of approximately 40-60 years, in which one of each basic technology/innovation[105] determines the developments. According to this we are currently in the fading 5th and beginning 6th wave and, as such, in a phase of change.

1.3.1 Network society

Since the 1950s network society has started to develop in parallel. First rather slowly, and then with the broad permeation of information technology throughout society, from the beginning of the 21st century, it picked up speed considerably.

[105] 1. Steam engine, early mechanisation, industrialisation → power; 2. Railway → transport; 3. Electrical engineering and heavy machines; chemistry → processing; 4. Integrated circuit, nuclear energy, transistor, automobile → automation; 5. Information and communication technology → integration, globalisation; 6. Probably psycho-social health, biotechnology, education

Whilst industrial society is characterised by standardisation, synchronisation, centralisation (hierarchic structures) and by concentration (mass armies, mass media, mass production, work in factories), the network society now establishing itself is marked by diametrical characteristics.[106] We witness tendencies toward individualisation (products, lifestyle), auto-coordination (via/through the Internet, *ad hoc* networking), decentralisation (energy supply, and nation states seem to lose their importance) and toward dynamic networking rather than concentration, which again questions hierarchic structures. Network society establishes itself as the third western form of society in addition to agricultural and industrial society, independent of corresponding religious or economic convictions.

The transformation process from agricultural to industrial society, between approximately 1650 and 1750, has not been a smooth one, having overthrown the one or other world view effective until then. Also today we see similar turbulences. Agricultural and industrial society are not completely ousted but rather this is a parallel development, creating additional challenges. Thus, conflicts are frequently caused by differing values and mentalities and not by reasons often given as an excuse such as seeming religious conflicts.

It is also remarkable that potential solutions and mentalities in the network society are much closer to agricultural society than to industrial society, which is to be put down to the prevailing use of energy. Industrial society was coined by the fossil fuel age, which will probably continue to have long-ranging consequences, such as looming climate change for instance. Furthermore it is to be expected that network society solutions, such as decentralised energy supply systems or production methods, could contribute to a positive further development in agricultural society, for instance in remote areas. In this way, important security policy objectives such as stabilisation on site could be fostered and achieved more easily.

[106] Cf. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0 [network society and crisis management 2.0]. Master's thesis, University of Management Budapest 2013.

If a life with dignity is possible locally, migration pressure and conflict potential decrease. Inequality and resource bottle necks, which were caused by industrial society, can be reduced again. The end of the still prevailing paradigm of growth is on the horizon. In a world of limited resources it is not sustainable and has a self-destructive effect. The essential question here is whether we could still successfully turn away without any "Schumpeter's gale"[107].

From this perspective quite a few contradictions and current developments shine in a different light, such as the dissolution of artificially-formed nation states in the Arabic region or that decentralised energy supply leads to a massive power shift, which will probably not be easily accepted by established, concentrated/centralised rulers. Of course, the simple cause and effect model represented here does not include numerous aspects that are still important. More on this below.

There are various different models that derive or describe cyclical developments from the past. They all have in common that they are forecasting a major phase of change for this decade.[108] The signs for greater change are already more than evident, whereas the actual effectiveness can only be evaluated retrospectively.

In order to be able to fathom the topic of hybrid threats in the light of these developments, it is necessary though, to have a look at some basic concepts. Systems seem to play central role here.

[107] German term "Schöpferischen Zerstörung" [creative destruction] coined by Austrian economist Joseph Alois Schumpeter (*1883, †1950) for the process of continuous renewal and improvement of production procedures and products triggered by competition. Schumpeter perceives the process of creative destruction, in which old goods and production techniques are continuously replaced by new ones, as the motor of economic development. Creative and imaginative entrepreneurs play a central role in this. They would be continuously driving progress by means of new ideas and the use of new methods, techniques and ways of processing. Source: Duden Wirtschaft von A bis Z: Grundlagenwissen für Schule und Studium, Beruf und Alltag. Mannheim 2013.

[108] Cf. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. [network society and crisis management 2.0.] Master's thesis, University of Management Budapest 2013.

1.3.2 Systems

A system describes the functional composition of various different system elements to form a whole. Here the relationships between the system elements are decisive, “causal network”. Because without relationships there is no system, just an accumulation or a cluster.[109] What is decisive is that a system is more than the sum of individual elements. What might not seem particularly spectacular is, however, quite complex. There are innumerable examples of cases in which this simple truth was not considered sufficiently, which led to far-reaching negative consequences. Be it with regard to environmental matters (flood control, environmental pollution), in development cooperation (well-construction) or the 2007/2008 financial crash with numerous consequential crises, in all cases this seemingly simple statement was not considered sufficiently.

Even if we know all chemical elements of the human body and have them available, we still don’t make another human. An orchestra is much more than the sum of perfect individual musicians. The “invisible connective threads” between the individual elements always play a role and only they make for the added value.

What actually constitutes a system depends on the corresponding viewpoint and detailing, whether one is observing a molecule, cell, organ, human or his social system.

Thus, a system can present content-related, temporal and/or social boundaries towards its environment, which might be influenced by system effects but has no influence on the causal network.[110] Therefore a system must not be perceived as something absolute.

[109] Cf. Ossimitz, Günther/Lapp, Christian: Systeme. Denken und Handeln. Das MetanoiaPrinzip. Eine Einführung in systemisches Denken und Handeln [systems, thinking and acting, the metanoia principle, an introduction to systemic thinking and acting]. Berlin 2006.

[110] Cf. Krizanits, Joana: Einführung in die Methoden der systemischen Organisationsberatung [introduction to methods of systemic organisational consulting] Heidelberg 2013.

Basically we differentiate between simple and complex systems. Simple systems (machines) don't represent a major problem with regard to their regulation, steering or control. Here we can look back to a success story. However, complex technical systems are a relatively recent phenomenon, with which we first have to learn to deal.[111] However, at the same time, we are constantly surrounded by complex systems, given that nature consists solely of open, dynamic and therefore complex systems. This means that we can learn a lot from system design in nature.

1.3.3 Complex systems

Complexity is a frequently used term, without being defined clearly. Usually we would intuitively think of unclear, complicated, complex or inexplicable situations or phenomena. Our world has become complex, everything "turns" faster. Frequently the "hamster wheel" is used as a metaphor; everything must happen or grow faster, albeit without reaching a goal. Only very rarely are we aware of the entire context.

Complex systems consist of a large number of elements connected with one another and which, however, also interact with their environment, continuously causing feedback. So there are technical systems (machines) with a large number of elements. However, these only function in a determinate environment and they can be subdivided into their individual parts and be put back together again. These then are complicated systems, like mechanical clockworks or printing machines. Thus they are described as dead systems.

But complex systems cannot simply be taken apart, analysed and then reassembled. Therefore we call them living systems and so networking in a non-determinable environment leads to complex systems that exhibit system behaviour differing completely from our simple or complicated systems (machines) to date.

[111] Cf. Malik, Fredmund: Komplexität – was ist das? Modewort or mehr? Kybernetisches Führungswissen. Control of High Variety Systems. <http://www.kybernetik.ch/dwn/Komplexitaet.pdf>, accessed on 10/12/2015.

In complex systems there is a constant feedback, creating intrinsic dynamics. Simple cause and effect correlations are lost, controllability (management) is weakened or becomes impossible. Long chains of cause and effect are created. Interventions have a delayed effect and are irreversible, leading to a risk of 'over-drive'. Small causes can have major effects and *vice versa*. A lot of work and next to no result. There are indirect effects that are not really calculable, and thus are not registered with our established risk assessment methods. The absence of a range limit enables domino and cascade effects that are all the more devastating the larger the networked system. The solution of one problem creates new problems (actionism). This leads to exponential developments and to increased dynamics with which we have difficulty dealing, like compound interest.[112]

This might sound theoretical but, on closer inspection, we again find numerous examples from everyday life. Be it helplessness in the face of numerous problems (educational, health, pensions systems), the delayed negative effects of the Internet with increasing challenges from cyberspace (cyber attacks, security weaknesses), a terror attack leading to two wars (9/11), repeatedly practiced *ad hoc* legislation or the irresoluble developments in our financial system; in all cases underestimated complexity and non-controllability play a role. Apart from the fact that all wars have been underestimated in terms of dynamics and effectiveness.

1.3.4 Emergence

In addition, with the degree of networking, emergence in a system is increased. Emergence means the spontaneous creation of new characteristics or structures as a consequence of the interplay of elements in a system. Here element characteristics do not allow for conclusions regarding the emergent characteristics of the system, which again leads to spontaneous self-organisation and to unpredictability of developments.

[112] In an assumed interest yield of 5% (compounded interest included) the sum invested/debts are doubled after about 14 years. After 28 years they are multiplied by four and, after 42 years, multiplied by eight. This process is called exponential growth and does concern borrowers in particular.

If this aspect is taken into consideration regarding current developments, they do indeed appear in a new light. It becomes more comprehensible that an organisation such as the Islamic State (IS) could appear from nowhere and become infamous. As a result of today's possibilities for networking through technology, it is possible for spontaneous and far-reaching self-organisation to arise. In this negative case this led to a reign of terror over a very large region within a very short time. However, it should not be assumed that this will be sustainable, because growth took place too explosively. Nevertheless it caused a great amount of damage and human suffering. The whole thing was amplified by today's propaganda possibilities, which we provide via the Internet. The blame here lies less with the delivery media and far more with the way we allow ourselves to be manipulated by them.

Unpredictability could also now lead to countermeasures against Islamic State becoming more violent, something already in the offing, which is not the intention of these groupings. But here too, the consequential effects cannot be estimated. Increasing concern about possible attacks in other countries is therefore more than justified.[113] An important problem here is that many reactions can be attributed to actionism and the treatment of symptoms.

1.3.5 Symptom treatment

A crucial change in the consideration of threats was prompted by the terrorist attacks on September 11th 2001 (9/11). Ever since, no debate about security could omit the issue of "international terrorism".

Particularly great efforts were made towards increasing aviation security which, *de facto*, comes up to preparations for the "last war", the last event that presumably will not occur in this form anymore, though not trying to generally call all the measures taken into question. Systematically reflecting,

[113] Cf. Sadowski, David/Becker, Jeff: Beyond the "Hybrid" Threat. Asserting the Essential Unity of Warfare. In: Small Wars Journal, 2010. <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-etal.pdf>, accessed on 10/12/2015.

one can promptly encounter a lot of aimless actionism. Whether regarding the "War on Terror" in general or the wars in Iraq and Afghanistan in particular, but also regarding the now widely installed, technical security solutions in aviation security, success has been limited or, more specifically, it was nearly always only the symptoms that were treated. Most measures did not lead to a substantial improvement of the overall security situation, but rather brought further destabilisation or the increase of pseudo-security and also led to unintended side effects like restriction of privacy or by putting a huge number of innocent people under general suspicion, due to escalating surveillance. Quite apart from that, these systems present a high potential for abuse

1.3.6 Terrorism

To be able to understand and face terrorism, it is first necessary to know how it works. In a nutshell, terrorism takes effect twice. Firstly through an attack's immediate impacts. Secondly through the victim's resulting reactions.[114] It is known from several studies that the secondary damage is substantially greater than that caused by the immediate incident.

It is currently assumed that the consequential costs of 9/11 extend to trillions of U.S. Dollars.[115] Hence it is not the immediate incident but rather our response to it that leads to substantially greater damage, and not only in financial terms. A large number of innocent people lost their lives as a consequence of the "War on Terror". Besides the vast number of soldiers[116],

[114] Cf. Vester, Frederic. Die Kunst vernetzt zu denken. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ein Bericht an den Club of Rome. [the art of interconnected thinking - tools and concepts for a new approach to tackling complexity - report to the Club of Rome.) Munich 2011.

[115] Cf. Anti-Terror-Kampf kostet USA eine Billion Dollar. [anti-terrorist war costs the USA one trillion dollars] In: Die Welt, 14/05/2011. <http://www.welt.de/politik/ausland/article13371713/Anti-Terror-Kampf-kostet-USA-eine-Billion-Dollar.html>, accessed on 22/12/2015.

[116] According to <http://de.statista.com/statistik/daten/studie/2006/umfrage/gefallene-oder-verunglueckte-soldaten-der-westlichen-koalition-in-afghanistan/> 3250 soldiers of western armies are said to have lost their lives in Afghanistan and, according to

an even larger number of civilians – directly but also indirectly. Has our world therefore become a safer place?

In recent years there was one positive example with no immediate overreaction. This was the case after the attacks on London's public transport system in 2005, as this possibility was taken into account and preparations had been made.[117]

An increasing problem is presented through the altered objectives of terrorist groups. In the 20th century, terrorism still tried primarily to accomplish political objectives, which is why it had to make allowance for an adversarial population. That has changed with 9/11. Fundamentalist, predominantly Islamic groups do not pursue this secular objective anymore, which is why certain inhibition levels disappeared. Hence, we have to expect greater damage through terrorism in future. At the same time, this is an important indicator for us not to focus too much on potential actors but rather on our vulnerabilities.

1.3.7 Reasons for terrorism

Contemporary "combating of terrorism" is mainly only the combating of symptoms. There is rarely an attempt to get to the bottom of the potential reasons and address them. The German risk researcher Ortwin Renn regards the growing discontent with unjust wealth and power relations in particular as a cause leading to social discontent and even to aggressive actions, such as social upheaval, fanaticism and terrorism.[118] To really contribute to a safe future, this has to be addressed. Unfortunately there are no simple technical solutions showing great promise in this regard.

<http://icasualties.org/Iraq/Fatalities.aspx> 4800 in Iraq.

[117] Saurugg, Herbert: Blackout. Eine nationale Herausforderung bereits vor der Krise [blackout - a national challenge before the crisis]. Seminar paper, University of Vienna 2012.

[118] Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten [the risk paradox - why we are afraid of the wrong things]. Frankfurt am Main 2014.

1.3.8 Cyber threats

Cyber threats are faced in a similar manner as is terrorism. While they have been neglected for a long time, there is also a lot of aimless actionism and pseudo-security to be observed, which is reflected in statements such as

> "[The core elements stated are the loss of information confidentiality, digital espionage and the implanting of computer viruses. Cyber crime is also increasing in significance albeit with a background of fraud by professional criminals and should rather not be rated as power projection.]"[119]

In this case we are also more oriented towards the past and to experience to date.

The real threat to our security and society is not data loss but rather the threat that our critical infrastructure, which is increasingly connected to the Internet, could physically fail, as a result of whatever event, which would in turn result in numerous knock-on effects. Our current system design and dependency does not allow for failure.

We have designed a lot of infrastructure of existential importance as "too big to fail", without being aware of, nor having a plan B for potentially large-scale malfunctions. And yet a threat is not only posed by aggressors but is also inherent in the system. On January 1st 2010, numerous EC and credit cards failed due to defective programming of the microchips. The customers affected could neither withdraw cash from cash machines, nor make cash-free payments.[120] Such a defect in highly interconnected infrastructure would presumably have devastating consequences, as was demonstrated once more at the hacker's conference Black Hat 2014. Researchers succeeded in compromising an intelligent power meter ("smart meter"),

[119] See Chapter 3.3.

[120] Cf. Geldautomatenproblem: 2010-Bug lässt Bankkunden verzweifeln [cash machine problem: 2010-bug leaves bank customers in despair]. In: Spiegel Online, 04/01/2010. <http://www.spiegel.de/netzwelt/netzpolitik/geldautomatenproblem-2010-bug-laesst-bankkunden-verzweifeln-a-670062.html>, accessed on 22/12/2015.

millions of which had been rolled out in Spain, and initiated a remote shutdown through the network.[121] A new business model for organised crime – society has become massively susceptible to extortion.

Another example of our “blind spots” is shown in the “Power Supply Dependencies in the Electronic Communications Sector”[122] report by the European Union Agency for Network and Information Security (ENISA). As a by-product of covering cyber incidents in the EU, it was exposed that “power cuts are a dominant cause of severe network and service outages in the EU’s electronic communications sector”. The greatest damage was therefore caused by overload, blackouts and software faults. In which context of course it is necessary to take into consideration that, in a complex system, a small cause can have devastating effects. But if not even simple homework has been done, this probably means that the vulnerability of these systems is greater by far than is commonly assumed; even if, surprisingly, no larger incidents have happened so far.

In this case we are likely to be subject to a dangerous “turkey illusion”[123].

Current cyber security concepts barely take these factors into account, not to mention that cyber defence does not constitute a second line of defence in a networked system in the way that people are keen to see it.

[121] Cf. Thoma, Jörg: Intelligenter Stromzähler. Gehackte Smart Meter machen Lichter aus [intelligent power meter: hacked smart meters turn off the lights] <http://www.golem.de/news/intelligente-stromzaehler-gehackte-smart-meter-machen-lichter-aus-1410-109923.html>, accessed on 22/12/2015.

[122] European Union Agency for Network and Information Security (ENISA): Power Supply Dependencies in the Electronic Communications Sector. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies>, accessed on 22/12/2015.

[123] A turkey that is fed by its owner day by day assumes, on the basis of its daily positive experiences, that the probability of something severe happening decreases day by day. At the same time its trust increases with every positive experience (feeding). However, on the day before Thanksgiving (when turkeys are traditionally butchered) the turkey faces a fatal surprise

1.3.9 "Blind spots"

Our general focus on combating the potential actors leads to our overlooking many things that are actually far more serious. Terrorism can only have effects if we allow it. On the one hand through our reactions and, on the other hand, by providing it with vulnerabilities of which it can take advantage. Whilst in recent years several billion euros have been spent on increasing aviation security, at the same time we have allowed our infrastructure to become more vulnerable.

Through technological interconnectedness we have mostly unwittingly created highly complex and mutually dependent systems with probably devastating systemic risks. Thus we are in no way prepared for strategic shock events ("black swan") resulting from this.[124] Regardless of whether this concerns the European power supply infrastructure, the telecommunication and Internet infrastructure or the food supply, we are in many areas walking on thin ice. A bigger incident in one sector would cause far-reaching domino effects, even beyond the system's boundaries.

A major disruption in the European power supply system ("blackout") would have devastating consequences, not only for the electricity industry but for society as a whole, as we are completely dependent on a faultlessly functioning power supply.[125] Such an event would simultaneously put our financial and economic system to a severe test or even cause further far-reaching domino effects. In this context it is irrelevant what and who caused such an event, whether it was through technical breakdown, natural events or terrorism. Therefore our focus and our energy should be put less on po-

[124] An event with the three attributes of rarity, major effects and predictability in retrospection (but not in foresight). See Taleb, Nassim Nicholas: The Black Swan. The Impact of the Highly Improbable. Random House, 2007.

[125] Cf. European Union Agency for Network and Information Security (ENISA): Power Supply Dependencies in the Electronic Communications Sector. Survey, analysis and recommendations for resilience against power supply failures. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies>, accessed on 22/12/2015.

tential actors and rather on the targets that we have created largely unwittingly. This does not only concern the vulnerability of our infrastructure, but also the capability reasonably to handle such disturbances as a society.

1.3.10 Systemic risks

The chaotic and non-systemic technical interconnection in recent years has led to a massive increase of the number of systemic risks in our society and in critical infrastructure.[126] These are characterised by:

- a high degree of interconnection (dynamics, complexity, interactions)
- the threat of domino effects
- non-linearity in the consequences (no simple cause-effect chain that can be captured by standardised risk management) and
- by systematic underestimation by the persons responsible.

This led to a massive increase in the probability of strategic shock events, which means events that are capable of enduringly – long-term and significantly – changing our coexistence ("game-changers"). Even though today's really big issues have not been directly covered yet:[127]

1. Threats through human interventions in the Earth's ecosystem (e.g. climate change, shortage of resources, freshwater crisis, endangerment of biodiversity)
2. Threats through regulatory deficits in economy and society (handling public goods, financial crises, pandemics).
3. Threats through undesirable social developments (unequal living conditions).

[126] Cf. Zurich Insurance Company Ltd and Atlantic Council of the United States (Eds.): Beyond data breaches. Global interconnections of cyber risk. <http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk>, accessed on 22/12/2015.

[127] Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten [the risk paradox - why we are afraid of the wrong things]. Frankfurt am Main 2014.

Furthermore, nowadays people or groups feeling powerless can cause large effects ranging up to catastrophes (small cause, large effect) with the aid of modern technologies. The terrorist attacks on 9/11 were ultimately initiated with a simple carpet knife:

> "[Though this weapon can be used to kill people, it only becomes a systemic risk if it is linked with the vulnerability of modern interconnected technologies. Because it was by means of a carpet knife that the terrorists were able to acquire substantially more effective weapons such as aircraft, which were in turn used to exploit the vulnerability of complex skyscraper structures. The cascade from simple means right up to global impact is made possible through the described interrelationships between technological development, virtualisation and the increase of vulnerability. (...) Added to this is the multiplier effect (domino effect) through globalisation and interconnectedness, through which the abuse of power, criminal actions and terrorism also possess substantially higher efficacy than before.]"[128]

1.3.11 Risk perception

One important reason for the many "blind spots" can be traced back to the fact that our perception of risk is primarily based on past experience and highly selectively filtered information from the media. The former has an evolutionary basis and has sufficed to date. But institutionally derived information is also largely subject to a predefined hierarchy of significance and largely reflects only a subset of reality.[129] In addition, the public are inundated by alternating waves of dramatisation (media) and belittlement (politics). The multiplicity of topics and constant urgency typically leave no time for deeper consideration. Moreover, a strong oversimplification ("management briefing") is often demanded. All this notwithstanding the fact that our mechanisms of control (management) remain oriented towards industrial thinking and action for both simple and complex systems (machines).

[128] Ibid, p. 494.

[129] Cf. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0 [network society and crisis management 2.0]. Master's thesis, Budapest School of Management, 2013.

Numerous falsely (and to some extent irrationally) perceived risks exist. Whilst we react almost hysterically to individual supposed risks, as for example recently in the case of Ebola[130], we essentially fail to perceive other, far more threatening risks, in which context Ebola stands as an example of ambivalence. Whilst the danger was underestimated for far too long in the regions affected, it is totally underestimated in our area. By way of comparison, in Austria around 8000 people die each year whether directly or indirectly as a consequence of alcohol consumption. To put it another way, around 16 times as many as in road traffic accidents.[131]

It is currently estimated that 25,000 people die every year in the EU as a result of infection by multi-resistant bacteria. The associated secondary costs are estimated at around 1.5 billion euros per annum.[132]

The global financial market is also the subject of keen discussion in connection with terrorism and the possibility of straightforward finance and capital transfer.[133] As a result of the financial crisis of 2007/2008, it was also possible to conclude that a much higher level of risk arises from the financial markets themselves and that the number of victims – indirectly including those killed – is much higher as a result of financial capitalism at a higher level. Nevertheless this is not so obviously evident and contradicts our current conceptual models. Here we have cognitive barriers.

[130] By the end of May 2015 around 11,000 people died. WHO: Ebola Situation Report - 27 May 2015. <http://apps.who.int/ebola/current-situation/ebola-situationreport-27-may-2015>, accessed on 20/12/2015.

[131] University of Salzburg: Alkohol. Fakten and Mythen [alcohol – facts and myths]. <http://www.unisalzburg.at/index.php?id=50709>, accessed on 20/12/2015.

[132] Hell, Markus: Clostridium-difficile-Infektion, antibiotikaassoziierte Diarrhö/Colitis. Nosokomiale Last. [clostridium difficile infection, antibiotic-related diarrhoeiah/colitis, nosocomial burden] <http://www.medmedia.at/univ-innere-medizin/infektiologien osokomiale-last/>, accessed on 20/12/2015.

[133] See Chapter 2.2 – also “global financial markets” facilitate capital transfers by terrorists.

Another example is provided by Switzerland's risk report of 2012.[134] This posits that a pandemic and loss of electricity supply would constitute the greatest risk for Switzerland in terms of scale of damage and probability of occurrence. At the same time, we speak of a European network in which all countries would be affected to the same extent, like in the case of a pandemic. Yet scarcely any other country in Europe addresses this to a comparably thorough extent. Indeed ignoring the fact that dealing with it at the level of public authorities (crisis management) is not possible and that it would require a comprehensive, societal approach in order to be able sensibly to deal with such strategic shock events.

1.3.12 Hybrid threat potential

But what does all of that have to do with hybrid threats? A great deal, even though many contradictions might seem to arise at first sight. Through the definition of hybrid threats, the aim was to take current developments into account.[135]

Nevertheless, there followed an attempt at classification according to the logical approach that had been successful to date, based on the assumptions of "actors", "enforcement of interests" and a "strategic threshold". Yet these "silos" stand in contradiction to the network society and to actual developments. This is also evident in the case of the "actor overview of hybrid threats"[136] for example. Here "silos", which had so far been clearly identifiable and conventional, were compared. The entirety can also be illustrated in a clear manner, albeit scarcely reflecting reality. Because there are multi-layered networks and crosslinks between the various domains ("invisible strands") with effects and dependencies that are delayed in time. Thus the consequences that can be inferred reflect the logic to date, albeit being appropriate only to a limited extent or not at all to VUCA developments.

[134] Federal Office for Civil Protection (FOCP): Katastrophen und Notlagen. Schweiz. Risikobericht 2012 [catastrophes and emergencies, Switzerland, risk report 2012] <http://www.alexandria.admin.ch/bv001490434.pdf>, accessed on 20/12/2015.

[135] See Chapter 1.3.

[136] See Figure 3.

But if one attempts to depict the initial question “what factors are decisive for the sovereignty of a state (community of states)” in a model, it quickly becomes confusing (Figure 11).

But the model is not at fault here, rather it is our wish to lay out complex circumstances as simply as possible, which leads to radical, readily illustrated simplifications that have little to do with the actual situation. Numerous failed large projects bear silent witness to this.

From research it is known that our minds can grasp the potential interactions between a maximum of 3 to 4 factors. Everything beyond that requires tools and visualisations. One possibility, as begun in the model “sovereignty of a state (community of states)” (Figure 11), is to gather and display the potential interactions and interrelationships. Further analyses can then offer insight into interactions that are delayed in time or otherwise not detectable.

On the other hand, modelling offers the possibility to observe and highlight individual aspects in isolation without losing sight of potential interactions (Figure 12). A model also makes it possible to gather together potentially contradictory views that will essentially exist for all time.[137]

[137] Cf. VUCA - volatile, uncertain, complex and ambiguous.

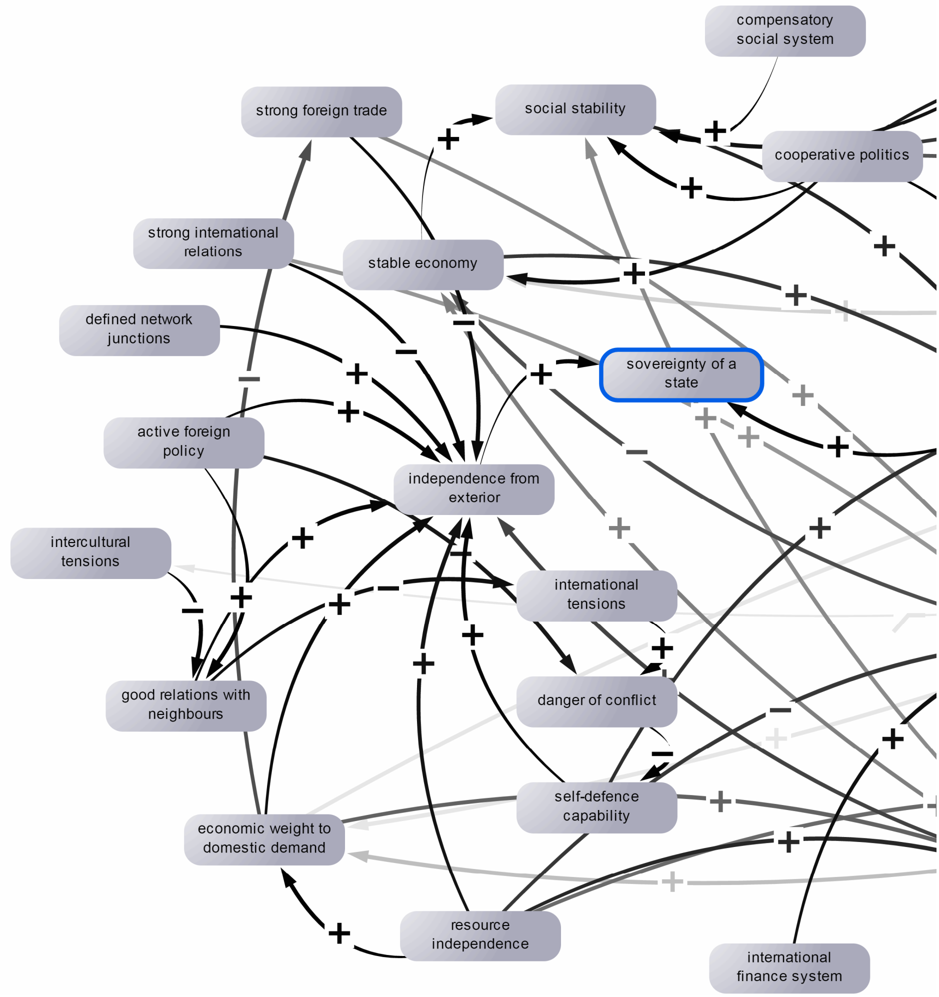
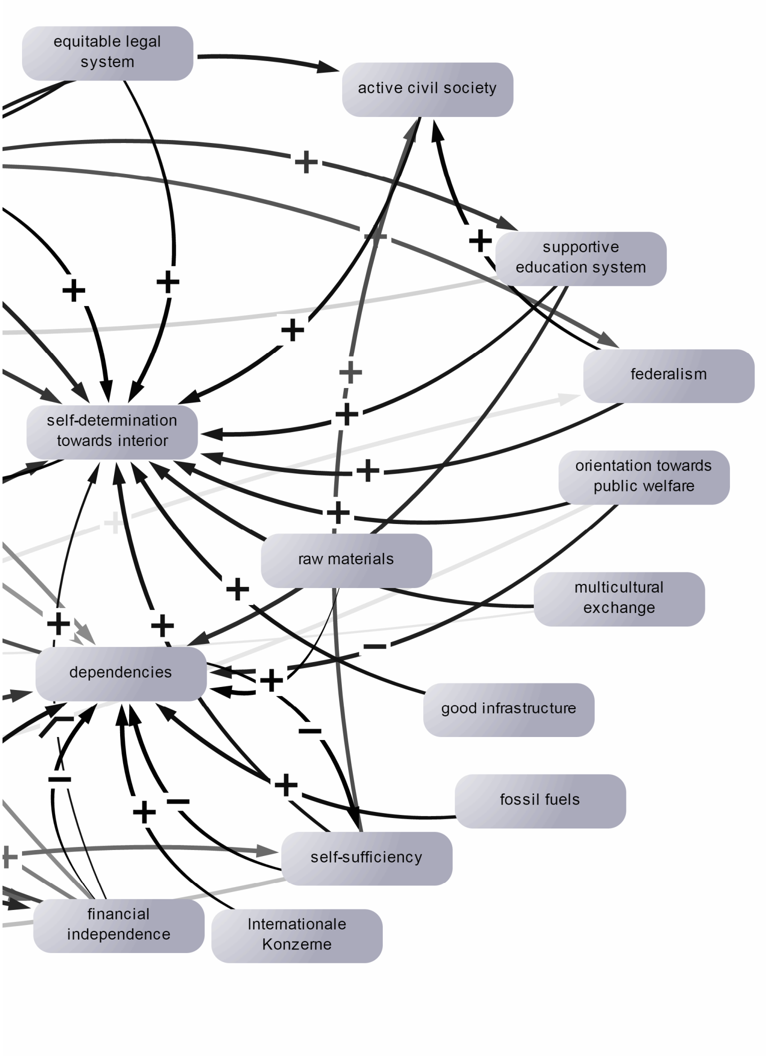


Figure 2: What factors are decisive for the sovereignty of a state (community of states), reduced depiction

Herbert Saurugg


equitable legal system
active civil society
supportive education system
federalism
self-determination towards interior
orientation towards public welfare
raw materials
multicultural exchange
dependencies
good infrastructure
fossil fuels
self-sufficiency
financial independence
Internationale Konzerne
+
−

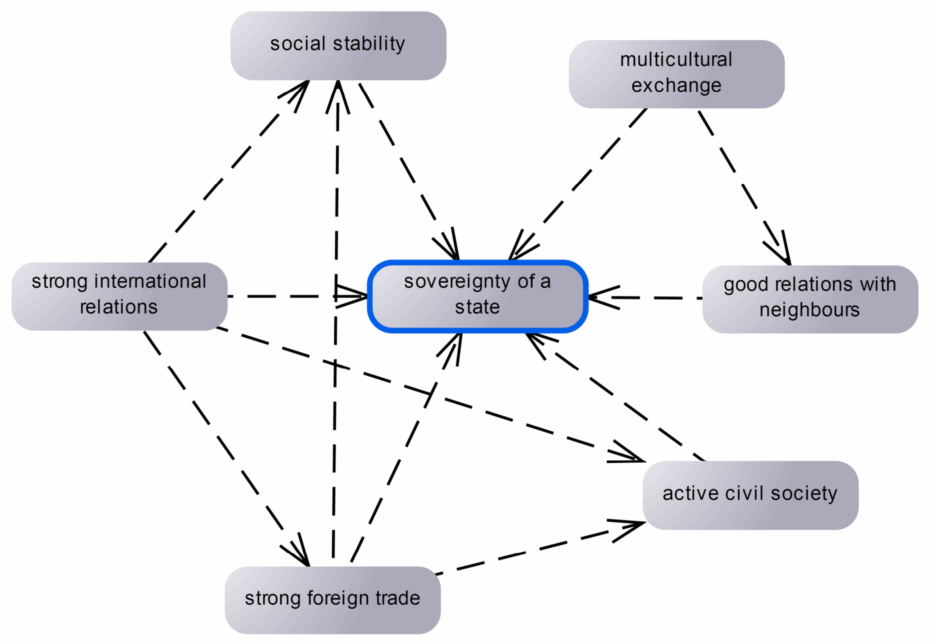


Figure 13: What factors are decisive for the sovereignty of a state (community of states)
Herbert Saurugg

However, a model is not a depiction of reality but rather just an attempt to come closer to it. Here we can draw on the comparison between a landscape and corresponding map. It is not the density of detail that leads to a better result but rather the depiction of the important features of the land. Naturally these differ according to purpose, for example for use travelling on foot or by aircraft. The same applies with models, which should reflect a subset of reality. They serve as instruments of communication, creating a common view. Thus, in order to be able to capture the actual dependencies and realities pertaining to the sovereignty of a state (community of states), actors would also have to exert their influence from their various "silos" in order to arrive at the best possible reflection of reality at the time of construction. This is becoming increasingly difficult as a result of today's dynamics and speeds. Strictly speaking, this would require a continuous process. Thus, as determined in the country analyses, the question arises as to whether non-formalised (Sweden)[138] or out-of-date strategies (Slovakia)[139] really deliver gains.

1.3.13 But how can one deal with hybrid threats then?

By critically examining the initial definition[140] and testing whether, in the light of the remarks so far, it is really appropriate or whether it might not be more necessary by far to define a new formulation of the question. If we assume that the future will be more volatile, uncertain, complex and ambiguous (VUCA), then we do indeed require a new conceptual model.

The individual country strategies demonstrate altogether promising approaches. For example in Sweden, where they do not emphasise formalised strategies or recorded concepts but rather a culture of cooperation that is flexible and adapted to reality, even if analysis shows that there is a need for improvement in terms of practical implementation.[141] On closer examination of many strategies it emerges that there are substantial differences between the formalised "aspirations" and actual implementation. Indeed there are several examples of this in Austria.

The statement by Michael Miklaucic, Director of Research and Editor of PRISM at the Center for Complex Operations at National Defense University, that "*A hybrid threat is more than just the sum total of its constituent parts. Combating such threats does not require new capabilities as much as new partners, new processes and, above all, new thinking*" is totally apposite.[142]

[138] See Chapter 2.2.

[139] See Chapter 2.1.

[140] See Chapter 1.3.

[141] See Chapter 2.2.1: "There is not even a white book or a green book dealing with national security. Threats are usually not faced with published concepts, but rather pragmatically, depending on the specific situation."; see also Chapter 2.2.2 "The orientation of Sweden's security policy is characterised by a strong culture of cooperation."

[142] NATO: Countering the Hybrid Threat. <http://www.act.nato.int/nato-countering-

Another aspect that stands out from the Swedish analysis is the Civil Contingencies Agency[143]. Whilst for example Germany also has a Federal Office of Civil Protection and Disaster Assistance (BBK) and Switzerland has a Federal Office for Civil Protection (FOCP), there is no such institution in Austria. Disaster control in Austria is a matter for the provinces and is correspondingly heterogeneous in its structure. National or indeed international crisis situations or strategic shock events can only receive insufficient coverage as a consequence. The recording of systemic risks is therefore also inadequately covered. With an organisational structure of this kind, care must be taken to avoid creating yet another silo but rather an instrument of networking. Because many of the necessary system elements are already present in some form today. What is missing is networking aligned to requirements and goals, whilst preventing that "silo-thinking and behaviour" seen to date.[144]

This is also addressed indirectly in the Slovakian analysis by Rastislav Báchora, in which there is a call for solidarity between institutional, non-state, civil-societal and commercial actors.[145] This intent has basically already been formalised in Austria in the comprehensive national defence (ULV) and, today, in the comprehensive security (USV) policies. Yet reality always lagged significantly behind the preconceived objectives.

Through standardised and simplified processes, over recent years great advances have been made in terms of standard missions, also leading to very high quality of supply. Broad collaboration between emergency response organisations has indeed become state-of-the-art, albeit often only in the case of real cases. Common training, or at least shared training mod-

the-hybrid-threat>, accessed on 21/12/2015.

[143] See Chapter 2.2.1: "One of the important actors is the Swedish Civil Contingencies Agency (MSB). The MSB's duty is the improvement of social capacities and assisting preparation for and prevention of emergencies and crises."

[144] Cf. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0 [network society and crisis management 2.0]. Master's thesis, Budapest School of Management, 2013.

[145] Institutional collaboration on combating threats includes both non-state and civil-societal as well as commercial groups.

ules, are still at an early stage or limited to individual areas. Interoperability between civil and military emergency response organisations has indeed been improved (with regard to leadership organisation for example), but there is still a great deal of room for improvement, in order also to be prepared for the effects of potential strategic shock events. Not to mention the challenge of collaboration in disaster situations with "volunteer assistance"[146] like the members of Team Austria.

Yet another example is the civil-societal initiative "Plötzlich Blackout!" [sudden blackout!] – preparation for a pan-European power failure.[147] Whilst to date there has been no national scenario for a potential, sudden, widespread and prolonged power failure ("blackout") offered from institutional sources in Austria, the initiative has been tackling this scenario since autumn 2013 and, through various events, has involved several hundred organisations from all areas important to society (authorities, emergency response organisations, businesses, research and civil society) and indeed created an international network. Particularly in the case of new topics, civil society is often more flexible and faster. More attention should be paid to this potential in the context of security policy topics.

It is possible that increasing financial pressure may lead in future to society paying more attention to potential synergies. Austrian culture is indeed characterised by "unofficial channels".

Wherever formalised structures are insufficient, informal channels ("invisible threads") proliferate and contribute to success. The counter example would be a menacing "follow the rules". Austrians often act intuitively according to the principles of network society, networking in a flexible and *ad*

[146] Cf. Kircher, Friedrich: Ungebundene Helfer im Katastrophenschutz. Die Sicht der Behörden und Organisationen mit Sicherheitsaufgaben [volunteer assistance in disaster control – the view of authorities and organisations with duties of protection]. <http://www.katleuchtturm.de/assets/content/images/pdfs/593_597_Kircher.pdf>, accessed on 21/12/2015.

[147] See Resilienz Netzwerk Austria, Plötzlich Blackout! Preparation for a pan-European power failure. <www.ploetzlichblackout.at>, accessed on 22/11/2014.

hoc manner to achieve gains. For this characteristic, we are often looked on with envy from elsewhere. Therefore we should consciously perceive it as a strength, foster it and utilise it to the benefit of the whole.

1.3.14 Vulnerabilities

As may be inferred from the preceding discussion, we should pay more attention to vulnerabilities than to potential actors. According to the definition of hybrid threats, it is also anything in the range from increasingly difficult to impossible for the potential actors to assert their own interests against others. They too are subject to the laws of complex systems. Albeit this does not exclude the possibility of temporary influence. Here it is necessary to think in terms that are not limited to the very short temporal horizons now common in business studies, but rather more long-term. Because many *quick and dirty* solutions concentrate just on the symptoms and can be implemented immediately, whilst fundamental solutions strive to resolve the cause of the problem. *Quick and dirty* solutions are typically quickly applied, yet they aggravate the actual problem in the long term, whilst fundamental solutions often deliver significant disadvantages in the short term and only reveal their advantages in the long term.[148]

A current example is the conflict between the EU/Ukraine and Russia. Neither side can really assess what the consequences of the threatening gestures and sanctions to date may turn out to be. At the same time, the mechanisms can be categorised according to former thinking. That the mundane should lead to catastrophe historically is anything but unique. Here too we have many “blind spots”.

For months now there have been indications of targeted cyber-attacks on western electricity supply companies, which are thought to have come from Russia, albeit something that can never be determined with certainty.[149] Never-

[148] Cf. Ossimitz, Günther/Lapp, Christian. Systeme: Denken und Handeln. Das Metanoia-Prinzip. Eine Einführung in systemisches Denken und Handeln [systems: thinking and acting – the Metanoia Principle – an introduction to systemic thinking and acting], 8 Edition, German publisher, Berlin 2006.

[149] Thomson, Amy/Rahn Cornelius: Russian Hackers Threaten Power Companies,

theless, alarm bells should be ringing. In 2007, the relocation of a Russian monument led to a massive cyber-attack on Estonia. At that time, "only" virtual systems were affected. Today our most critical infrastructure could be attacked and potentially caused to break down. Here it is important to steer clear of attributing such a possibility to one actor alone. Cyber-attacks in particular can rapidly go out of control and develop a momentum of their own that was never foreseen, as is indeed possible in complex systems.

In Switzerland this scenario was taken as the starting point for the security alliance exercise of 2014,[150] having the consequence of instabilities in the electricity supply system triggering a blackout. Assessed as even more serious were the subsequent power shortages stretching over several weeks, because neither society nor infrastructure is prepared for such a strategic shock event.[151]

In the summer of 2014, the Belgian government passed a national emergency plan, involving the preparation of national emergency shut-downs of power supply for the following winter. The cause was two nuclear power stations which, as a result of massive security concerns, had to be taken off the grid, along with worries that the supply of electricity could not be maintained throughout the winter.

Meanwhile, there are another 22 reactors of identical construction operating in Europe with the very same critical security flaws.[152]

Researchers Say. <http://www.bloomberg.com/news/2014-06-30/symantec-warnsenergetic-bear-hackers-threaten-energy-firms.html>, accessed on 07/01/2016.

[150] Cf. Saurugg, Herbert: SVU'14 – Überwinden der Krise [overcoming the crisis]. <http://www.saurugg.net/2014/blog/stromversorgungssystem/svu14-ueberwindender-krise>, accessed on 07/01/2016.

[151] Cf. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport [Federal Department of Defence, Civil Protection and Sport], Newsletter SVU 14 – June, <http://www.vbs.admin.ch/internet/vbs/de/home/themen/security/svu14/dokumente.parsys.9373.downloadList.82421.DownloadFile.tmp/infosvu14junid.pdf>, accessed on 26/10/2014.

[152] Cf. Resilienz Netzwerk Österreich: Belgiens Angst vor dem nächsten Winter [Belgium's fear of next winter]. <http://www.ploetzlichblackout.at/2014/

In its study entitled “Future Global Shocks - Geomagnetic Storms”, the OECD (Organisation for Economic Co-operation and Development) states:

> “The lack of valid risk assessments has limited risk mitigation efforts in many critical infrastructure sectors, as it is difficult to demonstrate the utility of investing in either hardening or operational mitigation efforts, especially if these investments reduce time and money spent in preparing for more common risks. (...) Geomagnetic storms can be categorized as a global shock for several reasons: the effects of an extreme storm will be felt on multiple continents; the resulting damage to electric power transmission will require international cooperation to address; and the economic costs of a lengthy power outage will affect economies around the world.”[153]

There is a substantial threat to our infrastructure systems arising from solar geomagnetic storms. Here too, our electricity supply infrastructure is massively endangered as a result of current system design.[154]

In connection with the smouldering conflict with Russia, a European stress-test was carried out on natural gas supply. The regulatory authorities seek to bring calm on the basis of statements that, in the event of an interruption of the supply of gas from Russia for several months, no danger would threaten. At the same time, the shortage of gas supply in 2012 would have practically led to a blackout.

Here too, we do not yet know what other dependencies or interactions may exist.[155]

08/21/belgiens-angst-vor-dem-nächstenwinter/>, accessed on 24/10/2014.

[153] OECD/IFP: Futures Project on “Future Global Shocks - Geomagnetic Storms”. <http://www.oecd.org/dataoecd/57/25/46891645.pdf>, accessed on 08/01/2016.

[154] Cf. Resilienz Netzwerk Österreich: Ein heftiger Sonnensturm hat die Erde im Juli 2012 knapp verfehlt [massive geomagnetic storm narrowly missed the Earth in July 2012]. <http://www.ploetzlichblackout.at/2014/07/26/ein-heftigersonnensturm-hat-die-erde-im-juli-2012-knapp-verfehlt/>, accessed on 24/10/2014.

[155] Cf. Saurugg, Herbert: Druckmittel Gas. Reale Gefahr oder Hysterie [gas pressure – real danger or hysteria]? <http://www.saurugg.net/2014/blog/gesellschaft/druckmittel-gas-reale-gefahr-oderhysterie>, accessed on 08/01/2016.

Just these few examples indicate the massive vulnerability of our critical infrastructure and therefore also our society. Yet to date, all these aspects have been scarcely taken into account with regard to the “protection of critical infrastructures”. In 2013 the EU Commission admitted:

> “The review process of the current EPCIP (European Programme for Critical Infrastructure Protection), conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries. (...) The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an interconnected network. Most work has been sectoral, but these methodologies show their limits when cross-sectoral issues need to be addressed, so a systems approach will be encouraged by the Commission from now on.”[156]

Critical infrastructure protection (CIP) is no longer anywhere nearly sufficient; rather, we also need “protection AGAINST critical infrastructure”, a Plan B, should a large-scale failure occur.

Over the mid to long term, with current systems design and the high degree of networked and mutual interdependency, it is not possible to guarantee the security and protection of the people. Thus in nature, the principle “small is beautiful” has prevailed, because excessively large structures are more susceptible to disturbance. Nature does not limit the interactions between beings, but rather just their size.[157]

[156] European Commission: Commission Staff Working Document. On a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. <https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf>, accessed on 08/01/2016.

[157] Cf. Vester, Frederic. The Art of Interconnected Thinking – Tools and concepts for a new approach to tackling complexity]. A report to the Club of Rome. Published by Mcb Verlag, 2007.

Given our complex technical systems and solutions, it therefore seems more than necessary to learn from nature too, in order to secure long term viability.

1.3.15 System design

The system security of any system against any disturbing influences can be raised using simple basic rules, whether the disturbance is triggered by a fault, natural event, chance or the actions of an aggressor.

1.3.16 Reducing energy demand

Every evolutionary development in nature takes place by virtue of a reduction in energy demand. This allows external dependencies to be reduced and the viability of a system to be raised. Albeit, this does not apply solely to classical forms of energy. Our highly synchronised system of logistics and supply for distributing essential foodstuffs exhibits massive vulnerabilities. Not to mention the high consumption of energy made necessary by transportation and processing. In addition, energy supply as achieved to date is impossible with volatile production. The energy revolution can only succeed if we are able significantly to reduce our demand by means of intelligent measures. This requires a cultural change and not merely technical solutions. This can also allow the reduction of the kind of dependencies that were necessary in the industrial age.

1.3.17 Decentralisation

The second aspect is decentralisation. Complex systems do not allow themselves to be controlled or organised centrally. They require decentralised, self-regulating feedback processes. At the same time, decentralised systems are more robust against and resistant to disturbances. Playing an important part here is the capacity for self-organisation, which is basically inherently present in the system. But decentralisation does not mean isolation or encapsulation, quite the contrary. Decentralisation means the emergence of viable structures that can, in turn, readily generate a greater whole with other structures (cellular structure), nonetheless without resort to chaotic interconnection. Many structures were already present before technical interconnection. They do not have to be newly invented. Nevertheless, with today’s possibilities it is possible to create additional value without jeopardising the whole system.

1.3.18 Error-friendliness

A further aspect is the error-friendliness and error-tolerance in a system. We have largely optimised our technical systems and strive to rule out errors to the maximum extent possible, something that regularly falls through in cases of the “human factor”. Yet instead of adjusting technology to people, the reverse continues to be pursued, with poor prospects of success. In nature, disturbances are not overridden but rather they are integrated into the process. This requires vacant spaces, buffers, redundancies, variations, diversity, flexibility and capability of change and adjustment. Of particular importance are barriers, in order to ensure the limitation of effective range in the event of disturbances.

Today the European electricity supply system possesses insufficient barriers capable of preventing the propagation of a disturbance. As a consequence, a major disruption could spread across the entire continent within a few seconds.

The Internet has access to innumerable sub-networks, yet there is a dearth of diversity in system elements. Consequently malware, for example, can spread very quickly. In addition, both systems are “too big to fail”. The error-friendliness of a system is a prerequisite for being able to deal with insecurities and turbulence, and it is not limited solely to technical systems.

In recent years and with increasing effort and outlay, attempts have been made to minimise or indeed eliminate security risks of any kind. Society has developed into a kind of “fully-comp-society” that is ever decreasingly prepared to put up with turbulence or failures of important pieces of infrastructure. So here too, new approaches are necessary.

1.3.19 Resilience

Alongside consideration of the aspects laid out above, decisive in the elevation of security for society is also people’s resilience. This term is not very common in the German-speaking world, but is gaining importance. It describes a system’s capability to deal sensibly with disturbances. Often it is misinterpreted as simply resistance, which falls short. It is not only about robustness but also about the capability to adjust and recover, as well as agility. This includes the capability to emerge stronger from disturbances. Following a disturbance, resilient systems can return to their original state or move to an improved, transformed level. The term "resilience" is used in psychology to describe people who, despite adverse circumstances, emerge from crises in a stronger state, whilst others collapse under the strain.

What does that actually mean? Many people are accustomed to the idea that there is always someone with responsibility who can hurry to help ("fully-comp-society"). Yet when it comes to strategic shock events, resources are limited. Only if a certain level of individual precautionary measures and responsibility is adopted can society sensibly overcome such events. Moreover, risk-responsibility and self-efficacy automatically lead to greater resilience. The effects of hybrid threats for example are limited as a consequence. The collective system that is society becomes more resilient.

1.3.20 Summary

This systemic examination draws the conclusion that current security policy assessments, as laid down in the European security strategy for example, fall far short of describing the current situation with regard to threats:

> "Taking these different elements together – terrorism committed to maximum violence, the availability of weapons of mass destruction, organised crime, the weakening of the state system and the privatisation of force – we could be confronted with a very radical threat indeed."[158]

A systemic examination and networked thinking therefore appear indispensable in order to be in a position to deal sensibly and successfully with current and future challenges. Security is always relative and subjective. But the choice of how we implement the process of examination and our resources is up to us. Security does not mean the elimination of risk, but rather dealing with it sensibly. Because security and continued develop-

[158] Council of the European Union: European security strategy. A Secure Europe in a Better World. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>, accessed on 10/01/2016.

ment are not possible without insecurity. The polar opposites are mutually dependent.[159]

As has also emerged from the investigation, we should step back from those "silo" viewpoints so common to date, because they do not correspond with networked reality and, in the best case, only create apparent security. Altered circumstances lead not only to the world becoming ever more opaque and uncontrollable, but also and rather to external control becoming anything from more difficult to impossible. Therefore it is less a matter of ascertaining potential actors and definite threats and much more one of active and robust system design that can deal with all disturbances, whether triggered by an aggressor, fault, natural event or whatever.

In order to be better able to deal with the resulting ambivalences, "not-only-but-also-thinking" is required. Our western "either-or-thinking" limits possibilities and hinders solutions. The ancient wisdom of the Chinese military strategist Sunzi, according to which war and conflict could be avoided as much as possible, is still completely valid today. So we should present as few targets for attack as possible.

It is therefore necessary for us to break open the "silos" we have had to date and secure cooperative networking and collaboration between politics, business, civil society and science. Only then will we succeed in effectively and efficiently limiting systemic risks whilst, at the same time, paying sufficient attention to the ecological, economical and social side-effects of potential risk-reducing measures.[160] Important characteristics of the network society are transparency, participation and collaboration and the assembly of *ad hoc* networks. It is not competition but rather cooperation that stands in the foreground. Here there cannot be the expectation that all people actively participate. But if it proves possible to bring the "brightest minds" together on respective topics, then we will again develop solutions that earn such a rating and are also adopted by the community at large.

[159] Cf. Völkl, Kurt/Wallner, Heinz Peter. Das innere Spiel. Wie Entscheidung und Veränderung spielerisch gelingen [the inner game – how decision and change playfully succeed]. Göttingen 2013.

[160] Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten [the risk paradox - why we are afraid of the wrong things]. Frankfurt am Main 2014.

From this it is possible to deduce a number of aspects for Austrian security policy and for the Austrian Armed Forces in particular:

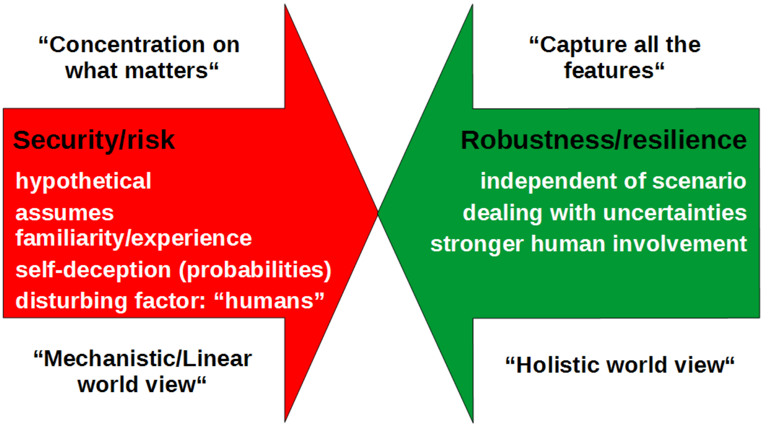
- Compulsory military service should be used to train young people in self-efficacy and the capacity for self-help. This would be of great value to society and contribute to raising overall societal resilience.
- The Austrian Armed Forces' self-concept should be more strongly oriented towards the new challenges. The Austrian Armed Forces will be granted neither the means nor the appreciation of a mass army of industrial society. The army of the network society is fragmented, flexible and adaptable. Above all this means more flexible structures that make this possible. But it also indicates the necessity not for a focus on core tasks (national military defence) but rather for a move towards greater flexibility, in order to be able to react to the maximum possible number of scenarios for the benefit of the people. All this regardless of what has triggered them and whether they constitute military tasks in the classical sense.[161]
- Permeability between the various security domains and better cooperation are required. The Austrian Armed Forces constitute a whole-of-nation strategic reserve, which is indispensable for society. This is not just about military capabilities but rather capabilities and resources that otherwise are not providable. This could also mean that, in a strategic shock event, soldiers might take over and support leadership and self-organisation at a local level. This requires new attitudes and adjustment to the organisational culture.
- Critical infrastructure protection must be reoriented. Strongly networked entities and infrastructures cannot be protected by security services. Far more likely is that, after a possible attack, soldiers will be required not to secure/protect entities but rather for clearing up. Other measures, such as the elevation of IT security, constitute only a small subset of today's requirements.

[161] Cf. Gutmann, Günther: Eisregen in Slowenien mit nachfolgendem großflächigen Stromausfall Anfang 2014 [ice rain in Slovenia with subsequent widespread power failure at the start of 2014]. In: Truppendienst - series 340, issue 4/2014. <http://www.bundesheer.at/truppendienst/ausgaben/ausgabe.php?folge=340>, accessed on 10/01/2016.

- Strategic shocks cannot be prevented. We can indeed minimise the preferred systemic risks, though this does not offer complete protection. We must therefore orient and marshal ourselves in such a way that we can overcome such events as quickly as possible and return to a new reality. Here sensible ways of dealing with insecurities and uncertainties are essential. However, this also requires discourse in society.

- A whole-of-nation viewpoint is required. There appears to be an urgent need for a national competence centre for civil protection in order, on the one hand, to be able to ascertain the multilayered problem scenarios and systemic risks and, on the other, to guarantee national or indeed international coordination and monitoring. But this must not involve the creation of any new "silos". Far more, the spotlight should be on networking individual elements that are already present. Crisis management itself must also continue to take place at a local/regional level as well as autonomously and through self-organisation when required.

- Promises of technical solutions should not be accepted without prior reflection. Many supposed solutions merely create greater problems.


"Concentration on what matters"
"Capture all the features"
Security/risk
hypothetical
assumes familiarity/experience
self-deception (probabilities)
disturbing factor: "humans"
Robustness/resilience
independent of scenario
dealing with uncertainties
stronger human involvement
"Mechanistic/Linear world view"
"Holistic world view"

The consequences are relevant!

Figure 14: Consequences
Herbert Saurugg

2 Description of the analysed security Strategies in the Reference States

As mentioned at the outset, this study focused upon two states that are comparable with Austria in some aspects, but also show great differences in others, such as in perspectives for cooperation due to their affiliation with other alliances. Security-relevant strategy documents from Slovakia and Sweden have been analysed by experts from the respective countries and experts with relevant language skills, regarding awareness of hybrid threats. If no references to hybrid threats were found, the experts had to analyse the violent actors mentioned in these documents regarding their relevance to hybrid threats.

2.1 Slovakia

Rastislav Báchora

2.1.1 Introduction

A modern approach to hybrid threats requires an adequate comprehension of security, as well as the necessary capacities within government institutions. Within the present study it shall be clarified how much importance is attached to potential hybrid threats in the Slovakian security strategy, as well as in other documents and which actions are covered conceptually and institutionally in repelling these threats by which regulatory instruments. Primarily, however, it has to be brought into question whether a document such as the Slovak Republic's (SR) security strategy from 2005 can actually meet the normative requirements to satisfy the scientific-analytical and real-political demands of hybrid threats.

Initially, the analysis at hand shall cover the essential security policy parameters. Thereupon it shall have a focus on addressing the perceived threats covered within the Slovakian security strategy, the defence strategy, the Slovakian Ministry of Foreign Affairs' strategy, as well as in the concepts for the protection of critical infrastructure. Further it shall also explore the interactions of different institutions in combating threats, as well as international crisis and conflict management (ICCM) within the security and defence strategy.

2.1.2 Key data about Slovakia

The SR is a subject of international law that emerged from the dissolution of the superordinate Czechoslovak state structure, the so called "Dismembratio"[162], and that shows several specifics regarding its territory, popula-

[162] Cf. Seidl-Hohenveldern, Ignaz: Die Staaten ()[The States], In: Neuhold, Hanspeter/Hummer, Waldemar and Schreuer, Christoph (Eds.): Österreichisches Handbuch des österreichischen Völkerrechts I. [Austrian handbook on the Austrian law of nations]Vienna 1997, p. 134ff, here p. 159.

tion, economics, membership in international organisations and armed forces.

Territory and population

Slovakia’s total territory covers 48,845km[163] with a 1611km-long state border and five neighbouring states. As of the 31st of December 2013, Slovakia had a total population of 5,415,949, of which 2,639,060 were male and 2,776,889 female.[164] Compared with its neighbouring states, the SR has the youngest population. The average age in Slovakia is 39.2, in the Czech-Republic 40.9, in Hungary 41.1 and 44.3 in Austria.[165] An additional characteristic of Slovakia is the relatively high amount of national and ethnic minorities, with the 458,467 members of the Hungarian minority constituting the numerically largest minority group.[166]

Economics and employment

Slovakia’s economic development in the recent years was highly influenced by the financial and economic crisis. While Slovakian economics increased strongly, up until 2008, the country had to face a 5.1% decrease in its economic performance in 2009.[167] Due to the economic crisis, unemployment increased as well, leaving approximately 386,000 people or 14% without

[163] Cf. Statistical Office of the SR. <http://portal.statistics.sk/showdoc.do?docid=65809>, accessed on 13.09.2014.

[164] Ibid.

[165] Cf. CIA: CIA Factbook: Slovakia, <https://www.cia.gov/library/publications/theworld-factbook/geos/lo.html>; Poland, <https://www.cia.gov/library/publications/the-world-factbook/geos/pl.html>; Czech Republic, <https://www.cia.gov/library/publications/the-world-factbook/geos/ez.html>; Hungary, <https://www.cia.gov/library/publications/the-world-factbook/geos/hu.html>; Austria, <https://www.cia.gov/library/publications/the-world-factbook/geos/au.html>; accessed on 15/11/2015.

[166] Cf. Statistical Office of the SR. <http://portal.statistics.sk/showdoc.do?docid=47949>, accessed on 13.09.2014.

[167] Cf. Statistical Office of the SR. <http://www.statistics.sk/pls/eutab/html.h?ptabkod=tsdec100>, accessed on 15/11/2015.

employment by the end of 2013.[168] The projections for the economic development 2015 were revised downwards with a growth of 2.6% after the outbreak of the conflict in the Ukraine and the EU sanctions against Russia.

Memberships of international/military organisations

International organisations have a central role in the security strategy and this is reflected in the defence strategy, as well as in the Slovakian Ministry of foreign affairs' strategy.[169] The Ministry of foreign affairs in Bratislava lists more than 30 international organisations with which Slovakia has established contractual relationships, although not being a member in all of them.[170] Essential for the Slovakian foreign and security policy processes are memberships of UNO, EU, NATO, OSCE, OECD, the Council of Europe and the Visegrad Goup.[171]

Armed forces and foreign assignments

In the years following the economic crisis the "Armed Forces of the Slovak Republic/Ozbrojené sily Slovenskej republiky" (OSSR) were greatly reduced, due to the decreased defence budget. Poor economic performance had immediate consequences on the military budget and therefore also on security policy measures. In 2012 the defence budget was cut by 19.3%

[168] Cf. Statistical Office of the SR. <http://portal.statistics.sk/showdoc.do?docid=67076>, accessed on 20.09.2014.

[169] Cf. Ministry of foreign affairs of the SR: Úspešné Slovensko v Bezpečnom svete – Stratégia MZV SR [A successful Slovakia in a Safe World – strategy of the Ministry of Foreign Affairs of the SR], p. 5. <http://www.mzv.sk/App/wcm/media.nsf/vw_ByID/ID_E64D391723AD1CCFC1257648004601A5_SK/$File/Strategia%20MZV%20definit%20260208.pdf>, accessed on 15/11/2015.

[170] Cf. Ministry of foreign affairs. <http://www.mzv.sk/sk/zahranicna__politika/medzinarodne_zmluvy-zoznam_podla_medzinarodnych_organizacii>, accessed on 15/11/2015.

[171] These organisations are the only ones listed in detail on the Ministry of foreign affairs' webpage. Cf. Ministry of foreign affairs. <http://www.mzv.sk/sk/zahranicna_politika/slovensko_v_osn-sr_v_osn>, accessed on 15/11/2015.

compared with the year 2008.[172] The OSSR's manning level in 2013 amounted to 15,850 persons in total, which was a decrease by 1279 persons compared with 2008.

In the second half of 2014, members of the Slovakian Armed Forces were on duty in UN peacekeeping operations as well as under the command of NATO and EU and participated in UNFICYP (Cyprus), UNTSO (Israel and Syria), ISAF (Afghanistan) and in the NATO staff in Bosnia and Herzegovina. As part of EU missions, Slovakian soldiers are involved in EUFOR ALTHEA (Bosnia and Herzegovina) and the EUMM in Georgia.[173]

2.1.3 Security policy concepts

In general the concepts developed for Slovakian security are characterised by different institutional and thematic settings of priorities. It is necessary to distinguish between whole-of-nation concepts and those documents that include institution-specific responsibilities. It should be noted that all measures derive directly or indirectly from the security strategy.

Systematics of "protective-strategies"

Basically the distinction of strategies between whole-nation approaches and "partially administrative" competences has proven to be useful, as Table 1. shows.

[172] In the Central-European context, an even bigger defence budget cutback was made in Hungary. In 2012 the Hungarian Ministry of Defence had a 27.1% lower budget at its disposal than in 2012. Cf. Báchora, Rastislav: Regionale Kooperationen als umfassende Security Provider? [Regional cooperations as broad Security Providers] In: Frank, Johann/Matyas, Wolgang (Eds.) Strategie und Sicherheit [Strategy and security] 2014. Vienna, Cologne, Weimar 2014, p. 327ff, here p. 329.

[173] Cf. Ministry of Defence of the SR. <http://www.mod.gov.sk/zahranicneoperacie/>, accessed on 15/11/2015.

<table>
<tr><th colspan="3">Whole-nation Strategies</th></tr>
<tr><td colspan="3">Security strategy of the SR (2005)[174]</td></tr>
<tr><td colspan="3">National strategy for information security in the SR (2008)[175]</td></tr>
<tr><td colspan="3">National anti-drugs strategy for the years 2013-2020 (2013)[176]</td></tr>
<tr><td colspan="3">Whole-nation strategy for the protection and promotion of human rights (Draft 2011, 2014)[177]</td></tr>
<tr><th>Exterior</th><th>Defence</th><th>Interior</th></tr>
<tr><td>The Ministry of Foreign Affairs' strategy (2008)</td><td>Defence strategy (2005)[178]</td><td>National action plan to combat terrorism (2005, 2006, 2007, 2011)[179]</td></tr>
<tr><td>The Ministry of Foreign Affairs's medium-term strategy until 2015</td><td>Doctrine of the armed forces (2009)[180]</td><td>National programme for the protection and defence of critical infrastructure (2007)[181]</td></tr>
<tr><td></td><td>The Ministry of Defence's planning model until 2015
(2010)[182]</td><td>Strategy for the prevention of crime and other actions against society for the years 2012-2015
(2011)[183]</td></tr>
</table>

[174] Cf. Ministry of defence of the SR. <http://www.mosr.sk/data/files/833.pdf>, accessed on 15/11/2015.

[175] Cf. Ministry of Finance of the SR. <http://www.informatizacia.sk/narodnastrategia-pre-ib/6783s>, accessed on 15/11/2015.

[176] Cf. Portal for the information on drugs. <http://www.infodrogy.sk/indexAction.cfm?module=Library&action=GetFile&DocumentID=1043>, accessed on 15/11/2015.

[177] Cf. Government council for Human Rights, national Minorities and gender balance. <http://www.radavladylp.gov.sk/celostatna-strategia-ochrany-a-podpory-ludskychprav-v-sr/>, accessed on 15/11/2015.

[178] Cf. Ministry of defence of the SR. <http://www.mod.gov.sk/data/files/832.pdf>, accessed on 15/11/2015.

[179] Cf. Ministry of Interior of the SR. <http://www.minv.sk/?akcny_plan>, accessed on 15/11/2015.

[180] Cf. Ministry of defence of the SR. <http://www.mod.gov.sk/data/files/831.pdf>, accessed on 15/11/2015.

[181] Cf. Ministry of Interior of the SR. <http://www.minv.sk/?ochrana-kritickejinfrastruktury>, accessed on 14.09.2014.

[182] Cf. Ministry of defence of the SR. <http://www.mod.gov.sk/data/files/834.pdf>, accessed on 15/11/2015.

[183] Cf. Government of the SR. <http://www.vlada.gov.sk/rada-vlady-sr-pre-

	White Book of defence (2013)[184]	Concept of combating extremism 2011-2014 (2011)[185]
		National action plan against human trafficking 2011-2014 (2011)[186]

Table 1: Systematisation of strategic documents
Ratislav Báchora

These security concepts can generally be labelled as "protective strategies", as they include governmental protective functions towards the citizens and the state. Among them are also those strategies that address specific threats and count as "traditional" security concepts in the narrow understanding of security. These include above all the security strategy and the defence strategy.

In accordance with the performance requirements of the Institute for Peace Support and Conflict Management's project, a study of the security concepts was conducted in regard to hybrid threats. Therefore the security strategy, the defence strategy, the Slovakian Ministry of Foreign Affairs' strategy, as well as the concepts for the protection of critical infrastructure, have been considered for the present analysis. The security documents are being analysed according to the analytical grid developed by Anton Dengg and Michael Schurian, in terms of three predetermined survey dimensions. These are:

prevenciukriminality>, accessed on 14.09.2014.

[184] Cf. Forum for international Politics. <http://www.mepoforum.sk/media/kniznica/kniznica/SR/Biela-kniha-o-obrane-SR-2013.pdf>, accessed on 14.09.2014.

[185] Cf. Ministry of Interior of the SR. <http://www.minv.sk/?dokumenty-nastiahnutie>, accessed on 15/11/2015.

[186] Cf. Ministry of Interior of the SR. <http://www.minv.sk/?dokumenty-nastiahnutie>, accessed on 15/11/2015.

(A) Perceived Threats;
(B) Operations and Interactions;
(C) International Conflict and Crisis Management.

The assessment whether the mentioned concepts include a "hybrid threat" is subject to different interpretation approaches. For that matter the definition by Anton Dengg, Walter Feichtinger and Michael Schurian from the Institute for Peace Support and Conflict Management (IFK), named "IFK-Definition" in the present analysis, represents the most important assessment framework.

2.1.4 Perceived threats

In the SR the defence strategy was adopted by Parliament on the 23rd of September 2005 while the security strategy was passed on the 27th of September 2005. Despite this inconsistency, both documents share coherent "perceived threats". While the defence strategy[187] lists threats, without further specifying them as to content, the security strategy deals with them more thoroughly.

Security strategy

The SR's security strategy, consisting of 83 paragraphs, covers altogether 16 threats, partly assuming different aggressive actors, but also unplanned incidents. In the present text the ranking and description of the threats is made in accordance with the listing in the original document. The objective is to explore the individual threats as to their content-related correlation with the determinants of the IFK-Definition for "hybrid threats". The threat numeration made follows the security strategy.

[187] Cf. Obranná stratégia Slovenskej republiky [Defence strategy of the SR], adopted by parliament on the 23rd of September 2005, chapter I.5: Slovenská republika v meniacom sa bezpečnostnom prostredí [The SR in a changing security environment].

Acquisition and use of weapons of mass destruction (WMD)

The acquisition and the use of WMDs are identified as the "biggest threats" within the strategy, as they are able to cause the "biggest harm" to the SR and its allies. Potential aggressive actors explicitly mentioned are terrorist groups, as well as "failed states".[188]

a.) Terrorism

Terrorism is declared as a "strategic global threat" and distinguished by ideological, ethnical and religious manifestations. Terrorism is aimed at "undermining democratic values" such as: "openness", "freedom of the individual" or "value of human life and tolerance".[189]

b.) Spreading of weapons of mass destruction

The SR regards the spreading of WMDs as a "global threat". The accessibility of those weapons for "states and non-state actors" poses a threat due to the "scientific and technological progress, the mobility of scientists, illicit trade with radioactive materials and dual-use goods [...]". In the context of the spreading of WMDs, the unregulated "proliferation of conventional weapons" is also labelled as a "serious problem".[190]

c.) "Failed States"

"Failed states" pose a threat on various levels, as they are "not capable or willing" to ensure the state's basic functions.

These include "their own security, as well as the observance of human rights", which is why they are becoming a "threat for their surround-

[188] Cf. Security strategy of the SR, chapter II, par. 17.
[189] Cf. ibid., Chapter II, par. 18.
[190] Cf. ibid., par. 19.

ings and contribute to regional conflicts".[191] This condition stimulates:

- Abuse of power;
- Hostilities between population groups;
- Suppression of democracy and civil society;
- Restriction of human rights and freedoms;
- Corruption and trafficking of humans, drugs and weapons.[192]

d.) Persisting regional conflicts

Regional conflicts are a threat to security in the Euro-Atlantic area and are mainly caused by armed national conflicts. Those conflicts are accompanied by:

- Extremism;
- Terrorism;
- Efforts to obtain weapons;
- Poverty;
- Mass migration;
- Organised crime;
- Weak economic development within the region.[193]

e.) Organised crime

Organised crime (OC) is considered a "direct threat" to the SR. Using modern technological equipment and means of communication, OC is trying to invade "all institutions of public life". A range of specific criminal activities by OC is listed below:

[191] Cf. ibid., par. 20.
[192] Cf. ibid.
[193] Cf. ibid., par. 21.

- Illegal production and distribution of drugs;
- Illegal migration;
- Human trafficking;
- Prostitution;
- Computer piracy;
- Intellectual property theft;
- Financial crimes.[194]

"International OC"[195] is labelled as the source for "financing personnel in terrorism", participates in the "spreading of WMDs" and exploits "regional conflicts" and failed states. Alongside the negative impact on the global economic system, it also causes a range of perceived threats for the state.

f.) Vulnerability of information- and communication-systems

As a result of information technology and modern means of communication, new types of threats emerge.

g.) Uncontrolled migration

The security strategy provides a general description of the threat emerging from uncontrolled migration from socioeconomically weak regions into the EU, leading to "populism and intolerance". Slovakia itself is declared as a transit country for migration, yet the security strategy assumes that the threat situation for Slovakia will increase in accordance with economic advancement. Various types of OC are related to illegal migration.[196]

[194] Cf. ibid., par. 22.

[195] The term "international organised crime" used in the strategy is usually called "transnational organised crime" in specialist literature.

[196] Cf. ibid., par. 24.

h.) Activities of foreign intelligence services

The activities of foreign intelligence services, using “traditional and non-traditional methods” and new technologies for their operations, present a constant threat for the SR. In particular the SR’s accession to NATO and the EU is seen as the cause of the expected increase of the threat situation.[197]

i.) Globalisation

Globalisation is responsible for both positive and negative consequences. An insufficient preparation for the effects of globalisation poses a “serious challenge for security”. Through globalisation the “margins between internal and external security” and between “domestic and foreign policy” become blurred. Explicitly mentioned are “globally operating economic operators that have a “growing influence on the worldwide development”, though they are not declared as a threat. “Information technology” and the “general access” to the Internet facilitate the “acquisition of weapon systems”, “operating instructions for their utilisation” and “plans to execute attacks”. Further “global financial markets” facilitate the movement of capital by terrorists.[198]

j.) Non-state actors

Directly interrelated with globalisation is the increase in non-state actors within the system of international relations, regarding the loss of the state’s monopoly position at ensuring security and the use of force.[199]

k.) Economic imbalance

The globally intensifying “social and economical differences between

[197] Cf. ibid., par. 25.
[198] Cf. ibid., par. 26.
[199] Cf. ibid., par. 27.

certain regions" result in "destabilisation and boost the emergence of security threats." The social divide in poor regions therefore causes the source of discontent and radicalisation and generates, according to the security strategy, the preconditions for:

- Extremism;
- Terrorism;
- Abuse of faith and traditions;
- Increase of religious fanaticism;
- Formation of authoritarian regimes;
- Illegal migration.[200]

Economic imbalance is not only regarded as the source for many wide-ranging threats, as it can further also have direct impacts on different socio-political areas.[201]

l.) The sense of identity loss

Due to the process of globalisation and labour migration, "feelings of threats to one's own living standard, culture and identity" arise within the population. Related to that is the rise of "radical nationalism and re-sentments" that are often backed by "political populism".[202]

m.) Growing demand for energy and raw materials

According to the strategy, a raw material and energy crisis will "presumably" arise and lead to further conflicts, due to the increasing consumption of raw materials, other vital resources and foodstuffs.[203]

[200] Cf. ibid., par. 28.
[201] Cf. ibid.
[202] Cf. ibid., par. 29.
[203] Cf. ibid., par. 30.

n.) Natural disasters

Natural environmental disasters, accidents and other disasters pose as a "permanent threat for life and property to a great extent", due to their non-predictability. Related to this are, among others, air pollution, the shortage of drinking water and the devastation of ecological systems.[204]

o.) Unbalanced demographic development

An unbalanced demographic development has adverse consequences for the "social security system", which could possibly lead to a "threat to the state's social stability". Therefore in this context migration is regarded as a factor for demographic development.[205]

The threats presented in the security strategy demonstrate a wide array of diverse challenges, where particular threats have to be distinguished by specific criteria.

Analysis

Summarising the particular threats in the Slovakian security strategy, they can be divided broadly into three categories:

a.) Threats originating from a deliberate, targeted action by a specific actor;

b.) Threats triggered by external processes, ostensibly not underlying a direct threat intention;

c.) National states of affairs or developments.[206]

[204] Cf. ibid., par. 31.

[205] Cf. ibid., par. 32.

[206] The categorisation of threats within the Slovakian security strategy, according to deliberate intentions, external and national processes, is based on the author's reflections.

a) Deliberate intentions	b) External processes	c) Internal processes
Acquisition and use of WMDs (1)	Failed states (4)	Vulnerability of information and communication systems (7)
Terrorism (2)	Persisting regional conflicts (5)	Sense of identity loss (13)
Spreading of WMDs (3)	Uncontrolled migration (8)	Unbalanced demographic development (16)
Organised crime (6)	Globalisation (10)	
	Economic imbalance (12)	
Activities of foreign intelligence services (9)	Growing demand for energy and raw materials (4)	
Non-governmental actors (11)	Natural disasters (15)	

Table 2: Classification of threats in the SR's security strategy
Rastislav Báchora

It is in the nature and characteristic of the threats that a clear differentiation, correspondent to the categorisation posed (Table 2.), cannot be made, albeit singular actors can be identified who could take corresponding threat actions according to the security strategy. Those actors are therefore the "link" to hybrid threats.

According to the IFK-Definition a hybrid threat exists if it originates from an actor's intention. Further the actor has to be capable of using his endangerment potential in multiple security-relevant dimensions. In the IFK-Definition, an aggressive actor can take "political", "economic", "military", "social" or "medial" actions to disturb security.

The naming of actors from which targeted security threats emerge is therefore the basis of recognising hybrid threats. The Slovakian security strategy names actors who pose diverse threats or who, according to the IFK definition, would have the "ability" to direct their "potential" "multidimensionally" against the SR's security strategy. These actors named in the security strategy can be called aggressive actors and are as follows:

- Terrorist groups (threat 1, 2, 4);
- States and non-state actors (threat 3);
- Terrorist and extremist groups and networks (threat 4);
- OC groups (threat 6);
- Foreign intelligence services (threat 9);
- Globally operating economic operators (threat 10);
- Non-state groups, organisations and networks (threat 11);
- Populism and nationalism by political groups (threat 13).

Basically two conclusions can be drawn from the depiction of the threat and the actors' situation: firstly all of the actors named in the security strategy could theoretically have the potential to launch activities pursuant to the IFK definition of hybrid threats. The security strategy itself though, does not cover them with the appropriate extent and depth. Secondly, those threats that are based on a targeted intention can be interpreted as "hybrid threats". Therefore four threats can be identified as "hybrid":

- Acquisition and use of WMDs;
- Terrorism, Spreading of WMDs;
- Organised crime;
- Foreign intelligence service activities.

Although in the security strategy non-state actors are regarded as a threat of their own, they make for a constant part within the framework of other threat patterns and are therefore not quoted separately. Applying a strict interpretation of the IFK definition's text and its operational application on the Slovakian security strategy, it can be stated that the threats through terrorism and OC are the ones matching the substantial definitions of the given "hybridity" the most. The extent to which the threats covered by the strategy can be labelled as "hybrid" depends also on the security concept as well as the methodological and analytical approaches of the observer. Therefore objective criteria have to be set through a further scientific procedure.

The Ministry of Foreign Affairs' strategy

Basically the Ministry of Foreign Affairs in Bratislava has a broad scope of influence regarding strategic questions within the security policy. Therefore the Ministry of Foreign Affairs' strategy from 2008, named "A Successful Slovakia in a Safe World", has to be considered in regard to the security policy challenges covered.

Overall the strategy defines four "strategic priorities". These are the areas of security, economy and regional matters, EU agenda and citizen service. Although the foreign policy strategy does not describe any threats in detail (as in the security strategy), they are however listed in the context of security-policy prioritisation. Specifically the EU and NATO are presented as the crucial frames for the structuring of Slovakia's international relations. In the chapter "Strengthening of security in the Euro-Atlantic area", the priority of "counteracting crisis and conflicts and facing the challenges and potential threats in the Euro-Atlantic Area" is presented.[207] In the chapter "Fighting global challenges and threats", fighting against terrorism, WMDs and OC are named as priorities.[208] Though the Ministry of Foreign Affairs' strategy does not specify any threats, it does confirm the security strategy's perceived threats.

Protection of critical infrastructure

The protection of critical infrastructure is not ascribed with any special priority within the Slovakian security strategy. Overall critical infrastructure is briefly mentioned three times, twice in the context of fighting terrorism and one time specifically upon the measures to increase information security.[209] However, within the security strategy, conceptual, administrative and

[207] Cf. Ministry of foreign affairs: strategy of the Ministry of foreign affairs, chapter 5: Strategické ciele [strategic objectives].

[208] Stratégia MZV SR - Úspesné Slovensko v bezpecnom svete [strategy of the Ministry of foreign affairs of the SR – A successful Slovakia in a Safe World], chapter 5.1.3: Bojovat proti globálnym výzvam a hrozbám [fighting global challenges and threats].

[209] Cf. security strategy of the SR, chapter II.18, Chapter III.44 and Chapter III 49.

legislative follow-up processes are being announced. Thus the "Concept of Critical Infrastructure in the SR and Method of its Protection and Defence" was drawn up in 2006. Already in 2007, the "National Programme for Critical Infrastructure Protection and Defence" was adopted by the government and therefore represents a central concept.[210] Further, relevant textual aspects were also included in the information strategy 2010. Finally, important parameters were established by law in the "law on the protection of critical infrastructure", which is fundamentally based on the operational programme 2007. According to this "National Programme", critical infrastructure is:

> "[...] that part of national infrastructure (selected organisations and institutions, buildings, sites, facilities, services and systems), whose destruction or functional impairment as a consequence of a risk factor causes a threat or a harm to the political or economical progress of the state or a threat to the lives and the health of the population"[211]

The protection of critical infrastructure is the responsibility of several "subjects":

- International partners and international organisations;
- Government and public administration;
- Regional authorities and institutions of self-government;
- State-run economic subjects;
- Private economic subjects.[212]

Within the programme, critical infrastructure facilities were divided into nine different sectors:

[210] Cf. Ministry of the Interior of the SR. <http://www.minv.sk/?ochrana-kritickejinfrastruktury>, accessed on 30.09.2014.

[211] Ministry of the Interior: Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [National programme for Critical Infrastructure Protection and Defence of the SR], Introduction 2007. <http://www.minv.sk/?ochrana-kritickej-infrastruktury>, accessed on 30.09.2014.

[212] Cf. ibid., Chapter 2.1: Aktuálny stav ochrany kritickej infraštruktúry v Slovenskej republike [actual situation of the protection of critical infrastructure in the SR].

- Water;
- Foodstuffs;
- Health;
- Energy industry;
- Information and communication technology;
- Transport;
- Public order and internal security;
- Industry;
- Financial sector.[213]

The central coordinating tasks for the protection of critical infrastructure apply to the Ministry of Interior, whilst the "National Programme" lists nine ministries in total that are conceptually and institutionally involved in the realisation of protective measures. Among them are also the ministries responsible for the primary security policy issues, the Ministries of Foreign Affairs and Justice. The interior intelligence agency is also cited separately.[214]

Terrorism and also disasters are explicitly emphasised as threats against which critical facilities have to be protected.[215] Terrorism can also be declared as a hybrid threat with regard to the concepts to protect critical infrastructure.

2.1.5 Operations and interactions

To combat nearly all kinds of threats, national and international mechanisms are necessary and require a specific degree of cooperation between different public administration institutions adapted to the specific kind of threat. The institutional cooperation on combating threats includes non-governmental groups as well as groups from the civil society and also commercial groups. The extent to which these interactions are

[213] Cf. ibid., Chapter 3.1 – 3.9.

[214] Cf. ibid., Chapter 4: Úlohy zainteresovaných subjektov [responsibilities of the interested subjects].

[215] Cf. ibid., Chapter 2.1.

conceptualized in the SR’s security strategy is analysed in terms of three essential aspects:

a.) Cooperativeness between government agencies;
b.) Security cluster approaches;
c.) Mutual situation assessments and mutual situation overview.

Cooperativeness between government agencies

Maintaining or creating security is the duty of security policy which, according to the Slovakian security strategy, is based on the “security system”. The “security system” is a “multifaceted complex” and includes the instruments of foreign policy, economy, defence, domestic policy, social security system, emergency services and environment protection facilities.[216] The state’s instruments for combating threats are marked as “traditional means” and are as follows:

- Foreign intelligence service;
- Armed forces;
- Security intelligence (domestic);
- Police;
- Judiciary guarding personnel;
- Customs administration;
- Fire brigade;
- Rescue institutions;
- Mining rescue services;
- High mountain range rescue services;
- Subjects of economy;
- Subjects of the financial market;
- Institutes responsible for data protection.[217]

[216] Cf. Security strategy of the SR, Chapter III.37: Bezepečnostná politika Slovenskej republiky [security policy of the SR].

[217] Cf. ibid., Chapter III.39.

In addition to a coordinated use of state instruments in fighting threats, there is also cooperation with other state and non-state actors on a national and international level. In concreto, the security strategy states that the security policy is carried out within the framework of set structures and means. This framework is as follows:

- UNO;
- EU;
- NATO;
- OSCE;
- Council of Europe;
- Visegrad Group;
- Central European Initiative;
- NGOs;
- International agreements and contracts;
- Norms and standards;
- Media.[218]

Especially the combating of hybrid threats, i.e. those threats that are based on intentional acts, calls for a conceptually set cooperation between different government agencies. Table 3 shall take a closer look at the means of combating against those intentionally generated and targeted threats within the security strategy.

[218] Cf. ibid., Chapter III.40.

Hybrid threat (intentional)	Defence cooperation
· Acquisition, spreading and use of WMDs	· International norms · Sanctions · Armament exports control · Cooperation with NATO and EU (par. 45)
· Terrorism	· Intelligence agencies · Special departments of law enforcement agencies · Coordination with foreign partner services · Disarming of terrorists using the military (par. 44)
· Organised crime	· Strengthening legal, economical and medial parameters · Preventive and repressive measures: intelligence services, police, public prosecution department, courts (par. 48)
· Activities of foreign intelligence services	· Increased information protection through the intelligence services and increased cooperation with partner services from NATO and EU countries (par. 51)

Table 3: Cooperation in combating hybrid threats
Rastislav Báchora

International organisations play an important role at combating threats. Looking at (potential) hybrid threats separately, the EU and NATO represent an essential scope of action for the Slovakian security policy.

Security cluster approaches

From the interpretation and assessment of the conceptual approaches within the security strategy, it follows that, on the one hand, they include a wide range of cooperation between institutions but, on the other hand, no cluster-conjunctions are applied, in the proper sense of state-administrative instruments, in combating specific threats.

The strategy's measures express that the security system is composed of all subcomponents of the public administration and coordinated by the government. The responsibility for the coordination of the security tasks on the highest decision level lies in the hands of the government's security council, whose function and tasks are however not mentioned at all in the security strategy. Thus a substantial coordinating body, operatively and conceptually combining institutional cluster approaches within the design of the Slovakian security system, is not addressed in the security strategy. This is particularly unusual since, according to the law on the "Governance of the state in crisis situations outside the framework of war and the state of war", the security council is assigned to central leadership tasks in times of peace.[219] Yet the security council does also perform central leadership tasks in states of emergency and war.[220]

Joint situation assessment and situation overview

A joint situation assessment, as well as a joint situation overview in terms of a whole-nation, cross-institutional, systematic presentation of the threats and assessments of their impact on the SR's security strategy, are nonexistent in the concept of the security strategy.

[219] Cf. Government of the SR, law 387/2002: O riadení štátu v krízových situáciách mimo času vojny a vojnového stavu [Governance of the state in crisis situatios outside the framework of war and the state of war], §3. <http://www.vlada.gov.sk/data/files/4373_387.pdf>, accessed on 15/11/2015.

[220] Cf. Government of the SR: Štatút Bezpečnostnej rady Slovenskej republiky [Statute of the security council of the SR], No.2. <http://www.vlada.gov.sk/bezpecnostna-rada-sr/>, accessed on 15/11/2015.

Contributing to the situation assessment of the foreign context, as well as to the situation overview for the interior are, amongst others, the intelligence services, who are pointed out in multiple passages in the text. Especially the assessment of developments in foreign countries and possible impacts on interior security are made primarily within the frameworks of NATO and the EU. Within the document itself, influence on the exterior scope is particularly pointed out, while situation assessment is neglected.[221] According to the security strategy, the memberships of NATO and the EU have a significant influence on the assessment of security-policy developments and influence the ICCM.

2.1.6 International conflict and crisis management

The emphasis at presenting the ICCM is set on foreign assignments and, at the same time, the security strategy and the defence strategy are considered as well.

ICCM in the security strategy

Central to ICCM is the participation of the Slovakian armed forces in foreign assignments, which is interpreted as a contribution to ensuring interior security and as an obligation through the alliance with NATO and the EU. Further the operations within the framework of the UNO conceptually also play an important role. In general the military ICCM engagement involves the sending of troops to actual crisis regions, as well as to post-conflict areas. At the implementation of measures against the threats, in the case of weak states, the security strategy plans for cooperation between military and civil forces within the framework of development assistance.[222] It is emphasised in multiple passages that the ICCM has to take place within the framework of NATO and EU.

[221] Cf. Security strategy of the SR, Chapter III.60.

[222] Cf. Security strategy of the SR, Chapter III, par. 47.

Thus the objective is, among others, to strengthen the EU's "operative capacities".[223]

In regard to specific threats on foreign assignments with interdependent effects on the homeland, the document establishes neither any conceptual nor any operative correlations that are relevant for administrative-institutional follow-up processes. Thus the ICCM in the SR's security strategy is rather characterised through general foreign policy and security policy positions. Thereby the relevance of the armed forces for the ICCM is emphasised and dealt with further in the defence strategy.

ICCM in the defence strategy

As in the security strategy, a stronger involvement in foreign missions within the framework of NATO and the EU is also emphasised in several passages of the defence strategy. More detailed information on the military ICCM is given in the chapter "Defence Requirements of the Slovak Republic". Within this chapter, a protection of the citizens and the state is emphasised, which also conceptually provides for the use of military means against terrorism in foreign countries.[224] In addition, according to the defence strategy, armed forces can be used against the spreading of WMDs and for the regulation of conflicts in crisis regions.[225]

Within the scope of the ICCM, the use of armed forces against terrorism is regarded as "most probable", which reveals the special hybridity of this threat and the corresponding perception in Slovakia.[226]

[223] Cf. ibid., Chapter III, par. 69.

[224] Cf. Obranná stratégia Slovenskej republiky [defence strategy of the SR], adopted by parliament on the 23rd of September 2005, Chapter III: Požiadavky na obranu Slovenskej republiky [requirements to the defence of the SR], par. 18.

[225] Cf. ibid., par. 20.

[226] Obranná stratégia Slovenskej republiky [defence strategy of the SR], adopted by parliament on the 23rd of September 2005, Chapter III, par. 26.

Regarding foreign assignments, the implication of NATO standards is explicitly demanded, with the training and preparation for foreign assignments having to be made in close cooperation with the partners.[227] In this context it becomes evident that the conceptual and operative design of the ICCM was adapted to the priorities of NATO and, in second place, to the EU.

Any conceptual and/or operative approaches for special precautionary measures in regard to interdependent effects between the place of action and the homeland were not included in the defence strategy, as they were not included in the security strategy. Thus the threat through terrorism and the spreading of WMDs remains the principal type of threat which, within the ICCM's framework, should be combated by military force. Due to the conceptual mission planning in the ICCM area, which emphasise terrorism as well as the spreading of WMDs, it is legitimate to speak of hybrid threats.

2.1.7 Conclusions

The principal conclusion is that the identification and particularly the conceptual and, in further consequence, also the administrative-institutional operative handling of security requirements in general and hybrid threats in particular, depend on the concept of security. In the case study of Slovakia, the citizens' security and the security of the state are equally prioritised in the security strategy's conceptual threat presentations. As a result, socio-political subject areas like "economic imbalance", "fear of identity loss" or "demographic imbalance" are linked in terms of security policy and conceptualized as threats for security. Regarding specific hybrid threats according to the "IFK operational definition" by Anton Dengg, Walter Feichtinger and Michael Schurian in the SR's security concepts, it can be concluded that the documents generally have to be adapted to a modern understanding of threats. Although threats originating from a targeted inten-

[227] Cf. ibid., Chapter IV: Rozvoj ozbrojených síl [development of the armed forces], par. 41.

tion of doing harm from one or more actors are being described, they are not systematically conceptualized as such and dealt with additionally.

It does not operatively distinguish between an intentional hybrid threat such as terrorism, the spreading of WMDs or OC on the one hand, or the more "process resultant" undefined threats like globalisation, weak states, migration etc. on the other hand. Though it does indeed list actors who have the potential of being the source of hybrid threats, they are consistently not explicitly classified as such. A precise characterisation of threats would inevitably also specify the administrative-institutional combating measures and lead to a better clarification of the administrative competences.

The security strategy clearly shows a crucial weakness in the field of illustrating conceptual and operative cooperation of institutions in combating threats, as well as within the ICCM. Thus for example the defence strategy – as well as the security strategy - completely disregards interdependent effects between threats at the place of action and in the homeland, although fighting terrorism and the spreading of WMDs by military means within the framework of foreign missions is provided conceptually. In general it has to be weighed as positive that specific sub-strategies for different administrative areas were created on the basis of the security strategy, but they are consequently not oriented towards the perceived threats.

In conclusion three crucial deductions can be made:

(1) A comprehensive conception of hybrid threats is primarily the result of a modern perception of security policy challenges.

(2) The analysis of threats in security concepts and their evaluation whether a hybridity in terms of the IFK-Definition exists, is subject to a certain range of variation. Variable interpretations are primarily the result of an insufficient state of research.

(3) General and generalisable statements about hybrid threats and their embodiment in security policy concepts require a further discussion process including expert groups from the fields of politics, science and sociology.

2.2 Sweden

Michael Fredholm

Explanatory note: the opinions expressed herein are exclusively those of the author and do not necessarily represent those of the Swedish government

Population:	9,684,858 (31/05/2014)[228]
Area:	528,447 km^2 [229]
GDP per capita:	SEK 379,300 (2013)[230]
Projection of economic growth:	N/A.
Membership in international organisations (military organisations):	EU (since 1995)
Size of armed forces:	19,995, additional to 20,596 in Home Guard units (31/12/2013)[231]

Table 4: Basic information about Sweden
Michael Fredholm

2.2.1 Perceived threats

Landscape of concepts

Sweden has not published any security relevant concepts. It is lacking a national security concept, as well as a foreign policy concept.

There is also no authorised security strategy or defence strategy. There is not even a white book or a green book dealing with national security. Threats are usually not faced with published concepts, but rather pragmatically, depending on the specific situation. Coming closest to a security concept is the Military Strategic Doctrine (MSD 12), issue 2012, being the only

[228] Statistics Sweden, <www.scb.se>.

[229] Ibid.

[230] Ibid.

[231] Website of the armed forces, <www.forsvarsmakten.se>.

document mentioning hybrid warfare and hybrid threats as a concept. The Military Strategic Doctrine's priorities are primarily relevant for international operations and ICCM. In reality, the Military Strategy Doctrine is probably not oriented towards territorial defence.[232]

The concept of hybrid power projection or of hybrid threats is not addressed much in Sweden, one of the reasons being the military planning process. Since hybrid warfare covers effectively everything from conventional warfare to terrorism to organised crime and cyber threats, it is difficult for the armed forces to plan their strength and size for such threats. Furthermore the Swedish armed forces lack the ability to react properly to the many types of hybrid threats. Many domestic threats have to be dealt with by other Swedish authorities, such as the police while, in an international context, they have to be mastered together with other states or organisations.

The Military Strategic Doctrine (MSD 12) only briefly and without details mentions hybrid warfare and hybrid threats as a concept of modern warfare:[233]

Because of the difficulty of making a clear distinction between irregular and regular warfare and the realisation that the simultaneous application of both types of use of force will pose a constantly growing challenge in the future, the term of "hybrid warfare", also expressed as "hybrid threat", becomes more frequently used. Basically it is a concept in which actors, regardless of their status, have access to regular military capabilities as well as to the whole spectrum of the use of force, which are usually related to irregular warfare (an example of hybrid warfare is the war of the Hezbollah against Israel in 2006).[234]

Hybrid warfare is understood to be that warfare which combines different strategies, tactics and fighting methods within the same conflict (area). It

[232] The Swedish government on 25 June 2015 issued a directive on a reinforced focus on territorial defence in the period 2016 to 2020.

[233] The main proponent of this concept within the armed forces is Dr. Håkan Gunneriusson at the defence university in Stockholm.

[234] Armed forces, Military Strategic Doctrine with doctrinaire reasons. Editione 2012, M7739 354023, p. 29. Translated from the Swedish language.

takes account of the effects of globalisation: communication has become more important and qualified weapon systems are easier to acquire. Hybrid warfare can be regarded as a further development of the concept of “irregular warfare” with the increased usage of modern technologies. It requires the ability of regular and irregular, but also unconventional warfare.[235]

Special operations keep up with the increased relevance of counterinsurgency, with irregular and hybrid warfare steadily gaining significance.[236]

However, for international operations, the armed forces require the competence to cooperatively face irregular enemies and hybrid threats and additionally also the competence for regular warfare. This regular warfare is necessary in a wide range of operations, regardless of the type of enemy.[237]

Furthermore, Sweden is not very well positioned in terms of its operative whole of government approach in an institutional context – as far as this is known from public information. Several Swedish ministries, departments and authorities are responsible for the protection against hybrid threats and the defence against them. Yet those authorities are independent of each other and not fully coordinated.

Identifying possible hybrid threat actors

In the public debate, Sweden has not identified any actual enemies with the capability of hybrid power projection.

However there are foreign state actors such as foreign intelligence services (for example in Russia; see appendix North Stream Project, Chapter 5.1) and non-state conflict actors in Sweden (in terrorism and in organised crime) who have potential capacities.

[235] Ibid., p. 29. Translated from the Swedish language.
[236] Ibid., p. 30. Translated from the Swedish language.
[237] Ibid., p. 134. Translated from the Swedish language.

When performing international missions in failing states or in regional conflicts, Sweden is also confronted with insurgents and terrorist groups that use hybrid threats (for example in the case of Afghanistan; see appendix).

The use of Weapons of Mass Destruction (WMD) by terrorists and IT-threats have also been identified as potential hybrid threats, although this is not mentioned in all official documents. Perhaps extremist actors and international terrorism such as Al-Qaeda can be included in this group.

Protection of critical infrastructure

The Swedish assessment of threats regarding critical infrastructure is developed multidimensionally. There are several national cooperation projects for the protection of critical infrastructure. However, there are no security concepts mentioning hybrid threats.

One of the important actors is the Swedish Civil Contingencies Agency (MSB).[238] The MSB's duty is the improvement of social capacities and assisting preparation for and prevention of emergencies and crises.

Further important actors are:

- The Counter-Terrorism Co-operative Council
- The National Centre for Terrorist Threat Assessment (NCT)
- The cooperation project “National Cooperation Council against Serious IT Threats” (NSIT)
- The cooperation project “National Cooperation Council against Serious IT Threats” (NSIT)
- The Cooperation Project against Hazardous Substances (SOFÄ)

[238] Myndigheten för samhällsskydd och beredskap, <www.msb.se.>.

The Counter-Terrorism Co-operative Council is a partnership between fourteen Swedish authorities with the objective of strengthening Sweden’s ability to combat terrorism. The Council held its first assembly in February 2005. The Council is chaired by the Director-General of the Swedish Security Service. Also represented on the council are the highest officials of the national police, armed forces, intelligence services, Civil Contingencies Agency (MSB), coastguard, customs, radiation protection and so on.[239]

Serving under the Counter-Terrorism Co-operative Council is the National Centre for Terrorist Threat Assessment (NCT). The NCT consists of representatives of the intelligence services and the security service. The duties of the NCT involve the creation of strategic analyses about incidents, trends and external developments in the context of terrorism, that affect or could affect Sweden or Swedish interests.[240]

The cooperation project “National Cooperation Council against Serious IT Threats” (NSIT) is a cooperation between the Security Service, the armed forces and the intelligence services. The cooperation project held its first session in December 2012. NSIT analyses and assesses threats and weaknesses and takes precautionary measures in cases of severe or qualified IT threats against the most important national interests.

Expert groups work on specific projects. The tasks are executed on behalf of the particular agencies and do not include any additional powers. NSIT does not act against cyber criminality such as financial fraud or *distributed denial-of-service* (DDoS) attacks against websites.[241]

[239] Samverkansrådet mot terrorism, Counter-Terrorism Co-operative Council: Website of the Security Service, www.sakerhetspolisen.se; Säkerhetspolisen, Årsrapport 2013, p. 15.

[240] Nationellt centrum för terrorhotbedömning, National Centre for Terrorist Threat Assessment: Website of the Security Service, <www.sakerhetspolisen.se>.

[241] Samarbetsprojektet Nationell samverkan till skydd mot allvarliga IT-hot: website of the MSB. < www.msb.se>; Säkerhetspolisen, Årsrapport 2013, p.12.

Serving under the MSB is the Cooperation Group for Information Security (SAMFI), a partnership between the national police, the Security Service, the armed forces, the intelligence services and so on.[242]

Also below the MSB is the Cooperation Project against Hazardous Substances (SOFÄ). This cooperation project is just a national forum and a reference group without additional powers, though it is an important expert group and plays a part in preparedness.[243]

Nevertheless, these different agencies are independent of each other and are not coordinated. Furthermore, their areas of responsibility are highly limited and they are not in control of the activities within their area. In the institutional context, there is no permanent inter-ministerial task group, there are only cooperation projects; in times of crisis temporary task groups are called in on an *ad hoc* basis (see appendix on the North Stream Project, chapter 5.1).

A further aspect in the protection of critical infrastructure is energy security. Sweden depends on imports of petroleum and petroleum products. Oil companies, large scale industry and power plants are required to ensure the emergency supply of crude oil and petroleum products in quantities that correspond to 90 days of normal consumption. The EU and the International Energy Agency (IEA) will decide the use of that emergency supply on the basis of international treaties. In the event of a crisis, these organisations will allocate the petroleum between the member states. Sweden does not exercise an independent control of this central crude oil storage.

Since Sweden consumes scarcely any natural gas, there are no similar precautions for emergency natural gas storage.[244]

[242] Samverkansgruppen för informationssäkerhet: website of the MSB, <www.msb.se>.

[243] Samverkansområdet Farliga Ämnen: website of the MSB, <www.msb.se>.

[244] Statens energimyndighet: Hur trygg är vår energiförsörjning? En översiktlig analys av hot, risker och sårbarheter inom energisektorn 2006 (Eskilstuna: Statens energimyndighet, Reference ER 2007:06, published 2007), p. 23 and 25.

2.2.2 Operations and Interactions

Cooperativeness between governmental authorities

The orientation of Sweden's security policy is characterised by a strong culture of cooperation. The domestic actors are forced to cooperate and to find a consensus. However it is not much developed in its whole-nation institutional context and the formal-structural cooperation between ministries is not very strong – as far as it can be assessed. Yet Sweden does have an actual whole-nation approach in national cooperation projects. This approach is shaped pragmatically and functionally, but it is not operationalised. In the event of an actual crisis, the cooperation would depend on practical and *ad hoc* approaches.

However, there is indeed cooperation. Ministries are bound by administrative law to cooperate with each other.[245] But there are only a few formalised intersection points for a joint situation assessment, should protective measures be required.

The actual willingness to cooperate cannot easily be assessed. Since there are only a few documents on this topic, pragmatic approaches are necessary. Practical experience with historical crises shows that cooperation will take place, though there are only a few formal preparatory arrangements between the relevant actors.

Security Cluster Approaches

In Sweden several different ministries, departments and authorities are responsible for protection against hybrid threats and, in the case of their deployment, also for defending against them. However, these authorities are independent and not fully coordinated, although they are obliged to cooperate. Furthermore their areas of responsibility are highly limited and they exert no actual control over the activities within their area.

[245] (Swedish) administrative law from 1986, § 6.

A usual approach is, as always, based on pragmatic *ad hoc* solutions. This would also allow for supporting the armed forces and, in return, getting support from other emergency organisations such as the police and the coast guards. Unfortunately the seeking of *ad hoc* solutions of course means that the security cluster approaches are not well established.

Intersection points between state and non-state actors

Intersection points between state and non-state actors are, as far as it can be assessed, not strongly defined or developed today. Exercises, like those common during the Cold War, take place rarely or not at all.

Joint situation assessment

A nationwide threat analysis, based on a w*hole-nation* approach, with a joint situation overview and a joint situation interpretation of state and non-state actors, is missing – as far as can be assessed – in many areas of responsibility. However, Sweden has an actual whole-nation approach in national co-operation projects, such as the projects regarding the protection of critical infrastructure. Hence relevant whole-nation elements can be identified in Sweden, but they are not institutionally manifested. Institutional structures for a joint situation assessment are missing.

Joint protective measures

Since a whole-nation threat analysis is lacking in most cases, joint protective measures cannot be very strong – as far as can be assessed.

2.2.3 ICCM

Interdependent effects regarding ICCM involvement in the operational area

In the operational area, only the armed forces have knowledge of a concept of hybrid power projection, which is however limited to warfare. The possibility of a hybrid threat within another range of responsibilities in the operational area has barely been identified, but it does exist (for example in Afghanistan; see appendix).

The Military Strategic Doctrine (MSD 12), which is *de facto* mainly relevant for international missions (and possibly only *de jure* germane to territorial defence), mentions hybrid warfare and hybrid threats as being relevant in the operational area.

However, for international missions, the armed forces need to have the ability to face irregular enemies and hybrid threats in cooperation with others, in parallel with the ability to conduct regular warfare. This regular warfare is necessary to different extents, regardless of the type of enemy.[246]

The phrase “in cooperation with others” has a pragmatic meaning in this context. In this way, for example, Sweden’s willingness to join ICCM missions in close connection to NATO is possible.[247]

Interdependent effects regarding an ICCM involvement in the sending state

The possibility of a hybrid threat in the sending state, as a reaction to the involvement in ICCM is – as far as can be assessed – rated as not pressing. But there are such possibilities, as explained in the appendix on Afghanistan.

Integration in security organisations

Considering the few existing documents on hybrid threats, it is hard to assess whether Sweden rates the protection against hybrid threats primarily as a national or an international duty. Sweden’s traditional non-aligned status and policy of neutrality make the assessment yet more difficult. As mentioned, the Military Strategic Doctrine (MSD 12) considers preparedness for ICCM, for example in close collaboration with NATO or other

[246] Armed forces, Military Strategic Doctrine with doctrinaire reasons. Editione 2012, M7739 354023, p. 29. Translated from the Swedish language.

[247] For a discussion see Gauster, Markus: Whole of Nation Ansätze auf dem Prüfstand. Ein neues Paradigma im internationalen Krisenmanagement? []Whole-of-nation concepts on trial. A new paradigm in the international crisis management?] Vienna 2013, p. 67ff.

security organisations. It can however be evaluated that the identification and mastering of hybrid threats is primarily seen as a national duty in Sweden.

2.2.4 Conclusions

The concept of hybrid power projection or hybrid threats is not addressed strongly in Sweden – as far as it can be assessed. In large part, this can be explained through Sweden's lack of willingness to phrase formal strategy documents for the non-military area. The concept therefore increases the difficulties for the armed forces.

Since hybrid warfare involves everything from conventional warfare to terrorism to organised crime and cyber threats, it is difficult to plan the prospective strength and size of armed force for these threats. Furthermore the Swedish armed forces lack the ability to react properly to all the various kinds of hybrid threat without the assistance of other emergency organisations.

In Sweden several different ministries, departments and authorities are responsible for protection against hybrid threats and, in the event of their deployment, also for defending against them. The formal-structural cooperation between ministries is not very strong – as far as can be assessed - yet Sweden has an actual whole-nation approach in national cooperation projects and a traditional culture of cooperation. This approach arises from the typical Swedish consensual orientation; but it is not operational. Furthermore the authorities are independent and not fully coordinated. Even so their areas of responsibility are highly limited and they are not in control of the activities within their area.

So far, Sweden has not publicly identified any enemies with the capability of hybrid power projection. However, there are foreign state actors (for example Russia) and non-state conflict actors in Sweden (terrorism and organised crime) with the potential capacity. In ICCM the possibility of a hybrid threat was also rarely identified, but it does exist (as for example in the case of Afghanistan).

3 Supplementary Analysis in the Context of Hybrid Threats

3.1 Hybrid threats: reflecting on deductions from EU strategic documents

Gerald Brettner-Messler

"Hybrid" means "composed from different types, mixed". So a hybrid threat is one that is composed of different elements that are (or can be) used in concert. This description aims to lay out a significant aspect of today's threat situation. The diverse possibilities and their use by particular adversaries of the rule of law and the societal system of the European Union should be clearly identified by this new term, with a view to combating them appropriately. But is there actually any mention of hybrid threats in the strategic documents of the Union?

The central paper is the European security strategy (ESS), which was adopted during the session of the Council of the European Union on December 12th 2003. The important challenge, following the attacks of September 11th 2001 in New York and Washington, was the fight against terrorism. In 2004 a "strategy against the financing of terrorism" was presented. A year later, following the attacks in Madrid in 2004 and London in 2005, came the "EU counter-terrorism strategy" and the "strategy for combating radicalisation and recruitment for terrorism".[248] Also presented in 2005 was the "strategy on the external dimension of the area of freedom, security and justice". Technical development received due attention in 2006 with the "strategy for a secure information society".

[248] Regarding terrorism and EU see: Hauser, Gunther: Europa und der Kampf gegen den Terrorismus [Europe and the fight against terrorism]. In: Hauser, Gunther/BrettnerMessler, Gerald (Eds.): Sicherheit und Recht zu Beginn des 21. Jahrhunderts [security and law at the start of the 21st century]. National Defence Academy publication series 8/2007. Vienna 2007, p. 11ff.

In 2008 the “report on the implementation of the ESS” was presented, which dealt with ESS points in updated form. In 2010 the “EU internal security strategy” followed.[249]

3.1.1 Theoretical consideration of the term “hybrid threat/warfare”

The term “hybrid threat/warfare” appeared no later than 2002 in US military technical publications.[250] It took some time for discussion thereof to reach Europe; even today, it is not really fully engaged. There is mention in an article of 2012 that it had only just begun in Germany.[251] Correspondingly, this form of threat is also not explicitly mentioned in current documents. This is true not only for the EU. NATO’s strategic concept of 2010 is equally silent on hybrid threats. Threats (terrorism, cyber-attacks, proliferation of weapons of mass destruction etc.) are mentioned but no synopsis is applied, resulting in no statement about what it means if several threats arise simultaneously in a targeted manner or what can be deduced from such simultaneity. Yet this factor is very important for characterising a threat as “hybrid”. Michael Miklaucic is of the opinion that hybrid threats are more than the sum of individual threats. He also underlines that it is not a matter of the mere chance simultaneity of threats, but rather about their systematic application to the achievement of objectives. Therein lies the distinction: the threats themselves are not at all new, but the novelty lies in their combination. It is important to note that this is not merely about non-state adversaries; the threat can also, though doesn’t have to, come from a state.

[249] There is also a series of other documents that deal with the EU’s stance with respect to security. Those listed above are the central papers on the topic; the list is not exhaustive.

[250] See: Hoffman, Frank G.: Hybrid Threats: Neither Omnipotent nor Unbeatable. In: Orbis, Vol. 54, Issue 3, 2010, p. 441-455. According to Hofmann, one of the first pieces of work on this topic: Nemeth, William. J.: Future War and Chechnya: A Case for Hybrid Warfare. Monterey, CA, Naval Postgraduate School, June 2002.

[251] Oprach, Marc: Hybrid Warfare – neue Dimension der terroristischen Bedrohung. Herausforderung an die Sicherheitspolitik [hybrid warfare – new dimensions of terrorist threat – challenge to security policy]. In: Die Politische Meinung, No. 508, March 2012, p. 59ff, here p. 59. <http://www.kas.de/wf/doc/kas_30476-544-1-30.pdf?120402104509>.

States will implement hybrid warfare above all when the purpose is to deploy means that cannot be traced back to them (e.g. by deploying soldiers abroad without badges of rank or service in the presence of resistance to such incursion – Russia is said to have proceeded in this manner in the Ukraine[252]). This situation must be considered in the event of countermeasures. Combating hybrid threats is not so much about new capabilities as new processes and new thinking.[253]

Through the term "hybrid threat", the altered character of military challenges should be comprehensively described and conventional characterisations should lapse, in order to be able better to grasp the current reality. Following 9/11, the USA faced an adversary who, for relatively little monetary outlay, had wreaked damage on a scale that, to date, would only have been thought within the capability of regular armed forces. Following 9/11, terrorism, and criminality as an important potential source of finance for terror groups, need to be included appropriately in theoretical considerations of threats. Frank Hoffman, who played a significant role in shaping the debate on the term "hybrid threat", quoted a British general who opined that, in the armed forces, the past and tradition were powerful prisms through which current and future trends are observed. Armed forces should become aware of this effect of distortion.[254]

Hoffman is of the opinion that the debate about the nature of wars has often wavered between the two poles of "counterinsurgency" or "nation-building" and conventional wars, a "bipolar discussion" judged to be inadequate.[255]

[252] Kleine grüne Männchen, ein "HybridKrieg" und die Probleme der NATO [little green men, "hybrid warfare" and NATO's problems]. In: Vorarlberg Online, 25/06/2014. <http://www.vol.at/kleine-gruene-maennchen-ein-hybridkrieg-und-die-probleme-der-nato/4006225>.

[253] Miklaucic, Michael: NATO Countering the Hybrid Threat. 23/09/2011. <http://www.act.nato.int/nato-countering-the-hybrid-threat>.

[254] Hoffman, Frank G.: Hybrid Threats: Neither Omnipotent nor Unbeatable. In: Orbis, Vol. 54, Issue 3, 2010, p. 441-455.

[255] Ibid, p. 5.

He asked himself the question, what does “conventional” actually mean, and observed correctly that (in the USA) no-one was assuming that any conflict with China, North Korea, Iran or Russia would be conducted “conventionally”, namely with tanks, rockets, jet fighters etc., Hoffman’s interpretation of the term “conventional”.[256] So are Russia, China etc. not conventional adversaries? As an example of modern “hybrid warfare”, he put forward the conflicts with Hezbollah in Lebanon in 2006. This non-state group had succeeded in hitting an Israeli boat with an anti-ship missile, thereby shattering conventional assessments of such groups’ capability of maritime warfare.[257]

Hezbollah was fully aware of the manner of its warfare and their chief, Hassan Nasrallah, also reflected on this. He described his organisation’s manner of warfare as “something between classic warfare and guerrilla combat”.[258] The central factor for such a form of warfare is the assessment that, in western societies, people cling to life whilst, for their Islamic opponents, death holds no terror – thus ultimately no (psychological) victory is to be achieved through physically terminating the adversary because, in the eyes of Hezbollah, the very continuation of his existence is a success in itself and a defeat for the adversary.[259] A critic of Hoffman’s views, Dan G. Cox, objected that the former’s concept was too imprecise to be able to do anything with it in practice. Ultimately findings with regard to new threats and warfare need to yield actual options for action. But ahead of this comes the discussion as to precisely how this new threat, and the manner of waging wars, is structured.[260]

[256] Ibid, p. 6.

[257] Ibid, p. 6f.

[258] Sahm, Ulrich W.: Raketenbedrohung Israels. Der neue islamistische ‘hybrid Krieg’ zur Judenvernichtung und Weltherrschaft [Israel under threat from rockets – the new Islamist ‘hybrid war’ to annihilate Jews and dominate the world]. 16/12/2011. <http://honestlyconcerned.info/2011/12/14/raketenbedrohung-israels/>

[259] Ibid.

[260] Cox, Dan G.: What if the Hybrid Warfare/Threat Concept Was Simply Meant to Make Us Think? 13/02/2013. <http://www.e-ir.info/2013/02/13/what-if-the-hybridwarfarethreat-concept-was-simply-meant-to-make-us-think/>.

"Hybrid warfare" denotes a combination of regular and irregular methods of warfare. Hybridity can be interpreted as a reflection on the unity of material and cognitive elements in warfare. The decisive means of relevance to war is not the military. According to this point of view, anyone can wage wars, independently of what "military" (quotation marks adopted from original text) means he possesses.[261] In their piece, Sadowski and Becker seek to discuss the true nature of war and, through these general observations, they develop a holistic approach. With the cognitive elements it's about influencing the human mind. Acts of deception, distraction, scaring and dissuasion influence the adversary's will. Feelings, behaviour and perceptions constitute the target at which means are directed.[262] Materiel assets (e.g. weapon systems) are thus side-stepped and yet it is still possible to have an effect on the adversary. Such a form of warfare is of particular interest to a warring party who is at a material disadvantage compared with his adversary[263] – see the example of Hezbollah above. Ultimately both elements are essential for overall success: it is necessary to reach the adversary's minds, but material success (physical damage) is nevertheless indispensable. It is necessary to integrate both elements and apply them in the correct proportions. Materially inferior adversaries will utilise low-cost means that cause enormous damage (e.g. 9/11).[264]

Sadowski and Becker list the following kinds of "small wars" as threats for the USA: uprisings (Iraq, Afghanistan), piracy (Horn of Africa, Strait of Malacca), terrorism (al Qaeda), organised crime (Taliban, Mafia, drug cartels), restriction of "general goods" (attacks in cyberspace, blockading the Strait of Hormuz), proto-states (organisations with quasi-state character tolerated by official state institutions, e.g. the Farc – Fuerzas Armadas Revolucionarias de Colombia [Revolutionary Armed Forces of Colombia] – or Hezbollah). As an example of "big war" they nominate a confrontation with China over Taiwan.

[261] Sadowski, David/Becker, Jeff: Beyond the "Hybrid" Threat. Asserting the Essential Unity of Warfare. In: Small Wars Journal, 2010, p. 4. <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-etal.pdf>.

[262] Ibid, p. 4f.

[263] Ibid.

[264] Ibid, p. 5f.

"Big wars" will indeed be waged using conventional armed forces, including the possible application of nuclear weapons. The numbers of casualties are higher, the spatial extent reaches further and they are over relatively quickly. Material elements will play an important role and the breadth of means deployed (military, economic, diplomatic) will be large. In "small wars", success depends more on cognitive elements, the duration will be longer, so there is a need for patience and staying power.[265] The big challenge with such diverse possibilities of conflict will in future reside in ensuring the unity of warfare with regard to the need to make use of the different elements of warfare in correspondingly appropriate ways – high adaptability is thus required, in order to be able to react quickly to the unexpected.[266] The proposition of the two authors regarding the waging of a war ultimately applies to overcoming hybrid challenges as a whole, because the means must be coordinated in peacetime to prevent escalation to war.

3.1.2 Hybrid challenges or threats?

For this reason, it is indeed better to talk of "hybrid challenges", because security policy should be formulated sufficiently early for threats to be unable to arise. For a threat to be described as such, it must exceed a certain "strategic threshold". But the threat comes into existence before this threshold is reached. Combating it must already begin there. The European security strategy demands the following approach:

> "The new threats are dynamic. The risks of proliferation grow over time; left alone, terrorist networks will become ever more dangerous. State failure and organised crime spread if they are neglected. (...) *This implies that we should be ready to act before a crisis occurs. Conflict prevention and threat prevention cannot start too early*."[267]

[265] Ibid, p. 7f.

[266] Ibid, p. 10.

[267] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 7. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

So action must be taken before threats become evident. "*Preventing threats from becoming sources of conflict early on must be at the heart of our approach.*" is the additional comment in the implementation report.[268]

Broken down to the operating level, this means for example, as defined in the strategy for combating terrorism, that travel to areas of conflict should be monitored. Travel is not in itself an activity that is legally relevant to combating terrorism, but it is necessary for the relevant authorities to acquire information about it.[269] Recently there was a case relevant to this in Austria. Two young girls, 15 and 16 years old, went missing in Vienna, and their mobile phone signals were located in Turkey a short time later, allegedly also in Syria. In online postings, the girls (or persons claiming to be them) asserted that they had joined Islamist fighters in Syria.[270] One of the pair had already expressed corresponding ideological views in Vienna. Such journeys cannot be prevented, but it is important to know about them in order to have knowledge of sentiment and attitudes in particular population groups and, in consequence, apply countermeasures; in a case like this for example, raising the gathering of intelligence about terrorist movements among (Moslem) adolescents.

Of course the identities of Islamist fighters should be uncovered to the maximum possible extent in order for security forces to be able to take appropriate measures against them.

[268] Council of the European Union: Report on the Implementation of the European Security Strategy - Providing Security in a Changing World. Brussels, 11/12/2008, p. 9, 407f. <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf>.

[269] Council of the European Union: The European Union Counter-Terrorism Strategy. 14469/4/05 REV 4. Brussels 30/11/2005, p. 8. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204>.

[270] Henckel, Elisalex: Postergirls of the Dschihad. Teenager mit einem Herz für al-Qaida [postergirls of the jihad - teenagers enamoured of Al Qaeda]. In: Die Welt Online, 15/05/2014. <http://www.welt.de/vermischtes/article128025803/Teenager-mit-einem-Herz-fuer-al-Qaida.html>.

States can also present challenges, before an actual threat arises. For example, without doubt, China constitutes a security policy challenge to European states. Talk of a threat would indeed be going too far, because it would not correctly describe reality. As the EU's second-largest trading partner, China is, as the word implies, an important partner for Europeans. This does not mean that China is an ally or behaves as such. The country has various means that it can deploy in order to enforce its interests: military, economic, diplomatic, media-related, technical. It presents a hybrid challenge because it deploys its means in a targeted and concerted manner, and will do the same in the event of conflict too. This is well illustrated by the example of Chinese cyber-espionage. According to the U.S. Ministry of Justice, unit 61398 of the Chinese People's Liberation Army carries out espionage via the Internet. It is said to work for Chinese state enterprises with the aim of creating commercial advantages for them. There is no clear separation between military and commercial. For the People's Republic, security has a commercial dimension, with the result that this form of espionage is not simply "industrial espionage".[271] The Chinese intellectual approach is altogether holistic and directed less toward individual categories like state, commerce and so on. So the People's Liberation Army also has to collaborate on the country's economic development – this is stated in the Chinese white book for defence 2012.[272] China has already proven that, in the event of conflict, it is prepared to utilise its commercial potential. As the dispute with Japan about islands in the East China Sea escalated in 2011, China prevented exports to Japan of "rare earths", important metals for technical products.

[271] Schmidt, Michael S./Sanger, David E.: 5 in China Army Face U.S. Charges of Cyberattacks. In: The New York Times Online, 19/05/2014. <http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-withcyberspying.html?_r=0>.

[272] The Diversified Employment of China's Armed Forces. IV. Supporting National Economic and Social Development. 16/04/2013. <http://www.china.org.cn>, <http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm>.

China dominates the market for these raw materials and showed Japan that it would not shy away from methods of commercial pressure.[273] When Chinese activities in cyberspace are noticed, these are highly likely also to be preparatory measures for any direct confrontations, in order to have the necessary information to hand at the right moment to hinder and circumvent the actions of an adversary and be able to hit back with maximum force.

At this point it is important to note that the USA also has the potential to present a hybrid challenge. Dan G. Cox notes that the concept of hybrid threat can be interpreted in such a way that the USA presents "the most dangerous" hybrid threat, because it can deploy various means (military, political, commercial) in a concentrated manner.[274] These authorities' surveillance activities, exposed by former National Security Agency staffmember Edward Snowden, serve to confirm such an assessment: technical potential is exploited for political, commercial and military purposes. However, for most EU states, the USA is an ally through NATO, and presents no challenge, at least not in any official assessment.

China also has no wish to give an impression of being a threat. Beijing applies "soft power" in a targeted manner, aiming at the feelings of Europeans. Panda bears serve as "ambassadors" communicating a friendly image of China. When two of these bears arrived in their new "homeland" Belgium in 2014, shortly before a visit by the state and party leader Xi Jinping, the Belgian head of government Elio Di Rupo was well aware of the significance of the animal guests. "For our economy, commerce, our scientific and cultural ties, this is truly a major event",

[273] Brettner-Messler, Gerald: Internationale Rundschau China [China international review]. In: Österreichische Militärische Zeitschrift, 1/2011, p. 111ff, here particularly p. 112.

[274] Cox, Dan G.: What if the Hybrid Warfare/Threat Concept Was Simply Meant to Make Us Think? 13/02/2013. <http://www.e-ir.info/2013/02/13/what-if-the-hybridwarfarethreat-concept-was-simply-meant-to-make-us-think/>.

commented the Prime Minister.[275] Serving an equally promotional role is the Chinese State Circus; there is also no attempt to conceal this function:

[True to tradition and facing the future with innovative ideas, it has succeeded in showing enthralled audiences not only acrobatic highlights but also and in particular China's history, culture and people], according to the homepage. The artistes who perform are trained in more than 1000 (!) circus schools throughout the country.[276] Sports events like the Olympic Games, performances by Shaolin monks and others are also directed at convincing the world of China's cultural grandeur, as well as its peaceful ambitions.

The European Union, which (unlike NATO) possesses civil and military means, should actually be particularly able to move to counter hybrid threats. Among the fundamental strategic documents, the term hybridity has long failed to appear. The European Security Strategy was adopted in 2003, when discussions on this topic were first starting. The term is still not mentioned in the 2008 report on implementation of the ESS, because it had not yet achieved widespread recognition.

Hybrid threats require an initiator who brings a variety of means to play. Specific actors are scarcely mentioned in the European papers. States, if mentioned, are described mainly as "partners", including Russia and China. In the 2008 implementation report, Iran and its nuclear programme are described as a "danger for stability in the region and for the whole non-proliferation system"[277]. North Korea is named explicitly in connection with the nuclear threat. There is no hybrid threat by this state can be determined. Also named in the report is Afghanistan, though this state cannot

[275] Giant pandas get a celebrity welcome in Belgium. In: Reuters, 23/02/2014. <http://www.reuters.com/article/2014/02/23/us-belgium-pandasidUSBREA1M0MV20140223>.

[276] The Chinese State Circus. <http://www.chinesischer-nationalcircus.eu>.

[277] Council of the European Union: Report on the Implementation of the European Security Strategy - Providing Security in a Changing World. Brussels, 11/12/2008, p. 1.

be described as an actor, given its internal problems, and is therefore also described as a target for measures towards stabilisation. The same applies to the Democratic Republic of the Congo, Guinea-Bissau and Somalia, the latter also named because of piracy emanating from it.[278]

Al Qaeda is specifically named in the ESS as a terror group; it is also named along with the "groups it inspires" in the terrorism strategy, because they presented the "main threat to the Union"[279] – indigenous, European terrorism is deemed subordinate. The strategy documents mention challenges arising from phenomena like poverty, competition for natural resources and energy dependency.[280] Nominated as threats are processes such as regional conflicts (e.g. the Balkan conflict), the failure of states and piracy.[281]

3.1.3 Elements of hybrid threat

Terrorism and organised crime are methods of action that endanger security. Terrorism is a form of waging conflict that is used by an actor and can therefore form part of a hybrid threat. "Terrorists" themselves can of course also constitute a hybrid threat in that they deploy a variety of means, not all of which are individually "terrorist". The fact that the danger presented by terrorism is multi-layered is mentioned in the implementation report to the extent that terrorists are described as potential proliferators of weapons of mass destruction.[282] There is indeed also

[278] Ibid, p. 3, 7f.

[279] Council of the European Union: The European Union Counter-Terrorism Strategy. 14469/4/05 REV 4. Brussels 30/11/2005, p. 7. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204>.

[280] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 2f. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

[281] Ibid, p. 4f; Council of the European Union: Report on the Implementation of the European Security Strategy - Providing Security in a Changing World. Brussels, 11/12/2008, p. 1, 8.

[282] Council of the European Union: Report on the Implementation of the European Security Strategy - Providing Security in a Changing World. Brussels, 11/12/2008, p. 3.

an implicit indication of hybrid threats in the ESS, given the following summary at the end of the section on key threats:

> "Taking these different elements together – terrorism committed to maximum violence, the availability of weapons of mass destruction, organised crime, the weakening of the state system and the privatisation of force – we could be confronted with a very radical threat indeed."[283]

One can interpret this sentence as saying that the threats could have simultaneous and targeted effects on Europe, and one might assume that the authors also intended this.

Organised crime is a special form of commercial activity pursued by organisations dedicated to this purpose and which can also arise from states. Cybercrime is another form of criminality that is named in the ESS, the implementation report and also in the strategy for interior security. In this case too, it can arise from state and non-state actors and can be one element of a hybrid threat.

The breadth of cybercrime is great. It ranges from espionage of state secrets or commercial secrets of companies in cyberspace, through Internet fraud (obtaining money by means of email under false pretences to the effect that some financial deposit is necessary in order to qualify for an inheritance or other allegedly accessible fortune), to trading of illegal goods on the Internet (anything from counterfeit drugs, fashion, electronic goods etc., pirate copies of films and music, child pornography to weapons and drugs). But criminal activities in cyberspace can also take place as a part of other actionable activities. Dutch hackers successfully broke into computers belonging to the harbour administration of the Belgian port of Antwerp and manipulated the destinations and arrival times of containers. Drugs were loaded into the affected containers, which were then received by drug dealers without any risk of being caught by the police.[284]

[283] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 5. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

[284] Interpol: Against Organized Crime. Interpol Trafficking and Counterfeiting Casebook

For terror groups, cyberspace is essential to their self-portrayal in the media. They campaign on the Internet for "holy war", in order to recruit people to their cause, whether as active fighters or as cash donors. The media presentation of their activities has developed into an important aspect of these groups' work. On YouTube, Twitter and other services, advertising is pursued intensively to promulgate each group's objectives and present each organisation as particularly efficient. Yet this is not just about mobilising a potential target audience, but also about the cognitive element in warfare. During their operations in Iraq in June 2014, "Islamic State" (IS) spread fear and terror in cyberspace too by placing pictures and videos of atrocities on the Net. The intentions were to spur on their own fighters whilst intimidating and demoralising their enemy. The use of the Internet is at a very professional level. This potential is also recognised by the other side. Thus the Iraqi government has blocked various services and called on the largest Internet service providers in the provinces controlled by IS to block Internet access.[285]

Terrorist organisations often work multi-dimensionally and deploy the dimensions of their activities in a targeted and concerted manner. They do not merely conduct operations like bomb attacks or abductions, but rather are also active in the social domain. This applies to the Palestinian organisation Hamas, which was rated as a terrorist organisation by the EU and the USA.[286] The "Internationale Humanitäre Hilfsorganisation" [International Humanitarian Aid Organization] was a German association that collected donations for social measures on the Gaza Strip, without engaging in any terrorist activities itself. Due to its close links with Hamas, the association was outlawed in 2010 (the similarly-named Austrian association continues

2014, p. 80. <http://www.interpol.int/Media/Files/Crime-areas/Trafficking-in-Illicit-Goods/Against-Organized-Crime-INTERPOL-Trafficking-and-Counterfeiting-Casebook-2014>.

[285] Kotrba, David: Terrorgruppe ISIS im Irak. Islamisten führen Dschihad im Internet [ISIS terrorist group in Iraq – Islamists wage jihad on the Internet]. 18/06/2014. <http://futurezone.at/digital-life/terrorgruppe-isis-im-irak-islamisten-iminternet-dschihad/70.817.550>.

[286] Note: in December 2014, the European Court of Justice instructed the EU to remove Hamas from the list of terrorist organisations.

to exist). The purpose of its social activities (which it had conducted since its foundation) on behalf of Hamas was to secure an appropriate level of societal anchoring within the Palestinian population and, at the same time, to create more financial leeway, which made more terrorist activities possible.

The hybrid character of terrorist organisations had already been implicitly established by the German Federal Administrative Court in 2004, in that it saw the political, social and terrorist activities of Hamas as inseparable.[287]

Conversely terrorism is an instrument that can also be deployed by states and thus become a component of a hybrid threat. This is demonstrated by an example from German history. In the event of a German-German conflict, the minister for national security of the German Democratic Republic (DDR), Erich Mielke, considered the deployment of left-wing terrorists from the ranks of the Rote Armee Fraktion [Red Army Faction] behind the adversary. However, actual attacks were supportd by the DDR. An attack on the French cultural centre in West Berlin, resulting in one death, was prepared in East Berlin by a man associated with the terrorist Carlos.[288] Another example is Libya's former head of state, Muammar al Gadaffi. He has been accused of numerous connections with terrorist activities. The most spectacular case was the bombing of a passenger aircraft owned by the U.S. company PanAm above the Scottish town of Lockerbie, in which 189 U.S. and 43 British citizens died. The precise details have indeed not been clarified to date, though Libya accepted responsibility for the attack, with the former Libyan minister of justice accusing Gaddafi of having personally given the order for the attack. The former U.S. Secretary of State

[287] Federal Ministry of the Interior: Press release 12/07/2010, Bundesinnenminister Dr. de Maizière verbietet Hamas-Spendenverein [minister of the interior, Dr. de Maizière, bans Hamas-donor-association]. <http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/07/vereinsverbot.html>.

[288] Federal commissioner for the files of the state security service of the former German Democratic Republic: Ein "Faustpfand" des MielkeApparates. Die Staatssicherheit und die Rote Armee Fraktion (RAF) [a "bargaining chip" for Mielke's forces – state security and the Red Army Faction]. <http://www.bstu.bund.de/DE/Wissen/Aktenfunde/RAF/raf_node.html>.

Hillary Clinton has accused Gaddafi of having been behind plans to assassinate the king of Saudi Arabia. What cannot be denied is that, in 1984, demonstrators were fired upon from the Libyan Embassy in London and a female police officer died.[289]

Organised crime (OC) is also a hybrid threat. Illegal business blends with legal business, society is influenced by the criminal activities, with the media also often unable to elude them. The potential scale is declared tersely and concisely in the ESS: "In extreme cases, organised crime can come to dominate the state."[290] It is in the nature of OC to appear in many dimensions. The illegality of the various areas of business forces criminals to create a favourable environment for their "business". Politicians and civil servants have to be made amenable by means of corruption or threat, in order that the rule of law and criminal proceedings operate at an appropriately lax level, whilst the media should have as little freedom as possible to report on criminal activities. In this context, the strategy for interior security states: "In addition, corruption is a threat to the bases of the democratic system and the rule of law."[291] In order to create a favourable "working environment", the bosses often present themselves as philanthropic, cultivate a Robin Hood image and can demand favours in return.

Terrorism and OC are partially linked: "[...] It can have links with terrorism."[292], states the ESS. One example is the left-radical guerrilla organisa-

[289] Daniel Bates, Clinton: Gaddafi responsible for Lockerbie bombing. In: Scotsman Online, 11/06/2014. <http://www.scotsman.com/news/politics/top-stories/clintongaddafi-responsible-for-lockerbie-bombing-1-3439871>; Gaddafi ordered Lockerbie bombing. In: Aljazeera Online, 24/02/2011. <http://www.aljazeera.com/news/africa/2011/02/20112232135478455546.html>.

[290] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 5. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

[291] General Secretariat of the Council: Internal security strategy for the European Union; Towards a European Security Model. Luxemburg 2010, p. 14. <https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf>.

[292] Council of the European Union: European security strategy. A Secure Europe in a

tion Farc (Fuerzas Armadas Revolucionarias de Colombia [Revolutionary Armed Forces of Colombia]), which is active in the cocaine business. For a long time, this narcotic has been their main source of income at around 4 billion USD per annum. Originally the guerrillas collected “taxes”, but later they joined criminal organisations with no political background to become part of international drug trafficking.[293] The borders between OC and terrorism are fluid. Both have to operate under cover and so it is logical to cultivate synergies.

OC possesses networks for arms dealing and money laundering. But other services, such as counterfeiting documents, are taken on by terrorist groups. Using OC methods it is possible to finance terrorist activities. OC and terrorist groups learn from one another and complement one another to their mutual benefit. One example of this is the financing of Al-Shabaab militia in Somalia through illegal trade in ivory. Meanwhile, in Northern Ireland, a source of money for republican paramilitaries is the smuggling of diesel-fuel from the Republic of Ireland into British Northern Ireland.[294]

The fact that OC is a hybrid threat is also reflected in the ESS:

> “Restoring good government to the Balkans, fostering democracy and enabling the authorities there to tackle organised crime is one of the most effective ways of dealing with organised crime within the EU.”[295]

Better World, p. 4. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

[293] Endres, Alexandra: Kolumbien. Die Farc geht auf Kokain-Entzug [Farc off to cocaine rehab]. Die Zeit Online, 17/05/2014. <http://www.zeit.de/politik/ausland/2014-05/farc-kolumbien-kokain>.

[294] Interpol: Against Organized Crime. Interpol Trafficking and Counterfeiting Casebook 2014, p. 112ff. <http://www.interpol.int/Media/Files/Crime-areas/Trafficking-in-Illicit-Goods/Against-Organized-Crime-INTERPOL-Trafficking-and-Counterfeiting-Casebook-2014>.

[295] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 6. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

Conversely this implies that weak state structures serve the interests of OC, so the latter will contribute to maintaining such conditions where possible. Their hybrid character is also to be found in definitions of OC. The German Ministry of the Interior writes on its homepage:

> "[The prerequisite (for the presence of OC; author's note) is that more than two collaborators work together, using industrial or apparently commercial structures or violence or other means directed towards intimidation or bringing influence to bear on politicians, the media, public administration, justice or business for an extended or indefinite period.]"[296]

Just a few numbers demonstrate the potential for a comprehensive exercising of influence. According to UNO, worldwide OC business amounts to 2.1 trillion USD, with the Italian Mafia alone accounting for up to180 billion USD. The criminal police bureau of Baden-Württemberg estimates these criminals allow around half of their income to flow into legal business. In this manner they gain commercial and societal influence way beyond their own circles – a reality that should be noticed as little as possible.[297] In Germany the objective is to turn up unnoticed, thereby seeking not to attract the attention of law enforcement authorities. Where possible, murders will not be committed here; instead potential victims are lured to Italy. Protection racketeering also scarcely arises in Germany. The intention is that Germans should, if possible, not notice that the Italian Mafia is extremely active in their country. The money flows through restaurants, property and construction companies.[298]

[296] Federal Ministry of the Interior: Sicherheit, Kriminalitätsbekämpfung, Organisierte Kriminalität [security, fighting crime, organised crime]. <http://www.bmi.bund.de/DE/Themen/Sicherheit/Kriminalitaetsbekaempfung/Organisierte-Kriminalitaet/organisierte-kriminalitaet_node.html>.

[297] Diehl, Jörg: Organisierte Kriminalität: Deutschland versagt im Kampf gegen die Mafia [organised crime – Germany fails in the fight against the Mafia]. In: Spiegel Online, 08/04/2014. <http://www.spiegel.de/panorama/justiz/mafia-indeutschland-die-geschaefte-der-kriminellen-clans-a-963027.html>.

[298] Schraven, David: Mafia in Deutschland. Geschäfte im Inland, Morde im Ausland [Mafia in Germany – business at home, murders abroad]. <http://mafiafilm.correctiv.org/>.

This modus operandi of OC has to be recognised for it to be possible to take the necessary countermeasures, particularly legislative. The chief prosecutor of Palermo has accused Germany of having enacted too few statutory regulations to be able to combat OC effectively. Mafiosi invest in Germany because they find the legislative situation favourable, unlike in Italy, according to the chief prosecutor. In Italy, even in the event of suspicion of Mafia connections, assets can be seized, but this is not possible in Germany. In politics and society in Germany, the level of consciousness of being in danger from an organisation like the Mafia is unremarkable. Following a spectacular murder of six men in 2007 in Solingen, awareness did indeed increase temporarily but persisted only for a limited time. Up until 2009 some 2.4 million euros were seized but, following that, the total amounted to but a few hundred thousand euros.[299]

Organised crime is not inevitably linked to business that directly contravenes the law, e.g. drug dealing. In Berlin, street vendors turned up who sold canned drinks to people in queues. Organised groups quickly took over this illegal form of vending. Political scientist Regine Schönenberg used this example to demonstrate that OC takes possession of "spaces" that are insufficiently or not at all regulated by the state. In this context, the researcher gives a further example: workers engaged in counterfeiting products in China. Following China's admission to the World Trade Organization (WTO), China's authorities were obliged to act against this illegal branch of manufacturing. The problem is that if the people engaged in such business sectors cannot be relocated by the state to other areas of activity, they remain trapped in criminal structures.[300]

OC is not limited to non-state organisations like the Mafia. North Korea has a long tradition of criminal activities. In 1976 a series of North Korean diplomats were expelled, including the ambassador in Norway, because

[299] Schraven, David: Der lachende Solinger [laughing Solinger]. <http://mafiafilm.correctiv.org/der-lachende-solinger/>.

[300] Endres, Alexandra: Organisierte Kriminalität: "Die Politik is verstrickt" [organised crime – politics are involved]. In: Die Zeit Online, 19/06/2013. <http://www.zeit.de/wirtschaft/2013-06/organisiertekriminalitaet-interview>.

they were involved in substantial smuggling of alcoholic beverages, cigarettes and hashish.[301] In the same year, other diplomats from North Korea were caught in Egypt with 400 kilos of hashish. Officially these cases were portrayed as individual misdeeds, but the mere fact that such people had been diplomats for years suggests a state-organised system.[302] From the mid-1990s, North Korea was said to have limited itself to drug production, with distribution delegated to criminal organisations abroad.[303] Even though North Korea's isolation makes it difficult to obtain definite information, the involvement of North Koreans in drug dealing was so intensive that experts worked on the assumption of state-organised drug dealing.

In recent years, the role of the state seems to have changed, having apparently withdrawn from drug dealing, which might be interpreted as indicating that it now only draws income from "private" drug dealers who can rely on state protection in return.[304]

3.1.4 Hybrid threats: future need for analysis in Europe

The ESS makes due mention of the multi-layered nature of hybrid challenges, given that the "comprehensive approach to security", as a concept for dealing with such challenges, is a strategic basis for the EU's defence against threats.

> "Each (of the new threats; author's note) requires a mixture of instruments. (...) Dealing with terrorism may require a mixture of intelligence, police, judicial, military and other means."[305]

[301] Greitens, Sheena Chestnut: Illicit. North Korea's Evolving Operations to Earn Hard Currency. Committee for Human Rights in North Korea, Washington DC 2014, p. 16. <http://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf>.

[302] Ibid, p. 16f.

[303] Ibid, p. 18f.

[304] Ibid, p. 76ff.

[305] Council of the European Union: European security strategy. A Secure Europe in a Better World, p. 7. <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>.

Albeit a complete cessation of the partition into internal security, which is protected by the judiciary and police, and external security, which is provided by the military, has not yet been achieved even in the strategic basis documents. In the strategy for internal security, the armed forces receive practically no mention; only for international crisis management missions is there a requirement, regarding internal security, for responsible agencies and bodies to work together "[...] with all other services involved on the ground (military, diplomatic, emergency services, etc.)".[306] Elsewhere it states:

> "The cooperation of law-enforcement and border authorities, judicial authorities and other services in, for example, the health, social and civil protection sectors is essential. Europe's internal security strategy must exploit the potential synergies that exist in the areas of law-enforcement cooperation, integrated border management and criminal justice systems."[307]

The use of armed forces is not anticipated here. In a case of emergency it will not be possible to do without them, if one just thinks of natural disasters or those with a human cause (which are listed among threats in the strategy for internal security) or major terrorist attacks. In Austria, alongside security police assistance deployment along the eastern border to prevent illegal crossings, the need was recognised for military deployment without a condition of national emergency.

Albeit, for the "surgical" application of these instruments, it is also important to know how the adversary will think and act. Because the adversaries of the EU consider very precisely what measures have already been or could be set within the EU so that they can circumvent them in good time. North Korea is an example of a state that appears to have developed great skill in circumventing obstacles to its illegal business activities by tailoring highly flexible products, production facilities, transportation routes,

[306] General Secretariat of the Council: Internal security strategy for the European Union; Towards a European Security Model. Luxemburg 2010, p. 30. <https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf>.

[307] Ibid, p. 8.

financial infrastructure and the position of the regime to the prevailing requirements. It is said that “think tanks” were set up with the task of studying international sanctions. The specialists within them devise ways and means to circumvent these sanctions, whilst also recognising future measures in advance, in order to be able to circumvent them in good time.[308]

Conversely it would be important for the EU and its member states to know such potential threats and address them openly, in order to create broad awareness of the danger. This would already constitute a step towards early, and thus timely, control. In the case of states, the decision about such strategic assessment is politically delicate and therefore difficult to achieve via European committees. The fact that, in Europe, the thinking is not in terms of cut-and-dried, friend-foe scenarios can be judged as basically positive, given that orientation towards categories of “partnership” commonalities with other states stands in the foreground, by means of which differences can be overcome.

There will indeed be security policy disagreements among actors, as well as states, which cannot be settled by negotiation (alone). In the European context, it should be possible to address such differences openly.

In Europe, security policy thinking changed when the necessity of networked thinking was recognised. The “coherent use of our instruments”[309] is demanded in the implementation report, but the adversary also uses his instruments in a coherent manner. Thinking oriented towards hybrid approaches is important not only in relation to defending against sources of danger but also for recognising sources of danger. Such sources of danger

[308] Greitens, Sheena Chestnut: Illicit. North Korea’s Evolving Operations to Earn Hard Currency. Committee for Human Rights in North Korea, Washington DC 2014, p. 106. <http://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf>.

[309] Council of the European Union: Report on the Implementation of the European Security Strategy - Providing Security in a Changing World. Brussels, 11/12/2008, p. 9. <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf>.

can thus be more precisely captured and appropriate countermeasures applied. This would make an important contribution to a secure Europe, because it would be possible to react early to threatening developments, whilst challenges and threats would not develop into complex risks for European security. The connotation of "comprehensive security" could be oriented more towards practical needs, because the threats would also be correspondingly "comprehensively" defined.

3.2 State Support of Terrorist Organisations as a Potential Means of Hybrid Threat Projection

Ramy Youssef

3.2.1 Introductory remarks

According to Clausewitz, war is the mere continuation of policy by other means. A widespread interpretation reads this dictum as implying a temporal sequence, in which the military takes the place of politics, after all political means of resolving a conflict have been excluded. Even if this interpretation were to reflect Clausewitz correctly, it would still remain empirically improper, at least under modern conditions. Particularly thus far as a political system cannot be reduced to the organisational complex that is classically referred to as state administration (including the military), but further includes political parties, unions, NGOs, protest movements and a public that is politicised in the broadest sense.[310]

In this case it can increase its possibilities to enter into global political relations with other political systems on various formal and informal channels and levels at the same time and maintain them (as more or less conflictual). Further modern state administrations are *per se* already internally differentiated to such an extent that they dispose of specialised sub-organisations and professional staff for warfare, as well as for diplomacy, which may operate largely autonomously in relation to each other. Therefore, it is possible to be at war and negotiate at the same time. An empirically more appropriate (and significantly more efficient) interpretation of Clausewitz could therefore be that the choice of a certain strategy of influencing a political system, as well as the choice of the means of a militant use of force, always depends on the underlying political and social structure in which the war faring parties are embedded. Which means that

[310] For the internal differentiation of modern political systems see Wimmer, Hannes: Die Modernisierung politischer Systeme: Staat, Parteien, Öffentlichkeit. [the modernisation of political systems: state, parties, public] Vienna 2000.

the course of war is fundamentally co-determined by (internal) political and societal realities.

The alteration of these parameters also means a change not only in the character of the “chameleon” war but further, in a broader sense, the possibility of projecting threats in global political relations. These do not have to be solely based on military capacities, but can rather include several levels and social sectors at the same time and can utilise their services to enforce global political interests.

The term “hybrid threat”, meaning the capacity to pool political and social resources on multiple dimensions and apply them in a timed context for global-political objectives, aims at comprehending these phenomena. The following reflections shall in this respect be understood as a contribution towards testing out this term using state-sponsored terrorism (SST) by way of example. They originate from the question as to how SST is made possible and under what conditions SST can be applied in the hybrid threat context. Therefore, it shall be rather seen from the perspective of the sponsoring state (and not the one of the target state), as it seems to be a higher priority initially to be able adequately to describe and understand the phenomenon of SST in the first place. It is left for analyses in future to work out implications for defending against specific threat scenarios. This report section represents the supposition that SST presents a feasible option for a state, through which a potential threat can be established with relatively low resources. At the same time the efficiency of this strategy depends on the threatened political system’s degree of differentiation, as it has to not only dispose of an established monopoly on the use of force, but also of a political public sphere with free news coverage, for terrorism to take effect. Further it is assumed that terrorist organisations cannot be implanted in any other state, but can only originate from protest movements and this process cannot be directed by a sponsoring state. These assumptions now have to be further refined in several sections. In this process the term hybrid threat shall be located in a wider context of the scientific examination of global politics (Chapter 3.2.2), followed by discussing the conditions for the possibility of differentiating terrorism (Chapter 3.2.3). Ultimately, the specific pattern of SST shall be discussed, regarding its threat potential (Chapter 3.2.4) to finally compile the results in a conclusion (Chapter 3.2.5).

3.2.2 Analytic frame

Looking at the theoretical history of the academic discipline of International Relations (IR) reveals that big paradigms have always also been partly shaped by the political constellations of their time of origin. From the end of the Second World War until the early 1990s, the theories of IR have been largely characterised by (neo)realistic approaches that regarded states and their relations as the exclusive subject of analysis. This involved regarding the world of states or the international system as an anarchic structure that has been thought of as being decomposed into functionally equal entities (states) that only differ regarding their military capacities. In this sense, the category of power has always been identified with military superiority or inferiority. The asymmetries of power thereby emerging in the international relations would lead to the development of alliances, with the objective of preventing political imbalances by synchronising and concentrating military power resources and creating a balance of power.[311] This theoretical string may have had a certain justification and empirical validity for a long time but, with the end of the Cold War (and the inability of realistic theories to predict it), a paradigm shift occurred in theory construction as well as in practice. This is why a substantial change of state policymaking can be observed, taking place parallel to the emergence of new liberal and constructivist theories. Since then the priority is no longer geopolitical competition and the distribution of military resources to enforce state interests violently. State power is also not mainly defined by the availability of weapon technologies anymore, but also by “soft” ways of enforcing interests (soft power).[312] New modes of cooperation, particularly within the framework of international and supranational organisations, take on greater significance. The classical hierarchic task of bureaucratic rule (government) is, whilst not replaced, still supplemented by the practice of such forms of cooperation, which operate under the headline of ‘(global) governance’.

The emergence of new, private actors and the rise of public-private part-

[311] Cf. Waltz, Kenneth: Theory of International Politics. Reading et al. 1979.

[312] See Nye, Joseph S.: Soft Power. The Means to Success in World Politics. New York 2004.

nerships is also being realised and analysed on a sub-state level. On the international level the genesis of multiple new states can be put down to the process of decolonisation and the collapse of entities such as the Union of Soviet Socialists Republics (USSR) since the end of the Second World War.

Therefore, overall one can clearly perceive the emergence of multiple new actors in global politics who also act transnationally and can establish mutual relations much more easily than previously. Furthermore, the spreading of new communication media, such as satellite television and the internet, facilitates such processes that contribute to establishing transnational networks in which all actors involved, be they states, NGOs, protest movements, media etc., may become mutually relevant for one another. The increasing number of relevant political actors is accompanied by an exponential growth in social complexity that can be boiled down to a simple mathematical formula. Assuming that with, for instance, 193 existing states, each state maintains relations with all other states, the sum of the resulting relations, that is the complexity c, can be calculated and determined, according to the formula $c= (n^2-n)/2$, as being 18,528 (more or less conflictual) relationships in the world of states that could become virulent at any time. Complexity theories have coined the adjective 'noncomputational' for such cases – a system complexity that cannot be simulated with the aid of computers anymore, not to mention the plausibility of forecasts. Now states are not only mutually confronted by one another but can also maintain indirect relations with one another, be it through international or supranational organisations or sub-state private actors, bringing further complexity into international relations.

In the field of security policy this means, on one hand, increased cooperation through coalitions and defence alliances, as well as military collaboration in primary non-military organisations (thinking for example of battlegroups within the framework of the European Security and defence Policy ESDP). On the other hand, sub-state private violent actors (private security companies, mercenary armies, terrorist organisations etc.) also become essential, as states can cooperate with them to achieve particular policy objectives. Complexity in international relations is therefore synonymous with a vast variety of acting options being at the particular actors' disposal.

It is no longer the classical dichotomy war/diplomacy – if that ever existed. Furthermore there are new possibilities for the enforcement of interests provided by the accession to new spaces (and thereby new battlefields), such as cosmic space or cyber space, as well as by the interrelationship between state actors and private actors. Thus, in this context the terms hard/soft power are further complemented by the term hybrid power, meaning the synchronised use of various military and non-military means to enforce one's political will. The resulting threat scenarios in transnational conflicts have hence become complex, not to say unpredictable.[313]

But what does this mean for scientific analyses within the framework of the ICCM? It could be further claimed that forecasts are, considering the hybridity and complexity of prospective perceived threats, nothing more than pointless speculations, with their verification being sheer coincidence. However, regarded from this point of view, any anticipation of threats would become useless – since, after all, it is inherent to threats that they are always aimed towards an unknown future.[314] However this does not relieve politics of the burden of having to make decisions in the present that would codetermine this future. The contribution that scientific analyses can make to this matter would have to put hybridity and complexity themselves in the centre of the research interest and illustrate how policy-makers could develop strategies, with regards to this multitude of different interrelatable instruments of power, and what preconditions have to be met in order actually to be able to apply certain acting options reasonably.

The following contribution seeks analyse SST as a possible option for states within international conflicts, with regard to whether and under what conditions it can be considered as an element of a hybrid perceived threat.

For this purpose, it is necessary to discuss the conditions under which ter-

[313] Cf. Wallace, Ian: The Difficulties in Predicting Future Warfare. In: Australian Defence Force Journal, 183/2010, p. 27ff.

[314] Cf. Schirmer, Werner: Bedrohungskommunikation. Eine gesellschaftstheoretische Studie zu Sicherheit und Unsicherheit. [threat communication - a socio-political study on security and insecurity] Wiesbaden 2008, p. 104f.

rorism emerges at first, to be able subsequently to work out the possibilities and problems of state support for terrorism.

3.2.3 Terrorism and protest: on the emergence of terrorist organisations

To discuss terrorism in the context of political protest movements is far from obvious within the relevant literature.[315] However, there are multiple good reasons to take an at least cursory look at political protest movements, before conducting an in-depth description of the phenomenon terrorism. To begin with Peter Waldman, we can assume that "[a merely cursory look at terrorist campaigns is enough to become alert to their tight chronological correlation with broad political protest movements]".[316] This empirically observable correlation between the emergence of protest movements and terrorism cannot be ignored. At the same time, it is necessary to warn against pushing this correlation in an inevitable low-complexity causal pattern of the "if-then" kind. Instead the attempt should be made to illustrate a possibility to describe and explain the appearance of terrorist campaigns as an emergent phenomenon of protest movements. Another reason to consider protest movements is that there are certain common features regarding the modes of operation of protest movements and terrorist movements: both strive to mobilise the political public sphere for certain matters, both are, in this regard, particularly dependent on the capabilities of modern mass media and try to attract attention to themselves through unconventional communication. There are also significant similarities regarding their inner structures that cannot be limited to organisations at all, but rather take on the character of a network.[317]

[315] Cf. Gunning, Jeroen: Social Movement Theory and the Study of Terrorism. In: Jackson, Richard/Breen Smyth, Marie/Gunning, Jeroen (Eds.): Critical Terrorism Studies: A New Research Agenda. London/New York 2009, p. 156ff, here p. 156f.

[316] Waldmann, Peter: Terrorismus. Provokation der Macht. [terrorism - provocation of power] Hamburg 2005, p. 160.

[317] Cf. ibid., p. 161f. See also Ibrahim-Kudelich, Kardalan: Transnationaler Terrorismus als periphere Organisation des politischen Systems? Zur systemtheoretischen Beobachtbarkeit von Terrorismus. [transnational terrorism as a peripheral organisation of the political system? – on the observability of terrorism according to system theory] In:

The highly advanced research work that has been conducted so far to describe social movements and protest movements, could therefore certainly provide interesting insights into the mode of operation of terrorism and give substantial impetus to terrorism research. Further, phenomena of terrorist violence, which are usually regarded in isolation from the social environment, could be more easily embedded into a social context by referring to the respective protest movement.

Thus, terrorism is, according to the hypothesis represented here, a social phenomenon that can emerge if there are political issues that become the cause of conflicts and wider protest movements, in the course of which radicalisation and the secession of extremist factions take place, since:

> "None of the known terrorist groups started their career by the application of terrorism. Most modern terrorists had reached their terrorism gradually. They had been radicalized into it. (...) Sometimes the history of the radicalization is longer and goes back to older roots of anti-regime struggles and rebelliousness (...). But whatever the radical past is, it is lesser in intensity and brutality than terrorism and moves to terrorism by gradual evolution."[318]

However, terrorism cannot be understood *as protest*. As Ibrahim-Kudelich states: "[What draws a clear line for the violent escalation of 'demonstrations or spectacular acts of civil disobedience': the preservation of a positive public image seems to be suspended in the case of terrorism]"[319]. The emergence of violence delegitimises protest and is rather a undesired side

Kron, Thomas/Reddig, Melanie (Eds.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven [analyses of transnational terrorism - sociological perspectives]. Wiesbaden 2007, p. 194ff, here p. 200ff.

[318] Sprinzak, Ehud: The Process of Delegitimation: Towards a Linkage Theory of Political Terrorism. In: Terrorism and Political Violence, 3(1) 1991, p. 50ff, here p. 51.

[319] Ibrahim-Kudelich, Kardalan: Transnationaler Terrorismus als periphere Organisation des politischen Systems? Zur systemtheoretischen Beobachtbarkeit von Terrorismus. [transnational terrorism as a peripheral organisation of the political system? – on the observability of terrorism according to system theory] In: Kron, Thomas/Reddig, Melanie (Eds.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven [analyses of transnational terrorism - sociological perspectives]. Wiesbaden 2007, p. 194ff, here p. 203.

effect than a strategy for the democratic enforcement of political causes.

The purpose of protest is the demand for a change of collectively mandatory decisions, which shall be induced by establishing a threatening power through mass mobilisation. Towards the state, protest movements employ the medium of communication typical for politics - power[320], because they have the ability to do so – to the extent that they can mobilise a corresponding contingent of individuals and organisations. Terrorism, on the other hand, is not a communication of power but rather a communication of powerlessness.

> "[It is used by those who do not have or see any other chance of wielding influence. This applies as well and particularly if a terrorist act tries to turn the tables and simultaneously demonstrate to the state, the police or a population its powerlessness in dealing with such violence.]."[321]

The use of force means the failure of any communication of power – political power is expressed through being able to go without force. Terrorism is left with nothing but the "provocation of power", which it achieves by

> "[exactly addressing an enabling condition of the political *per se*, the monopoly on the use of force. In some way it parasitizes on this condition and that also means that it is itself anything but political, as much as politics can address it as being politically motivated. It is not about collectively binding decisions. It somehow stands – aside.][322]

Therefore, protests do not merge into terrorism, but rather they persist or decline, without this necessarily doing harm to terrorism. In this respect, terrorism is not a side stage of protest on which there is, besides the basically non-violent types of protest communication, also violent communication with the aim of

[320] Cf. Luhmann, Niklas: Macht. Stuttgart 2000. [Trust and Power, Chichester: Wiley, 1979].

[321] Baecker, Dirk: Die Gewalt des Terrorismus. [the violence of terrorism] In: Aderhold, Jens/Kranz, Olaf (Eds.): Intention und Funktion. Probleme der Vermittlung psychischer und sozialer Systeme. [intention and function - problems of conveying psychological and social systems] Wiesbaden 2007, p. 219ff, here p. 221.

[322] Fuchs, Peter: Das System "Terror". Versuch über eine kommunikative Eskalation der Moderne. [the terror system - attempting a communicative escalation of modernity.] Bielefeld 2004, p. 42.

changing political decisions. Terrorism is rather a conflict with its own history and inherent logic that is determined by the mutual application of force.

However, terrorism cannot merely ‘civilise’ itself by getting closer to the centre of the political system through de-escalation and integration, but can also detach itself from politics. This happens when terrorists separate themselves in a political conflict or a protest movement, and establish themselves as autonomous actors. As soon as this process is essentially completed – it is not until then that we can speak about ‘terrorism’ as such – a momentum is taking effect. Then it is no longer about political decisions, about power superiority/inferiority, but rather only about the friend/foe distinction and zero sum logic of violent attacks and counterattacks, which lead to the initial protest movement becoming less important and other problems gaining importance. Here one can particularly think about the consequences of the terrorists’ ‘self-preservation instinct’ which, once they have gone underground, leaves them with nothing to do, apart from criminal activities, than to carry out attacks. Just as a state cannot leave an attack – and therefore the undermining of the monopoly on the use of force – to go unpunished and has to bring the people responsible to justice.

Therefore, it can be observed that if terrorism is understood as a conflict system, there is also a focus on the state, whose counterterrorist measures also play a significant part in the reproduction of terrorism, just as terrorist attacks do. It is only because of the existence of a state that a strategy of terrorism makes sense:

> “(T)he ‘weapons of the weak’ are forceful only when they are backed by *the strength of the other*, which is in most cases a state. Terrorism, because of its lack of resources and its unconventional ways of fighting, is in fact characterized by *a triply indirect instrumentality*. It is *the overreaction of the other (the enemy state)* which is crucial in terrorism. It is that over reaction which is able to produce sympathy for the terrorists' cause by third parties such as populations hostile to the attacked and overreacting state, and other states.”[323]

[323] Schinkel, Willem: Aspects of Violence. A Critical Theory. Basingstoke 2010, p. 146 (the emphasis is taken from the original).

If this is the case, terrorism has to be described rather as interaction between state and terrorists and not as a succession of terrorist attacks.

This does not mean that the state itself has to act as a terrorist organisation, or that this is about some bond between state terrorism and 'private' terrorism. Rather it means that it is necessary to consider both sides in a conflict, to be able to understand matters. Thus, this does not change the fact that the only effective means against terrorists is the state's monopoly on the use of force. With this observation, a perverse paradox also becomes apparent: that it is only the state's monopoly on the use of force that can stop terrorism, yet terrorism only makes sense in areas with established statehood, since its attacks aim directly at modern states' monopoly on the use of force. Therefore, the modern state is the condition for both the prevention and the emergence of terrorist attacks at the same time.

3.2.4 State-sponsored terrorism as strategic option for a hybrid threat

Terrorism is often described as a type of warfare and discussed in the context of 'petty', 'new' or 'asymmetric' wars.[324] This is a distinction to the concept of 'big' international conflicts, in which regular armies combat each other with respect to rules of international law. With the transformation of political parameters, i.e. the incomplete spreading of statehood and the emergence of new non-state violent actors under the conditions of global communicative availability in the world society, the character of warfare changed as well. The emergence of terrorist strategies is therefore being analysed in the context of the dissolution of the Westphalian state order and the loss of its war-regulating function. The 'new' asymmetric war would therefore supersede the symmetric war of states and become the dominant mode of violent conflict.[325] However, this raises the question as to whether this would lead to a dilution of the term war, if it is used to describe not only the Second World War but terrorist campaigns too, such as those by the Red Army Faction.

[324] Cf. Münkler, Herfried: Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie.[the change of war - from symmetry to asymmetry] Weilerswist 2006, p. 221ff.

[325] Cf. Kaldor, Mary: New and Old Wars: Organised Violence in a Global Era. Cambridge, Malden 2012.

Furthermore, terrorism is in this respect not comparable with war, as attacks are rarely aimed against regular state armies, but rather against 'soft' targets. This does indeed not exclude the possibility of states framing terrorist attacks as belligerent attacks, to which they react with military means – but slogans such as 'war on terrorism' have therefore to be regarded rather as semantics in political discourses and not as scientifically binding descriptions of a conflict system.

Terrorist strategies can nevertheless also become important in international conflicts. SST represents a special case of armed conflict, because it involves not just one state facing one or more terrorist organisations, but rather there is an additional state involved as a conflicting party. This represents an overlapping of different conflicts: a conflict between a state and a terrorist movement and an international conflict, in which a state tries to instrumentalise a terrorist organisation against an opposing state. In that case, SST can be the means in a strategy of international confrontation in which "[the deployment of armed forces does not directly undermine the enemy's power potential, but rather indirectly, i.e. through threats, demonstrations etc. of violence, it forces the adversary to fulfil the foreign will.]".[326] It is in this respect a possible hybrid threat, as a state tries to enforce interests not only through its own military threatening potentials, but also to purposefully and simultaneously project a threatening posture on a political level, as well as through a non-belligerent use of force by a "proxy", in order to enforce its interest towards another state. This option shall hereafter be evaluated regarding its practical conditions, to reach a more specific assessment of this potential threat.

It is difficult to tell how far cooperation between states and terrorist organisations has spread.

However, it can be determined statistically that the number of terrorist attacks in international conflicts is significantly higher and reasonable as-

[326] Gustenau, Gustav E.: Zum Begriff des bewaffneten Konfliktes. [on the term armed conflict]In: Österreichische Militärische Zeitschrift, [Austrian Military Journal] Number 1/1992, p. 45ff, here p. 50.

sumptions of state support for terrorist organisations are not absurd.[327] Here the types of support range from training and teaching, through supplying money and weapons, to logistic support like issuing passports. However, the most important thing is the provision of territorial refuge for terrorists.[328] Usually terrorist organisations operate under the condition of secrecy, which initially enables their operational mode on one hand, but on the other hand also limits it to a great extent. The elimination of such obstructions would allow them to grow their membership and therefore establish a higher inner complexity, subsequently to be able to carry out much more complex operations.

What can be ruled out is that terrorist organisations could be 'created' artificially by a sponsoring state with a view to then 'implanting' them in the political system of an opposing target state. The emergence of terrorist organisations and a terrorist strategy is bound to too many preconditions, which have already been described here, for this to happen. Therefore states rather support already existing protest movements or terrorist movements to put political pressure on another (usually neighbouring) state.[329] It is therefore not a belligerent conflict, but rather a means of pressure that is used in international relations as a tactic within the framework of *coercive diplomacy.* Whilst this does involve the use of force by a terrorist "proxy", nevertheless direct military confrontation is avoided by staging a proxy conflict.[330] In that case terrorism can be a relatively efficient instrument to apply political pressure, because it gives rise to scarcely any costs and does not require any particularly elaborate technologies.

[327] Cf. Conrad, Justin: Interstate Rivalry and Terrorism: An Unprobed Link. In: Journal of Conflict Resolution, 55(4) 2011, p. 529ff.

[328] Cf. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, p. 59ff.

[329] Cf. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, p. 37f.

[330] Cf. Gal-Or, Noemi: State-Sponsored Terrorism: A Mode of Diplomacy? In: Conflict Quarterly, 13(3) 1993, p. 7ff.

This could be especially interesting for states that possess relatively limited military capacity and yet can project threats far beyond their own territorially defined sphere of influence, by applying such types of SST.[331] The secret support of terrorist organisations ultimately provides states with a *plausible deniability*[332], in particular the possibility to apply pressure on the target state on the one hand whilst, at the same time, being able to deny any cooperation when acting on a diplomatic level. They remain responsive to diplomatic communication, which can again be applied to enforce interests towards the target state. Therefore, it is diplomacy and terrorism that create the most important components of a strategy of hybrid threats and power projection, which nevertheless does not exclude the possibility of using military force at any time.

Contradictory to such a strategy is that terrorist organisations are only to a small degree dependent on state support: their armament is usually quantitatively and qualitatively limited and rarely exceeds conventional small arms that can also be acquired on the black market.[333] Financial means can be earned through criminal activities[334] and networks of sympathisers[335] and the provision of training can be ensured by the terrorist organisations themselves, since the operative know-how necessary hardly exceeds the instructions to build bombs that can also be built by individual 'private persons'. As complex as the preconditions for terrorism on a strategic level might be, so simply does it function at the operational level:

[331] Cf. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, p. 38.

[332] Cf. Byman, Daniel / Kreps, Sarah E.: Actors of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, p. 1ff, here p. 9.

[333] Cf. Schroeder, Matthew: Small Arms, Terrorism and the OAS Firearms Convention. Federation of American Scientists, Occasional Paper No.1, March 2004, p. 19ff.

[334] See Hutchinson, Steven / O'Malley, Pat: A Crime–Terror Nexus? Thinking on Some of the Links between Terrorism and Criminality. In: Studies in Conflict & Terrorism, 30(12) 2007, p. 1095ff.

[335] Cf. Waldmann, Peter: Terrorismus. Provokation der Macht. [terrorism - provocation of power]. Hamburg 2005, p. 71ff.

> “Since terrorism is a technique - basically boiling down to killing civilians to influence (impress, provoke, shock, coerce, harm) relevant third parties - it can be used by many different ‘players’. All you need is plenty of explosives and no scruples and the conviction that terrorism ‘works’.”[336]

Moreover, problems frequently occur in the relation between the sponsoring state and the terrorist organisation, which can for instance result from terrorist organisations changing their strategies, without having to be considerate of the interests of their sponsoring state.

Important mechanisms of the internal adaptation of terrorist organisations are in particular their strategies, which can also be regarded as as goal-oriented programmes and which are always aimed towards an uncertain future.[337] These purposeful programmes are also adaptable. Therefore, there are frequent shifts from goals to means,

> “[that generalise goals to such an extent that the achievement of the goals loses any relation to points in time and cannot be determined as being positive, nor negatively as elusiveness. Goals are confound with the values that serve as the explanation of the intended differences”[338]

One then realises that the goal, being the defeat of the adversary, is becoming temporally indeterminable and the focus is put on the means. This is what describes the frequent transformation of terrorist organisations into criminal fund-raising organisations.[339] The growing volatility in choosing terrorist targets can also be regarded as the reprogramming of purpose programmes. Therefore, it is possible that, over time, the potential targets for a terrorist organisation such as Al Qaeda can be the USA, Israel, Arabic states and even Iraqi Shiites.[340] Strategy changes in terrorist organisations

[336] Schmid, Alex P.: The Routledge Handbook of Terrorism Research. New York 2011, p. 18.

[337] Luhmann, Niklas: Organisation and Entscheidung. [organisation and decision.] Opladen 2000, p. 266.

[338] Ibid, p. 270.

[339] See Dishman, Chris: Terrorism, Crime, and Transformation. In: Studies in Conflict & Terrorism. 24(1) 2001, p. 43ff.

[340] Cf. Schneider, Wolfgang Ludwig: Religio-politischer Terrorismus als Parasit.[religio-

are furthermore also highly determined by internal social dynamics and not always compatible with the rationality of state organisations.

Nevertheless the sponsoring states have to grant the supported terrorist organisations broad autonomy – not least to be able to, in case of doubt, deny any cooperation.[341] But this can also mean that the state and terrorists pursue different objectives and strategies. Thus, terrorist organisations can use violence to an extent that is no longer compatible with the sponsoring state's intended use of attacks to apply political pressure on an opposing state. After all, the sponsoring state and the terrorist organisations each have very different sources of information at their disposal. States possess intelligence services and diplomatic channels, whilst terrorist organisations have to obtain their information mostly from mass media or from underground sources. This asymmetry of information highly limits the sponsoring state's capability to exert control over the terrorist organisation.[342] In order to force terrorists into dependency, states even take the option of recruiting competing terrorist organisations, to play them off against each other or even get them to fight each other.[343] Both terrorist organisations and sponsoring states are therefore not reliable partners in the context of such cooperation.

In contrast to SST, a state's support for partisans or guerrillas[344] and insurgents is much more self-evident and promising: their irregular combat units are, to a high degree, dependent on sponsoring states, since they usually have a larger number of members that have to be armed, supplied and salaried. They also often require weapons that are harder to obtain, such as

political terrorism as a parasite] In: Kron, Thomas/Reddig, Melanie (Eds.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven. [analyses of transnational terrorism - sociological perspectives] Wiesbaden 2007, p. 125ff, here p. 148ff.

[341] Cf. Byman, Daniel/Kreps, Sarah E.: Actors of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, p. 1ff, here p. 6.

[342] Cf. ibid, p. 7.

[343] Cf. ibid, p. 11f.

[344] For a general description, see Ibrahim, Azeem: Conceptualisation of Guerrilla Warfare. In: Small Wars & Insurgencies, 15(3) 2004, p. 112ff.

portable surface-to-air missile launchers or shoulder-fired anti-tank weapons that are oriented towards a direct confrontation with regular armed forces in the course of a 'hit and run' strategy and yet are hardly suitable for use in attacks by terrorist organisations against civil institutions.

Guerrillas have practical knowledge of asymmetric warfare, which regular armies scarcely have – it is precisely this expertise that can bring states to resort to the capabilities of guerrilla troops.[345] Indeed the support of guerrillas is more attractive than SST not least because of the much higher probability of inducing regime change in the target state, depending on the degree of success achieved by the insurgent guerrillas in their attempts.[346] In contrast with the terrorists, guerrillas raise a realisable, territorially defined claim to power: "[The guerrilla tends to occupy the territory, then later on to capture the thinking, whilst the terrorist occupies the thinking, as he cannot take the territory.]"[347] State cooperation with guerrillas is probably also easier in as far as their structures are more similar to those of regular armies and their actions cannot be so strongly hindered by the internal network of relations as is the case with terrorist organisations, due to guerrillas' relatively high degree of formalisation in their chain of command. However, it cannot be ruled out that guerrillas or partisans may also commit attacks that nerely constitute a tactical element of an asymmetric warfare strategy and do not have the same significance as within an ideal-typical terrorism strategy.

3.2.5 Conclusions

For states threatening opposing states through hybrid power projection, there are certain advantages that emerge from supporting and instrumental-

[345] Cf. Byman, Daniel / Kreps, Sarah E.: Actors of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, p. 1ff, here p. 3f.

[346] Cf. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, p. 38f.

[347] Wördemann, Franz: Terrorismus. Motive, Täter, Strategien [terrorism. motives, perpetrators, strategies]. Munich 1977, p. 57; see also Waldmann, Peter: Terrorismus. Provokation der Macht [terrorism - provocation of power]. Hamburg 2005, p. 19f.

ising terrorist groups: terrorists can politically debilitate the government of an opposing state by establishing an omnipresent threat posture. At the same time, sponsoring states can officially deny any cooperation with terrorists and still apply pressure on a target state. By doing so, a sponsoring state can effectively use force against the civil population of the target state, without this leading to a military conflict and thus to a further escalation of the conflict. Thus diplomatic channels can be kept open and still be used for the purpose of a strategy of hybrid power projection to enforce the interests of the sponsoring state. In addition, SST is also a very resource-efficient facility for power projection that represents in particular an option for states with limited military capacity. However, SST also provides an opportunity for medium-sized powers to pose as a significant threat – and to do this far beyond the limits of their own sphere of influence (and beyond the range of ballistic missiles).

However, cooperation between states and terrorist organisations is not easily possible. Initially there have to be certain highly differentiated structures in the target state's political system for the application of a terrorist strategy to make sense at all. These are in particular a state's established monopoly on the use of force, as well as a political public sphere with a free media scene, as terrorism cannot unfold the intended shock effect in areas with limited statehood and omnipresent violence, given that public media coverage is essential for the success of a terrorist strategy. Furthermore, a terrorist organisation cannot be created "artificially", but has itself to emerge initially within the framework of political protests in the political system of the target state, which is a process with many preconditions and that is controlled by coincidence. A certain ideological compliance between sponsoring state and terrorist organisation also constitutes an important precondition for cooperation against a mutual adversary. Ultimately terrorist organisations are, according to the opinion represented herein, scarcely controllable by a state, as they are particularly influenced by their internal social dynamics. Moreover, they depart from their initial strategy and definitions of adversaries for reasons of self-preservation and coherence, or to prevent inner conflicts of power, and pursue other objectives that could collide with those of the sponsoring state. Finally, it could also be conceivable that terrorists would use violence in doses larger than planned by the sponsoring state, resulting in an unwanted escalation of the conflict.

Here the support of guerrillas and insurgents has been assessed as much more probable. With regard to their armament and internal constitution, these groups are much more oriented towards regular state armies and therefore often show great structural similarities to them. This substantially facilitates cooperation with a state, since larger combat units, such as guerrillas, show a much higher degree of formalisation and a lower volatility in choosing their targets than those shown by smaller terrorist organisations. Further, there is even the chance of regime change, provided the guerrillas are successful, which is rather improbable with the support of terrorists. From the perspective of international law, the support of guerrillas is also easier to justify, as their status as combatants, in contrast with terrorists, provides them with at least a certain degree of approval. However, in both cases, whether it be the support of terrorists or guerrillas, the necessary prerequisites for hybrid power projection are not at the sponsoring state's disposal. A state that wants to enforce its will by applying such means of pressure, is in both cases always dependent on an already advanced escalation of conflict within the political system of the target state, of which it can take advantage. Hence the instrument of sponsoring terrorists/guerrillas differs from other possibilities within the framework of hybrid power projection, such as economic sanctions, intelligence operations, cyberspace attacks etc., for which a state has to resort to its own resources and infrastructure.

The description of SST proposed herein deliberately took the perspective of the sponsoring state and focused on its relations with terrorist organisations. Regarding specific recommendations as to how target states might deal with this type of hybrid threat, they can herein only be identified as *desiderata*. The objective of the reflections made herein was to provide a contribution to the understanding of problem contexts and the preconditions for possible SST. If this objective has been met, it may serve as an important proposition for the development of adequate counter strategies.

3.3 Cybersecurity – Raising Awareness in Society

Alfred Gulder

As part of the project "Hybride Bedrohungspotenziale und daraus resultierende sicherheitspolitische Ableitungen für Kleinstaaten" [potential hybrid threats and the consequent security-policy-related deductions for small states] at the Institute for Peace Support and Conflict Management (IFK), particular emphasis was placed on analysing the threat factor of cybersecurity for the three reference states, the Netherlands[348], Sweden and Slovakia.

The basis for this was set by the findings from the IFK's preliminary study "Hybridität politischer Machtprojektionen" [hybridity of political power projections], which reveal the influences of hybrid threat potentials and factors in the Great Powers USA, Russia, China and India, and illustrate their strategies for dealing with them. Based on these findings, a deduction of these power projection mechanisms shall be made, regarding the three reference states mentioned above, in order subsequently to draw possible conclusions regarding perceived threats from the Austrian perspective, particularly considering the cyber component. Power projection is defined as:

> "The ability of a nation to apply all or some of its elements of national power - political, economic, informational, or military - to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability."[349]

An example for an earlier, classical objective of power projection is the struggle over resources, which was in the past realised by means of ships and airplanes.

[348] Since there were data on the field of cybersecurity in the Netherlands, provided through an expert talk, the decision was made to include them in this section.

[349] Definition of power projection. <http://www.dtic.mil/doctrine/dod_dictionary/data/p/10683.html>, accessed on 13/02/2016.

Today the roles of objectives and means of the realisation are considerably more distinct, in particular in the field of information and communication technology (ICT). At the same time, nearly the entire national economy of a state (energy supply, financial system etc.) depends on a functioning ICT infrastructure that has to be protected. However, to enforce political or economic interests for example in another state as power projections, it is specifically those critical areas that have to be harmed. A short or long-term harm to the ICT areas can be effected through, for example, a cyber-attack on critical infrastructure, with consequences that are, to date, only theoretically estimable.

An IFK project from 2011-2013 covered and explained recognised hybrid threat factors for Great Powers. From that work, cyber threats have already been presented as a crucial element of power projection. This element shall now be more specifically analysed for the 3 reference states within various subject areas. Based on the fields of action from the “Austrian Cyber Security Strategy“, the subject areas have been reasonably adapted and used as the foundation for the enquiry. Therefore, the following subject areas have been evaluated and the result is presented on the subsequent pages in tabular form.

- What does the threat scenario look like?
- Are there defined overall concepts/methods of resolution?
- Are there defined strategic objectives?
- Are there drafted structures and processes? (Roles, responsibilities, competencies of state and non-state actors.)
- Is there a drafted cooperation between state, economy and society?
- How does national collaboration with the military take place?
- How does an international collaboration take place and what does the embedding in security organisations (e.g. NATO) look like?
- How are sensitising and training performed?
- How are research and development performed?
- How is the protection of critical infrastructure performed?

Findings from the analysis of the three reference states, Netherlands, Sweden and Slovakia (See Table 5 for details):[350]

In recent years, assessments have been made in all three states to work out a detailed national situation overview and *threat scenario* regarding cybersecurity. The core elements stated are the loss of information confidentiality, digital espionage and the implanting of computer viruses. Cyber-crime is also increasing in significance, albeit with a background of fraud by professional criminals, and should rather not be rated as power projection.

From the assessments, *methods of resolution* and strategic objectives have been defined, which have been written down in a national document on cyber strategy in all three states. The number of defined strategic objectives spans from three in Slovakia to five in the Netherlands and Sweden.

The Netherlands' *strategic objectives* focus on an intensified national and international collaboration, those of Sweden focus also on collaboration and the provision of capabilities and those of Slovakia on prevention and commitment.

Regarding the pooling of cybersecurity activities and the *creation of national structures*, in the Netherlands a National Cyber Security Centre had already been put into operation by the beginning of 2012. In Sweden and Slovakia there are several contact points acting in various ministries. Sweden's Civil Contingencies Agency (MSB) should undertake the implementation of a national, operational coordination point for cybersecurity. Hence, it was recognised that too many stakeholders, with partially unclear tasks and interfaces, cannot operate effectively.

All states have an international networked Computer Emergency Response Team (CERT) operationally in service, as a *point of contact for commerce*.

[350] Federal Chancellery of Austria: Austrian Cyber Security Strategy. <http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf>, accessed on 13/02/2016.

National collaboration with the military is carried out similarly in all three states. In the Netherlands a “Defence Strategy for Operating in Cyberspace“, with six areas of action, has been defined additionally. In Sweden, military collaboration and the exchange of information is performed through a National Cyber Defence Organisation, in Slovakia through the Ministry of Defence’s Institute of Security and Defence Studies.

International civil collaboration in all 3 states is performed through the European Government Computer Emergency Response Team. *Military cooperation* is executed through bilateral communication and the exchange of best practices with the most important partner, NATO, and NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estonia. Further, local networking with the neighbouring states is in Sweden constituted through the Nordic Defence Cooperation (Norway, Finland, Sweden, Iceland, Denmark).

Training courses for qualification and further education are accessible via the Internet and well developed through respective training centres in all three states. Various documents and series of papers are being provided.

In the case of *research and development*, coordination of research programmes between institutions is conducted in the Netherlands via the National Cyber Security Council, in Sweden by the military institutions of the Swedish Defence Research Agency and in Slovakia through at least three universities.

For *critical infrastructure protection*, a platform (Centre for Protection of National Infrastructure) has been established in the Netherlands for the area of critical sectors for the exchange of information on incidents, threats, vulnerabilities and good practice. As early as 2005, the National Telecommunications Coordination Group was founded in Sweden, which assists in restoring national infrastructure for electronic communication. In Slovakia this task is performed by the Governmental Computer Security Incident Response Team.

Conclusions and deductions for Austria:

Austria is acting nationally and internationally[351] in the cybersecurity sector. In March 2013 a cybersecurity strategy was compiled, defining the following 7 fields of action.

- Structures and processes
- Governance
- Cooperation between state, economy and society
- Critical infrastructure protection
- Sensitising and training
- Research and development
- International collaboration

The perceived threats for Austria are illustrated in the cybersecurity strategy's Appendix 1 as cyber risk matrix 2011. Threats named as having devastating consequences alongside high probability of occurrence include non-detected ICT anomalies, malware and cyber-espionage.

The "National ICT Security Strategy Austria"[352] was published in 2012 and describes the strategic objectives and measures in five core areas:

- Stakeholders and structures
- Critical infrastructure
- Risk management and situation assessment
- Education and research

[351] Federal Chancellery of Austria: Austrian Cyber Security Strategy. <http://www.bmi.gv.at/cms/BMI_Service/cycer_security/130415_strategie_cybersicherheit_en_web.pdf>, accessed on 13/02/2016.

[352] Federal Chancellery of Austria: National ICT Security Strategy Austria, 2012. <https://www.digitales.oesterreich.gv.at/DocView.axd?CobId=48411>, accessed on 13/02/2016.

The security strategy names all stakeholders involved and their collaborations. The extent to which the practical implementation of the collaboration is applied cannot be verified. At least there are many initiatives in Austria for collaboration between society, economy, interest representation groups, academia and the public domain, as well as projects for raising "awareness".

In 2008 a master plan for critical infrastructure protection (APCIP = Austrian Program for Critical Infrastructure Protection) was adopted by the cabinet, laying down principles, responsibilities and particular operational steps for developing an Austrian programme on critical infrastructure protection, thus being the starting point for the implementation process on a national level.[353]

The national security research programme KIRAS acts in boosting security research in Austria and supports national research plans, with the aim of increasing security for Austria and its population.

Regarding the collaboration with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallin, Estonia, Austrian experts already participated in the "Locked Shields 2012" exercise in 2012. Urgent consideration should be given to finding an agreement on cooperation with NATO (similar to Slovakia), giving Austria the possibility to cooperate with other NATO states in the event of cyber-attacks and to assist in developing guidelines for a practical cooperation with other NATO partners in the cybersecurity area.

[353] Cf. Austrian Program for Critical Infrastructure Protection (APCIP). Adopted by the cabinet on 02/04/2008. <https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/schutz_strategischer_infrastrukturen/150211_APCIP_Bericht_BF.pdf?59kpl7>.

- Compared with the reference countries, the Netherlands, Sweden and Slovakia, Austria is well positioned, showing theoretically clear structures and responsibilities.
- Collaboration with the various stakeholders has to be examined and critically questioned by conducting practical cybersecurity assessments – similar to the assessments conducted annually in the Netherlands.
- It should also be considered to pool Austrian cybersecurity activities in a national coordination centre – as already done in the Netherlands and currently being established in Sweden.
- The civil and military collaboration or the expansion of information exchange on national and international levels, such as with the NATO centre CCDCOE, is one of the key factors for fighting cyber-attacks in Austria in a more timely and more effective manner or for being able to prevent them.

Subject area	Netherlands	Sweden	Slovakia
1. Threat scenario	Since 2011 the Netherlands annually perform the so-called Cyber Security Assessment in cooperation with ministries, military, economic and research institutions, to assess actors, threats, vulnerabilities, resilience and the instruments and methods used. The major threats named in the findings are digital espionage (particularly from the states Russia, China and Iran), disruption due to malware infections and spam and digital (identity) fraud. The 2013 assessment revealed that the biggest dangers are still originating from secret activities by professional criminals and states. The biggest threat for the government is related to information confidentiality and service continuity.□	In 2009 a Situational Assessment regarding information security was conducted in Sweden. The threat scenarios stated at that time were cyber-crime, and the loss of information confidentiality. More recent data could not be found.	The “National Strategy for Information Security of the Slovak Republic” identified the fastest growing threats as being the vulnerability of information and communication systems, their over-stressing, unauthorised access to information, the spreading of computer viruses and misinformation.

Subject area	Netherlands	Sweden	Slovakia
2. Overall concept/ methods of resolution	In June 2011 the Dutch government adopted "The National Cyber Security Strategy (NCSS)" document which describes the overall concept regarding cyber strategy, including the actors.	On February 1st 2010 the MSB (Swedish Civil Contingencies Agency) act on information security at authorities (MSBFS 2009:10) came into force. The government assigned MSB with the administration of the national action plan for information security (updated in 2010). Four areas have been determined as focal points: – There is a need for enhanced multi-sectoral and cross-sectoral work on societal information security. – A fundamental security standard for information security has to be established. – Society has to be capable of dealing with extensive IT-related disruptions and crises. □ – There is a lack of information security expertise at all levels of society. There is a need for extensive investment in qualifications in this area. - Es besteht ein Mangel an Information Security Know-how auf allen Ebenen der Gesellschaft. Weitreichende Investitionen in die Qualifizierung in diesem Bereich sind notwendig.	The "National Strategy for Information Security of the Slovak Republic" document was approved by the Slovakian government in August 2008. The national strategy for information security contains security for critical infrastructure, emphasises the prevention of attacks, building up defence and the maintenance of sustainable infrastructure.

Subject area	Netherlands	Sweden	Slovakia
3. Are there defined strategic objectives?	The document “The National Cyber Security Strategy (NCSS)”, June 2011) describes the following five strategic objectives: - Initiatives on linking and strengthening - Demanding individual responsibility - Creation of public-private partnerships - Demanding international collaboration - Creating a balance between self-regulation and legislation	The “STRATEGY FOR SOCIETAL INFORMATION SECURITY 2010 – 2015” document illustrates the following five strategic areas: - Information security in businesses - Provision of skills - information exchange, collaboration and answers - security in communication - security of products and systems	The “National Strategy for Information Security of the Slovak Republic” document contains 3 strategic objectives: - Prevention (to achieve adequate protection and minimise the occurrence of security-relevant incidents) - Commitment (establishing sufficient capacities to provide an effective reaction to security-relevant incidents, minimise their impacts and enable a timely restoration of the systems harmed) - A steady and sustainable level at INFOSEC (build-up, maintenance and development of know-how).

Subject area	Netherlands	Sweden	Slovakia
4. Are there drafted structures and processes? (Roles, responsibilities, competencies of state and non-state actors.)	The Cyber Security Council and the National Cyber Security Centre (NCSC) have been acting since 01/01/2012, in charge as national contact points. The Centre also contains GOVCERT.NL. The following responsibilities have been defined: The Ministry of the Interior coordinates inter-departmentally the issue of cybersecurity between various civil and military units responsible for cyber issues. Further, the Ministry of the Interior is responsible for the inter-ministerial coordination regarding cybersecurity through the National Security Programme.	Currently various institutions share the tasks and competencies. The Ministry of Enterprise, Energy and Communications, the Ministry of Justice and the Ministry of Defence are responsible for the coordination of the development of the national information-security policy/strategy, legislation and research in the field of cybersecurity. The execution of strategic policy is performed by the organisations supervised by the ministries named.	The following responsibilities have been recognised: The Ministry of Finance is named as the responsible national authority for information security for the subject of non-classified information. The National Security Authority, an independent state body, is, as a national security agency , responsible for the subject of classified information. The Government Plenipotentiary for Information Society is responsible for coordinating the Information Society.

Subject area	Netherlands	Sweden	Slovakia
	Cyber-crime is covered by the Ministry of Justice. Cyber terrorism is within the responsibilities of the national counter-terrorism coordination (NCTB). Cyber defence is a mutual responsibility between the Ministry of Defence and the Ministry of the Interior. Agencies (such as OPTA and the Netherlands Consumer Authority), government inspectorates (such as the Health Care Inspectorate), private enterprises (such as ISPs and security vendors), and national and international knowledge and research institutions.	Currently various institutions share the tasks and competencies. The Ministry of Enterprise, Energy and Communications, the Ministry of Justice and the Ministry of Defence are responsible for the coordination of the development of the national information-security policy/strategy, legislation and research in the field of cybersecurity. The execution of the strategic policy is performed by the organisations supervised by the ministries named. .	The Commission for Information Security, supervised by the Ministry of Finance, acts along with the Slovakian government as national authority for decision-making processes for the development of a policy for information security. The commission is a task force composed of the staff from the Ministry of Finance, national network and information security interest groups (such as other ministries) and external experts in the field of information security.

Subject area	Netherlands	Sweden	Slovakia
	Critical national infrastructure is handled by the Ministry of Economic Affairs. Further, the following bodies have to be mentioned: -AIVD (General Intelligence and Security Service) - MIVD (Military Intelligence and Security Service) - police, special investigative services (such as FIOD and SIOD), regulatory authorities (such as OPTA and the Netherlands Consumer Authority), government inspectorates (such as the Health Care Inspectorate), private enterprises (such as ISPs and security vendors), and national and international knowledge and research institutions.	- The Cooperation Group for Information Security (SAMFI) consists of: - Swedish Civil Contingencies Agency (MSB), responsible for the improvement and support of societal capacities for preparations in the event of and the prevention of emergencies and crises - Swedish Post and Telecom Agency (PTS) functioning as a regulatory authority for electronic communication (telecommunication, Internet and radio) and for using electronic signatures - Swedish National Defence Radio Establishment (FRA) acting in information security. On request, Försvarets radioanstalt (FRAU) supports authorities and state enterprises with current IT-threats and provides general advice to improve security.	The commission cooperates with Slovak Telecom, the Personal Data Protection Office, the Ministry of the Interior and the National Security Authority. The commission is responsible for the assessment of the proposed security standards for the protection of information security systems of the public administration in the context of non-classified information, the submission of security standard proposals, the amendment or modification of existing security standards for information security systems of the public administration.

Subject area	Netherlands	Sweden	Slovakia
		- The Swedish Security Service (Sapo) and the Swedish Criminal Investigation Service (RKP) are responsible for cyber crime - The Swedish Defence Materiel Administration (FMV) / Swedish Certification Body for IT Security (CSEC) is responsible for the regulatory authority for electromagnetic compatibility (EMC) - The Swedish Armed Forces (FM)/Military Intelligence and Security Service (MUST) are responsible for the military aspects of cybersecurity and cyber war.	

Subject area	Netherlands	Sweden	Slovakia
5. Is there a drafted cooperation between state, economy and society?	The NCSC also includes GOVCERT.NL (Computer Emergency Response Team) and is further considered the contact point for economy and society via the ICT Response Board (IRB). See also Point Structures: a CERT.NL for the civil component is drafted.	Cooperation is performed through the Cooperation Group for Information Security (SAMFI) and consists of the organisations named above. Every 2 months a voting meeting is held. Publications for economy and society are published at https://www.msb.se/en/Prevention/Information-security/Information-security-publications/ Further, there has been a CERT-SE draft since 01/01/2011.	CSIRT.SK (Computer Security Incident Response Team), predominantly active for the government in the event of attacks on national critical infrastructure, the public administration or the corporate sector (not for classified information and military incidents). A CERT.SK for civil issues is also operating.

Subject area	Netherlands	Sweden	Slovakia
6. How does national collaboration with the military take place?	Cooperation with the Defence Computer Emergency Response Team (DefCERT). □ Further, the document “Defence Strategy for Operating in Cyberspace” from June 2012 contains the following six fields of action: Adopting a comprehensive approach; Strengthening the cyber defence of the defence organisation (defensive element) Developing the military capability to conduct cyber operations (offensive element) Strengthening the intelligence position in cyberspace (intelligence element) Strengthening the knowledge position and the innovative strength of the defence organisation in cyberspace, including the recruitment and retention of qualified personnel (adaptive and innovative elements)□ Intensifying cooperation, both nationally and internationally (cooperation element).	Collaboration takes place between the Swedish Armed Forces (FM)/Military Intelligence and Security Service (MUST) and the Swedish National Defence Radio Establishment (FRA). In January 2013 a National Cyber Defence Organisation was formed, interchanging information from the cyber units of the organisations FRA, MUST and the national intelligence service and SAPÖ. Further, there is collaboration in the field of cyber defence and cybersecurity in the context of the Nordic Defence Cooperation (NORDEFCO) between Norway, Finland, Sweden, Iceland and Denmark.	Collaboration takes place between the Institute of Security and Defence Studies of the Ministry of Defence. The institute is responsible for the professional preparation of the documents for decisions in the field of security, defence and crisis management.

Subject area	Netherlands	Sweden	Slovakia
7. How does an international collaboration take place and what does the embedding in security organisations (e.g. NATO) look like?	International networking including: - European Government CERTs, ENISA (European Network and Information Security Agency) - International Watch and Warning Network (IWWN) - International network of Computer Security and Incident Response Teams (CSIRTs); particularly Poland, Australia, the USA and Japan. - Bilateral communication and exchange of best practices with the most important partner, NATO, and the NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estonia.	International networking including: - European Government CERTs, ENISA (European Network and Information Security Agency) - Bilateral communication and exchange of best practices with NATO on an agreement on cooperation and with the NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estonia - Military networking in the context of the Nordic Defence Cooperation (NORDEFCO) between Norway, Finland, Sweden, Iceland and Denmark.	Besides Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Spain and the USA, Slovakia is a sponsor of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Further, Slovakia has signed an agreement with NATO providing the possibility to cooperate with other NATO states in the case of cyber-attacks and to assist in developing guidelines for a practical cooperation with other NATO partners in the cybersecurity area

Subject area	Netherlands	Sweden	Slovakia
8. How are sensitising and training performed?	The NCSS describes cybersecurity education and operates a training centre. □ Further, users can register at <http://www.waarschuwingsdienst.nl/> and receive alerts automatically.	The Swedish Post and Telecom Agency can point to the following strategy for training and exercises in the field of cybersecurity: - A series of papers on the protection of information security can be found on the MSB's homepage (<www.msb.se/en/Prevention/>), which is also responsible for disaster management. - In 2011 the "National Response Plan for Serious IT Incidents" was published, describing cooperative approaches with industry and other institutions to minimise disruption.	The Slovak Association for Information Security (SASIB) has the aim of supporting its members' legal awareness and know-how regarding information security and software protection in the professional and public field. Training is also provided by the SCIRT.SK, according to the website <https://www.csirt.gov.sk> .

Subject area	Netherlands	Sweden	Slovakia
9. How are research and development performed?	The National Cyber Security Council coordinates research programmes between institutions and the corporate sector.	Research in the public sector is performed through, among others, the Swedish Defence Research Agency (FOI), a leading European research facility in the field of defence and security. FOI also develops systems for crisis management in the context of serious accidents and catastrophes. The current SCADA (Supervisory Control and Data Acquisition) project shall be named as an example, which includes research on security of industrial regulatory and monitoring systems.	Research and training take place at universities including: - Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University - Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava - Faculty of Electrical Engineering and Informatics, Technical University of Kosice

Subject area	Netherlands	Sweden	Slovakia
10. How is the protection of critical infrastructure performed?	The Centre for Protection of National Infrastructure (CPNI) is a platform on which critical sectors and public sector entities can share information on incidents, threats, vulnerabilities and best practice in the field of cyber-crime and cybersecurity, in a trustworthy environment. The aim being the increase of resilience against disturbances, particularly in the energy sector (EyeforEnergie). The AIVD's (General Intelligence and Security Service) National Communications Security Agency (NBV) promotes the protection of special information through provision and support in implementing approved security products, provisions and standards, and gives advice on the issue of information security.	The National Telecommunications Coordination Group (NTSG) was founded in August 2005 and is a voluntary cooperation platform to support the restoration of national infrastructure for electronic communication in the context of extraordinary events in society. The criterion for membership of the NTSG is that operators/ organisations, who run critical infrastructures for electronic means of communication in Sweden, have to bring in their own technical equipment, skills or resources.	The protection of critical infrastructure is the responsibility of CSIRT.SK (governmental Computer Security Incident Response Team), which also conducts national exercises in this field.

Table 5: Cybersecurity – comparative table of the Netherlands, Sweden, Slovakia
Alfred Gulder

3.4 Implications of Hybrid Threats in International Law

Christoph R. Cede, Reinmar Nindler and Paul Schliefsteiner

The following discussion addresses the potential implications of the concept of "hybrid threats" in terms of international law. This is limited solely to an initial framing of the problem, which certainly requires deeper consideration. On the one hand this framing of the problem deals with deductions relating to international law that already result from the elements of definition of the term "hybrid threats" and, on the other, with potential implications according to international law that arise from the nature of the hybridity of threats.

The definition of the concept of hybrid threat already contains (international-) legal terms. Thus for example a "state" is delineated in international law, according to Jellinek's three-element-model, by a state people, state territory and state sovereignty. It may be necessary to treat hybrid threats from a *failed state*, a *failing state* or a *de-facto regime* differently according to international law.

The degree of how specifically targeted the hybrid threat is, can have an important role in connection with the prohibition of the use of force for example. In contrast, the terms "capability", "potential" and "coordinated in time" are irrelevant in terms of international law, because the assessment of a situation according to international law is to be limited exclusively to the matters of fact.

However, alongside the terms clearly defined in international law, there are also some terms in the definition that must be examined more closely in each individual case. Thus in the case of "actor", there must be a strict distinction between state and non-state actors, because these categories can often invoke differing legal consequences. Non-state actors, e.g. armed groups acting on behalf of humanitarian international law, individuals or de-facto regimes, are often associated with a state politically and, in certain cases, legally too. It might be the case that a simple omission by a state is sufficient to constitute legally relevant accountability, or instead that action has to be present. If action is present, it is also necessary to question the extent to which it constitutes national responsibility, given that the International Court of Justice (ICJ) and International Criminal Tribunal for the former Yugoslavia (ICTY) demand "effective control" and "overall control" respectively. Thus it matters how determinable the chain of command is, albeit with the question of provability also becoming potentially important in practice. This can become a problem above all if the threatened state deploys measures (such as retorsion or reprisal) and justifies them on the basis of a threat from an actor, whose accountability cannot be proven. Quite apart from the general relevance under international law of the accountability of private and other non-state actions, the question of particular relevance to hybrid threats is how to proceed if individual levels of threat are attributable to different states.

The pairing of terms endangerment/threat is also not defined in any greater detail although, in terms of international law, the question of directness arises, i.e. whether the endangerment/threat is actually present, perhaps with the immediate threat of military attack, or whether simply some hypothetical potential threat will be present in the future. In no case can international legal consequences be derived solely from the definition of a threat as being "hybrid"; every consequence according to international law must always be geared to the circumstances of the individual case; for example regarding the threshold of force that has to be reached for an armed attack to exist according to international law. In relation to the closely connected right to self-defence in the face of hybrid threats, it is therefore also necessary to clarify the extent to which the latter justify the conditions for legally compliant use of various types of countermeasures.

One particular potential consequence of the hybridity of a threat in terms of international law is that, whilst the components of the threat might individually be legally compliant on many or indeed perhaps all levels, the resulting overall threat could nevertheless violate international law.

4 Summary and Conclusions

Anton Dengg

As a result of an ever increasingly networked structure, our society is becoming ever more vulnerable in practically all areas of life. The higher the degree of networking of structures, the more evident possibilities for hybrid threats become. Increasing insecurity about threats and actors will also dominate future perceived threats. Our future perceived threats will be defined by numerous influencing factors, as also stated in the Austrian partial strategy for defence policy.[354]

Hybrid warfare is indeed featured increasingly in international publications[355] as a new threat. Yet in the current conflict in the Ukraine, it is evident that conflicts are not waged solely by conventional, military, means, but rather that a great variety of other categories of exercising power find application. Thus, as a result of the possibility of using options for projecting state power to influence the capacity of other states to act, new threats emerge at a national level.

4.1 Summary

The Institute for Peace Support and Conflict Management (IFK) of the National Defence Academy has been working since 2011 on the research topic of "future conflict and threat scenarios" with hybrid threats. Here the focus is on the new potential, enabled particularly by technical developments, for states to wield power over other states.

Originally central among research interests at the IFK was the possibility of power projection by larger states (USA, Russia, China and India). In 2013,

[354] BMLVS: Teilstrategie Verteidigungspolitik, p. 5. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf>, accessed on 16/10/2015.

[355] E.g. Frank G. Hoffman: Hybrid Warfare and Challenges. JFQ, issue 52, 1st quarter 2009.

for more in-depth research, two comparable industrialised small European states were selected alongside Austria on the basis of structure, size of army, involvement abroad etc.: Slovakia and Sweden. In addition, the selected states were not only to demonstrate similarities and thus be comparable, but also had various alliances (e.g. UNO, NATO, non-aligned). The intent was accordingly to investigate whether the selected states might tend to rely more on alliance partners in the event of hybrid threats.

Initial analyses as part of the "potential hybrid threats and resultant security policy deductions for small states" project demonstrated the existence of plenty of material about "hybrid warfare", but scarcely any findings on hybrid threats that extended beyond "hybrid warfare" were present in the opinion of the IFK.

The objective of the project was to examine the security policy concepts of selected small states with regard to their appraisal of current threats. The intent was for findings and conclusions, particularly those relating to perceived threats and potential protective or defensive measures, to allow deductions to be made for small states and particularly for Austria. The project's research questions were:

- To what extent are potential hybrid threats at a national level registered and what strategies and concepts exist for tackling them?
- How significant is inclusion in security organisations, e.g. NATO?
- Is an interdependency between participation in the ICCM and the associated risks within the sending state perceived to be a threat and what are the effects of this in the context of overall national security provision?

Given that there were scarcely any international research results regarding hybrid threats, at the start of the project it was necessary to develop a working definition of "hybrid threats". As a result of a number of working sessions, the definition of a hybrid threat was ultimately tested and a working definition was laid down as follows:

> *A hybrid threat is a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests.*[356]

A significant aspect associated with this working definition is that the threat scenario must exceed the "strategic threshold" of a state. The IFK sees this as applying if the freedom of the state under attack to act or decide is substantially limited. At least two categories of hybrid threats must be used and defending against them must involve at least two ministries.

Joseph S. Nye's hard and soft power concept is the basis for the IFK project. For Nye, power can be wielded if one is in possession of the requisite possibilities or appropriate resources to be able to exert adequate influence.[357] Thus a threat can only emanate from those actors who not only have the will but also the necessary means to exercice power. According to Nye, power can be wielded in two forms: hard and soft power. An additional form of power – smart power, a mixture of those above – also counts, according to Nye. Nye describes hard power as incentive/threat tactics ("carrot and stick")[358], whilst he describes soft power more as the effort of convincing an entity to strive for values perceived as ideal.

Soft power comes to be applied successfully if an actor is convinced by the arguments applied and follows suit. Soft power is founded on cultural and political ideals as well as foreign policy, if the latter is judged to be legiti-

[356] Working definition developed by the Institute for Peace Support and Conflict Management of the National Defence Academy (Dengg/Feichtinger/Schurian) according to: Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald/Schreiner, Karl H. and Bruzek, Oliver. Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000.

[357] Cf. Nye, Joseph p. Jr.: Soft power. The Means to Success in World Politics. PublicAffairs 2004, p. 3.

[358] Ibid p. 5.

mate. Smart power, on the other hand, is "[...] the ability to combine hard and soft power into a successful strategy."[359]

In this publication, the topic of hybrid threats is addressed comprehensively with regard to many aspects, using examples for deeper illustration. Raising awareness of the area of hybrid threats as a future challenge was the highest ranking objective of this work. Core statements are brought together from a variety of viewpoints, accompanied by potential deductions for those active in security. In the project, using an empirical and analytical approach, actual material forming part of the security analyses of two selected reference states (Sweden and Slovakia) was examined for mention of hybrid threats and "bare patches" were identified. In the analysis component there is also some brief reflection on Austrian security strategy and examination of its relationship to the topic of "hybrid threats".

Analysis Results

To date this kind of threat has remained underrepresented in papers on security strategy. As mentioned above, security policy experts currently deal primarily with the term "hybrid warfare", which actually belongs in the domain of "hard power". For the requisite counter-strategies, the main focus is consequently more on a simple cause-and-effect level. The response to action rated as a threat is a proportionate counter-reaction. Thus terrorism, for example, is fought by means of an anti-terrorism strategy; the response to organised crime is via appropriate interior ministry security structures; attacks carried out using military resources are countered by armed forces. Various interactions of complex systems and relevant phenomena emerging as a result in terms of security policy are scarcely anchored in our patterns of thought.

Perceptions of threat are shaped by concepts of hard power, guiding the necessary countermeasures. The threat by means of soft power scarcely

[359] Nye, Joseph: Smart power. The Blog. <http://www.huffingtonpost.com/josephnye/smartpower_b_74725.html>, accessed on 16/10/2015.

attracts attention. Particular attention in terms of security policy should actually be paid to technological developments. For example, the Internet and thus also cyber components can massively amplify both hard and soft power effects.

Hybrid threats are to be found in practically no national security analyses. Only in the Swedish military doctrine 2012 and the "Austrian defence strategy 2014" is there mention of the term hybrid warfare or hybrid threats. If one assumes that the term hybrid threat is broader than hybrid warfare, this perceived threat also implies the necessity of comprehensive, state-level countermeasures. This state-level approach requires cooperation not only inter and intra-ministerially but also with other experts (often at an interdisciplinary level). There is a need for not only a national but also an at least pan-EU committee which, through continuous situation assessment, promptly recognises a hybrid threat development and consequently either invokes appropriate countermeasures/reactions or appropriately informs national (international) security experts as well as the general population. Regarding international crisis and conflict management, the "hybrid threat" factor should always be evaluated. It is all to easy for interministerially constituted national actors to be exposed to hybrid threats whilst on peace missions, only then to propagate a chain reaction on the relevant home country. In this way, hybrid threats can spill over into the home nation and lead to a variety of multiplication effects. Analyses of hybrid threats are deserving of particular interest when various different nations take part in peace missions. This applies particularly if states are exposed to differing levels of threat and then less affected states experience the elevated security risk of other states. In the various security analyses, mention is indeed made of actors who could constitute potential threats for states, albeit their potential cooperation and the synergy effects that might emerge as a result are not to be found. Challenges result in the context of hybrid approaches, particularly in relation to critical infrastructure[360] such as the cyber domain, power generation or

[360] The European Commission sees critical infrastructure thus: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, sa-

transportation and access routes. In brief, hybrid threats always present a hazard to critical infrastructure. Therefore the protection of critical infrastructure is also to be seen as protection against hybrid threats. Currently threats are generally perceived as being challenges to be treated as either serial (and unconnected) or individual and sectoral. Consequently, counter-strategies are also deployed serially and against the individual actor. Yet it is precisely in the case of hybrid threat patterns that a paradigm shift must occur.

The NATO Allied Command Transformation (NATO ACT) scenario experiment on "Countering Hybrid Threats" shows that, for an appropriate counter-strategy against hybrid threats, only a "comprehensive approach"[361] is productive. From this NATO assessment it follows that comprehensive collaboration is demanded not only on a national but particularly on an international level, in order to counter hybrid threats.

Even though, in its security strategy, the EU assumes a combination of different elements constituting a potential threat[362], no security policy spotlight falls on "hybrid threats". Only in the case of critical infrastructure protection can one recognise signs of an approach to combating hybrid threats. In contrast, in its security strategy Austria does indeed lay out a

fety, security or economic well-being of citizens or the effective functioning of governments in the Member States."; Commission of the European Union: Communication from the Commission to the Council and the European Parliament; Brussels, 20/10/2004, COM(2004) 702 final. < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702 >, accessed on 14/10/2015.

[361] "The comprehensive approach indicates a collective effort towards a coordinated and complementary approach in the context of ICCM at an international level." (see Feichtinger, Walter/BraumandlDujardin, Wolfgang: Part 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/BraumandlDujardin and Gauster, Markus (Eds.): Comprehensive Approach. Vom strategic Leitgedanken zur vernetzten Politik. National Defence Academy publication series 8/2011. Vienna 2011, p. 23). In this report, the term is also interpreted as a comprehensive, coordinated application of all intrastate forces and resources to defend against hybrid threats.

[362] Council of the European Union, A secure Europe in a better world, p. 5. <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>, accessed on 14/10/2015.

comprehensive approach to security and yet hybrid threats are not an explicit topic.

The Austrian Security Strategy

The currently valid Austrian security strategy (ÖSS) states that the "[...] security situation in Europe is now marked by new challenges, risks and threats [...]"[363]. There are no references to potential hybrid threats. Nevertheless, in its security strategy, Austria concludes that the challenges are becoming more complex, more strongly intertwined and, additionally, less predictable.[364] Reference is made to the simple fact that, from now on, complex security problems can only be solved through international cooperation.[365] Precisely this applies to the new challenges of the 21st century, which will be primarily of a hybrid nature. Numerous threats are listed in the ÖSS. There is no consideration of a networked interplay between several of the listed threats, which would result in a substantial increase in complexity. Associated with that would be an amplified unpredictability of developments and, in turn, greater difficulty planning countermeasures.

The depiction of conflict addressed in the ÖSS is comprehensive, nevertheless – even if the simultaneous appearance of the individual threats were not excluded *per se* – it envisages something more of a self-contained activity. Targeted, multi-dimensional and temporally defined activity by an actor was not explicitly analysed.

Nevertheless worthy of emphasis is the broad understanding of security, which must "[...] be based on a comprehensive and integrated approach, allow for active participation and be implemented in the spirit of solidarity"[366] – thus fundamental prerequisites for countering hybrid threats. Here

[363] Federal Chancellery of Austria, Austrian security strategy. Security in a new decade – Shaping security. Vienna, July 2013, p. 4.

[364] Ibid, p. 4.

[365] Ibid, p. 5.

[366] Ibid, p. 4.

too, great significance is attached to "whole-nation"[367], "whole-government"[368] and "comprehensive approach" positions, involving the assumption that the significance of individual states in this context will reduce. At the same time, reference is also made to the increasing relevance, economically and in terms of security policy, of a number of powers.[369]

On the basis of the observation that

> "[s]ecurity decisions at both national and international level must be based on a comprehensive assessment of the situation by all of the stakeholders and a common understanding of the situation derived from this in-formation [and] [...] efforts must be made to establish security synergies within the context of a collective national "security cluster"[370]

This also represents a basis for dealing with hybrid threats. Nevertheless, concentrated, targeted, multi-dimensional and temporally-defined hybrid power projections, as also mentioned in other analyses, foreign security policy strategy papers, are not examined as topics.

[367] "If, in a specific case, states act to involve NGOs too, then whole-of-nation coordination follows. Such a case is termed a Whole of Nation Approach (WoNA)." (see Feichtinger, Walter/Braumandl Dujardin, Wolfgang: Part 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/BraumandlDujardin and Gauster, Markus (Hrsg.): Comprehensive Approach. Vom strategic Leitgedanken zur vernetzten Politik. National Defence Academy publication series 8/2011. Vienna 2011, p. 24).

[368] "In the area of WoGA *(N.B.: Whole of Government)*, national measures for international peace efforts are prepared and coordinated both inter and intra-ministerially. In WGA, the individual CA *(N.B.: Comprehensive Approach)* contributor determines what means he can make available in what form and to what extent in order to support international engagement." (see Feichtinger, Walter/BraumandlDujardin, Wolfgang: Part 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/BraumandlDujardin and Gauster, Markus (Eds.): Comprehensive Approach. Vom strategic Leitgedanken zur vernetzten Politik. National Defence Academy publication series 8/2011. Vienna 2011, p. 24). In this piece of work, this term also links the inter and intra-ministerial coordination for interior defence.

[369] Federal Chancellery of Austria, Austrian security strategy. Security in a new decade – Shaping security. Vienna, July 2013, p. 5.

[370] Ibid, p. 10.

Going one step further than the ÖSS is the "Austrian defence strategy 2014". Here the hybrid factor is mentioned several times, albeit more in a hard power context.

Security policy strategies of Slovakia and Sweden

Almost without exception, the national security strategies analysed yielded differing offensive actors. Hybrid threats received no coverage, whether as a general phenomenon or as an example. Nevertheless actors emerge as a consequence with the potential to present a hybrid threat to a state. Among these are not only states but also non-state actors, such as terrorist organisations or globally active commercial enterprises. Yet a connotation between these actors and hybrid threats cannot be drawn. In the strategy papers analysed there is not even consideration of the potential "support" of achieving an actor's own objectives by means of terrorist organisations.

The topic of critical infrastructure receives differing weightings from the states examined, by inference from the frequency of mention of the nominated terms in the strategies. But for protecting critical infrastructure (SKI), the states developed their own concepts, which deal with the material in greater depth. Regarding practicable concepts for solutions to the SKI, it is in turn possible to recognise the need for an intrastate comprehensive approach in the strategy papers of the states examined. Accordingly, for the states analysed, the concepts for a comprehensive national security provision for the protection of critical infrastructure bear the greatest resemblance to potential counter-strategies against hybrid threats. In the ÖSS there is elevated attention directed towards the SKI. Here particular attention is directed toward the "[t]hreats from state and non-state actors, both in and from cyber space [...]"[371]. Multi-agency national exercises are demanded.[372] Cooperation between national and non-national areas is also demanded in security strategies. Collaboration within the community of nations gains an elevated ranking in the context of global security policy challenges.

[371] Ibid, p. 16.

[372] Ibid.

Whilst the need for inter-ministerial cooperation to guarantee national security has been recognised in the state strategies analysed, nevertheless one seeks in vain a collective assessment of the situation that spans all ministries. Such an assessment is demanded in the ÖSS, whereby "[...] processes shall be brought up to date and adapted to ensure their functioning with a view to a comprehensive approach to security [...]"[373]. This also implies a requirement for the optimisation of the collective effect of all security policy actors in the analysis and evaluation of situations relevant to security[374], an aspect to be evaluated as an important step towards recognition and handling of hybrid threats. Particularly in the case of military ICCM missions, there is evidence of an elevated preparedness and need for cooperation. Nevertheless, "hybrid threats" do not receive exhaustive treatment.

4.2 Conclusions

Regarding the topic of "networked security", on the Austrian Armed Forces (ÖBH) homepage is the statement that "[...] a work-sharing cooperation between international organisations and forums and their coaction towards a 'comprehensive approach' (networked security) is gaining importance for Austria"[375]. This is all the more apposite, particularly given the new "hybrid threat" challenge. It is important to counter the latter with a targeted, comprehensive security approach.

Analyses of all countries' security strategies have generally shown the special significance of the intrastate "comprehensive approach".

The Petersberg tasks, regularly referenced in connection with the European security strategy (ESS), are more directed towards missions in conflict regions outside Europe, exposing the EU to the entire spectrum of military

[373] Ibid.

[374] Ibid, p. 16/17.

[375] Austrian Armed Forces: Directorate for Security Policy. <http://www.bundesheer.at/wissen-forschung/bsp/>, accessed on 15/10/2015. Translated from the original German text

engagement.[376] "In the absence of a common European defence, missions for the defence of the national sovereign territory of member states are not included."[377] This is restricted to a hard power threat, with soft power being absent here. If there is a wish to be equipped to deal with hybrid threats in future, then not only small states but also, and particularly, the EU must tackle such scenarios to a greater extent. Here it would be necessary to analyse measures deemed necessary according to the collective defence clause laid down in the Lisbon Treaty (Article 42 paragraph 7 of the European Union treaty), as well as the solidarity clause, with regard to their effectiveness against hybrid threats.

In the event that, during a targeted power projection, unforeseen (initially unintended) negative effects arise, this is described as a multiplier effect. These render security policy analyses increasingly difficult. In the case of hybrid threats, the media have a significant influence on the success or failure of this strategy. Through their reporting they amplify, albeit unintentionally, the media presence of terrorist actors for example. This can result in significant losses in income from tourism and consequently reduced tax contributions. A negative financial trend like this would then imply reduced national expenditure on a variety of other (social) areas. Further multiplier effects can arise through sanctions against suppliers (uranium mining; transport and nuclear waste disposal), thereby raising the pressure on particular sectors (e.g. power industry). Therefore a great deal of importance is attached to the media and their reporting for the sake of minimising effects relevant to security policy.

Responsible journalistic research work, coupled with the aim of objective reporting, can be seen as making a valuable and significant contribution against hybrid threats.

[376] Ondarza, Nicolai von: Petersberg-Aufgaben. In: Bergmann (Ed.), Handlexikon der European Union. BadenBaden 2012. <http://www.europarl.europa.eu/brussels/website/media/Lexikon/Pdf/Petersberg-Aufgaben.pdf >, accessed on 15/10/2015. Translated from the original German text.

[377] Ibid.

Measures for an effective strategy against hybrid threats can be subdivided into a number of phases:

Awareness-building phase

- A hybrid threat will only be perceived as a threat once a strategic threshold is exceeded. So this level must be defined both qualitatively and quantitatively by the state. Here it is suggested that the strategic threshold represents a challenge if at least two ministries are involved in combating this threat.[378]
- Generally there were indeed reflections on future threats in the security strategies, but to date no emphasis has been placed on defensive measures against hybrid threats. Only this can explain the level of consternation with which the west is currently reacting to hybrid approaches in the Ukraine crisis. An understanding of the multiplicity of potential hybrid methods is a prerequisite for developing appropriate solution strategies (awareness building).
- Rethinking security policy on all levels must lead to a concentrated national approach to combating the dynamic threat.

It is essential to make allowance for the growing threat in the area of soft and smart power and to use it as input for situation assessments.

Early recognition, early warning phase

- An inter-ministerial analysis group should be created, with the task of continuously evaluating situation developments and threat scenarios.
- A benchmark is to be identified for defining the passing of the strategic threshold. Here it is suggested that this is the case if at least two sectors of the hybrid threats apply and defence against them involves at least two ministries.
- Particularly ICCM forces (drawn from a variety of ministries) can

[378] It is important to note that this applies solely to deliberate harm; natural catastrophes are excluded.

quickly come to be confronted by hybrid threats. In order to protect ICCM forces, ensure a successful mission and protect against domino effects on ICCM participants' home territory, situation assessments must take place continually.

- Effective combating of hybrid threats can only be ensured by means of a national "comprehensive approach". Here early recognition is most important. This requires not only an appropriate analysis tool but also an expert committee appointed at the highest political level, which conducts its analysis work continuously and develops solution concepts in a kind of emergency task force. Great effort must be given to pursuing the "Austrian partial strategy defence policy" requirement of

  > "[...]analysis reaching across all portfolios, planning and leadership processes and whole-of-nation security policy structure alongside the capability to recognise crises and changes in the strategic environment in time and to engage appropriately in the context of the whole-of-nation approach"[379].

  This requires more than a reliance on the exchange of intelligence information.

- There is a need for intensive national coordination in order to recognise an actor's concentrated hybrid approach.

Friend-or-foe differentiation in the event of cyber attacks present an extreme challenge. This features not only the problem of the territorial location of the sources of the attacks, but also the allocation to a particular actor. If the source of the attack appears to be a country, the question arises as to whether that country should be seen as the actual initiator responsible. It is possible that a different actor is merely using their infrastructure.

[379] BMLVS: Partial strategy defence policy. p. 8. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf>, accessed on 15/10/2015. Translated from the original German text.

Combat and restoration phase

- Only properly pursued, national, inter and intra-ministerial coordination ("whole-government") represents an appropriate counter-strategy against hybrid threats.
- Collaboration on a level pegging between civil and military staff is the foundation for a successful whole-of-nation approach.
- Information exchange functioning at all national and international levels contributes to the minimisation of risk. A coordinated approach shared by security entities, businesses, civil society, expert on all levels, diplomats and politicians etc. contributes to the combating of hybrid threats with every chance of success.
- A partitioned, cellular security architecture is unsuitable for the successful defence of a state. Complex systems require complex counter-reactions and can only be made secure through comprehensive inter and intra-ministerial coordination plus a high-quality "whole-of-nation" approach.

Of particular importance to the combating of hybrid threats is adequate resource provision in all areas and at all levels, being therefore a good investment within a functioning state.

General Deductions

The analyses to date enable deductions at both structural and operative levels. These are:

Conclusions at a structural "strategic" level

- Differentiation between internal and external threats is now feasible, subject to conditions. A usable solution concept can therefore only be achieved through intrastate coordination of all those responsible for security.
- No ministry or other institution can act in its own right against hybrid threats. A mindset that spans multiple portfolios, is networked and cooperation is a fundamental prerequisite for functional, national crisis management.

- The necessary expert committee must be appointed at the highest political level, functioning as an analytical and steering entity in order to assemble the whole-of-nation approach for defending against a hybrid threat.
- Under international law, hybrid threats, especially those based on soft power, scarcely feature and yet, in individual cases, do require thorough analysis with regard to international law.
- Successful combating of hybrid threats requires comprehensive legal framework conditions in order to be able to react appropriately. It is important to prevent hindrances or difficulties arising in the area of inter-ministerial administrative responsibilities. Cooperation between governmental and non-governmental security areas must also be regulated.

A "memorandum of understanding" is the pre-requisite for supra-regional and international countermeasures to hybrid approaches. As to whether this also represents a usable route for better national cooperation remains to be tested.

Conclusions at operational level

- In future, small states, as well as international organisations and institutions, must dedicate themselves more to the possibilities of hybrid threats in their situation assessments.
- Hybrid threats extend way beyond the "hybrid warfare" familiar to the military and require comprehensive, whole-nation security precautions. In order to achieve prevention in the face of hybrid threats, there must be whole-hearted dedication to a cooperative mindset at an operative level with regard to international institutions too.
- National and international security architectures must not be permitted to exist as separate, disconnected strands.
- In international terms, strong cooperation between the EU member states, linked to further organisations relevant to security, is indispensable for hybrid threats to be combated effectively.
- Armed forces must be geared towards hybrid threats. Because of the comprehensive threat potential, the response should have greater

flexibility in order to achieve efficient application of resources. The armed forces should be appropriately commissioned for the fight against hybrid threats. It is important to find niche tasks, in line with the "whole-government" approach. For armed forces, organisation similar to that for protecting critical infrastructure is suggested. Here too it is important to create the legal and resource-related preconditions for a smooth-running mission.

- Some states see their security as being closely coupled with security-related partners and confederates. On the one hand, cooperation can increase security whilst, on the other, it can have precisely the opposite effect.[380] When making decisions about cooperation it is therefore necessary also to take the hybrid factor into consideration.
- Amplified insecurity, which fluctuates alongside complex systems[381], requires an intensive whole-nation approach. Here particular attention must be paid to critical infrastructure. The more networked the infrastructural components are, as is particularly the case in power generation and in the cyber domain, the more focus they should receive.

Every effort should be made to raise awareness of the topic of "hybrid threats" among the media.

Conclusions for the ICCM

Conclusions for the ICCM have also resulted. These overlap to a certain extent with the general deductions. Here too there are deductions at both structural and operative levels.

[380] By way of example there is currently evidence that states are becoming the targets of internationally active terrorist organisations as a result of their international engagement. This can also arise through hybrid threats presented by states.

[381] Hybrid threats are to be seen as complex systems.

Conclusions at a structural level

- The capacity to act alone against hybrid threats in ICCM is just as restricted for a ministry, institution or a state. Here too, networked and cooperative thinking is a fundamental prerequisite for functioning international crisis management.
- The expert committee required for determining the situation must be appointed at the highest political level and, as an analysis and steering entity, support ICCM forces deployed on location in defending against hybrid threats.
- The aspect of international law in relation to hybrid threats also requires thorough analysis.
- Effective ICCM requires comprehensive legal framework conditions with regard to hybrid threats in order to enable deployed forces to react appropriately. Cooperation between state, non-state and international elements must be legally regulated.
- Usable solution concepts are now solely conceivable by means of "comprehensive", "whole-of-government" and "whole-of-nation" approaches.

A "memorandum of understanding" is the pre-requisite for international countermeasures to hybrid approaches.

Conclusions at an operating level

- In the future, international organisations and institutions must dedicate themselves more to the possibilities of hybrid threats in their situation assessments.
- Institutions acting internationally must coordinate with other international organisations present on location for the sake of the effective combating of hybrid threats.
- Armed forces deployed for ICCM must be geared towards hybrid threats. Because of the comprehensive threat potential, the response should have greater flexibility in order to achieve efficient application of resources. The ICCM forces should be appropriately commissioned for the fight against hybrid threats. It

is important to find niche tasks, in line with the “whole-of-nation” approach.

- If ICCM-deployed forces other than one’s own come under hybrid threat, this may possibly have two effects: on one’s own ICCM forces on location and on the sending state. Consequently the hybrid threats factor is to be assessed before any decision to send forces into international ICCM.
- Every effort should be made to involve the media in ICCM as early as possible and at an operating level, in order to minimise hybrid threats.

If particular perceptions of threat are not covered in security documents, this does not mean that they are not present. Terrorist attacks such as that of 9/11 were rated as very unrealistic before September 11th 2001 and yet they happened. The failure to address new forms of threat in good time brings exposure to elevated risk as the consequence. Only those who are prepared will be in a position to act.

In order to continue to offer the population of a small state comprehensive protection, territorial integrity and freedom of action, must be ensured “the availability of vital resources”[382]. Moreover one must be prepared for the “[m]aintaining an efficient national economy and taking precautions for the eventuality of crisis-related economic disruptions,”[383]. Thus intensive engagement with hybrid threats, as well as their possibilities and effects, is indispensable. Close inter-ministerial collaboration and greater cooperation with the private sector are essential to achieve synergy effects. In all states, a sense of comprehensive security provision must be a matter of wholehearted cooperation.

[382] Federal Chancellery of Austria, Austrian security strategy. Sicherheit in einer neuen Dekade – Sicherheit gestalten. Vienna 2013, p. 9.

[383] Ibid, p. 9.

> “Based on the national approach of the competent federal ministries, Austria will ensure that its ICT infrastructures are secure and resilient to threats. The governmental bodies will cooperate closely and as partners with the private sector.”[384]

That which is already laid down in the Austrian Cyber Security Strategy is also called for in the area of hybrid threats.

[384] Federal Chancellery of Austria: Austrian Cyber Security Strategy, Vienna 2013, p. 9.

5 Examples

5.1 Law Firms as an Example of Hybrid Threat

Christoph R. Cede

Increasing hybridity of interactions between actors draws a completely new image of conflicts, in the context of which the usually perceived threats should be rethought. The combination of military and non-military means will be playing an even bigger role in the future. Boundaries between aggression and competition blur, as well as between the use of force and (apparent) absence of force.

In order to be able to assess the situation correctly as an actor in this looming complex environment, it is necessary to think in networks and to act comprehensively. Large states with aggressive foreign policy, such as Russia[385], have already understood this and act accordingly. In the following we illustrate the characteristics of hybridity through the example of Chinese cyber-attacks and point out how unconventional thinking and creativity have given China a considerable advantage vis-à-vis the US.

5.1.1 Why law firms?

The relationship between the USA and China is characterised by competition and ongoing diplomatic dialogue, with the "*U.S.-China Strategic and Economic Dialogue*" playing an important role. Long-term negotiations are aimed at harmonising interests, so as to achieve positive results for both sides.[386] At the same time it is clear that a rising China and hegomonic USA often have conflicting interests, with the result that a potential for conflict exists.

[385] Gerasimov V. quoted by Galeotti, Mark: The 'Gerasimov Doctrine' and Russian Non-Linear War. <https://inmoscowsshadows.wordpress.com/2014/07/06/thegerasimov-doctrine-and-russian-non-linear-war/>, accessed on 11/02/2016.

[386] The White House, Office of the Press Secretary: Statement on Bilateral Meeting with President Hu of China. 01/04/2009.

In the private sector of the USA, there has been routine defensive action against Chinese industrial espionage[387] for years[388], though the latter is no longer conducted directly but rather in a hybrid way. In the past, the purpose of industrial espionage was often the acquisition of intellectual property, in order to gain competitive advantage. However, additional attention is now paid to damaging the competitor directly.

The Chinese government assigns the task of collecting data from particular law firms by means of cyber-attacks to private hackers, like the group Deep Panda, or the Chinese military. The law firms affected represent and advise foreign parties in negotiations with Chinese companies. Because the security precautions taken by negotiation partners are, given their experience of industrial espionage, generally very high, their lawyers are selected as next best targets.[389]

Because of the structure of large law firms, their way of working, the frequently encountered inertia in relation to dealing with IT and resulting rela-

[387] The term "industrial espionage" is sometimes disputed. The intended meaning is action of a state against a company. In economic espionage, the aim is to obtain general national economic data from the state sector. Cf. discussion by Cede, Christoph: Industrial Espionage under Public International Law: A Legal Smoke and Mirrors Game. In: Journal for Intelligence Propaganda and Security Studies 1/2015, p. 70ff, here p. 71; Cede, Christoph: Völkerrechtliche Betrachtungsweisen staatlicher Industriespionage [industrial espionage by states from the point of view of international law]. Diploma thesis, Karl-Franzens Universität Graz 2015, p. 9f; Sule, Satish: Spionage: Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage [espionage: analysis of state spying activities in terms of international, national and European law, particularly economic espionage]. Saarbrücken 2005, p. 30.

[388] U.S. said to be target of massive cyberespionage campaign. In: The Washington Post, 10/02/2013. <http://www.washingtonpost.com/world/national-security/us-said-tobe-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html>, accessed on 11/02/2016.

[389] Paller, Alan: Conversations About Cybersecurity. SANS Institute. <http://www.sans.org/security-resources/cybersecurity-conversations>, accessed on 09/08/2014; The Diplomat: China Expands Cyber Spying; The Diplomat: Why Are ;Chinese Cyberspies Targeting US Think Tanks?

tively low security against cyber-attacks, they present an easier target than their clients do. Partners have enormous influence within strictly hierarchically organised law firms and their decisions are scarcely questioned. Also, as a consequence of great time pressure, work is often carried out at home or on business travel; as a result confidential client data circulate on law firms' intranets or are sent by email. This raises susceptibility to cyber-attacks.[390]

Law firms are thus a worthwhile target for espionage, because hackers have access to confidential information via the documents they acquire and can therefore identify the opposite party's room for manoeuvre and thus negotiating strategy in relation to negotiations. As a consequence, the Chinese government creates an enormous advantage for particular Chinese companies in negotiations with foreign competitors who fall victim to damages.[391]

Governments react to this by calling on law firms to report threatening cyber-attacks; in the United Kingdom there was even discussion on a corresponding legal obligation[392]. However, such a report, were it to become public, would have immensely disadvantageous consequences for the law firm that submitted it, such as claims for damages, brought on the basis of inadequate protection of client confidentiality and consequent competitive disadvantage.

[390] Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, p. 48ff, here p. 52 and 54; Ames, Jonathan: Cyber security: Lawyers are the weakest link. In: The Lawyer, 28/10/2013. <http://www.thelawyer.com/analysis/cyber-security lawyers-are-the-weakest-link/3011315.article>, accessed on 11/02/2016.

[391] Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31/01/2012. <http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-targetlaw-firms> accessed on 11/02/2016; Mintz, M.: Cyberattacks on Law Firms-a Growing Threat. In: Martindale-Hubell-Blog, 19/03/2012. <http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat>, accessed on 09/08/2014.

[392] Big businesses should reveal cyber attacks, says Labour's defence spokesman. In: The Independent, 31/03/2014. <http://www.independent.co.uk/news/uk/politics/big businesses- should-reveal-cyber-attacks-says-labours-defence-spokesman-9210260.html>, accessed on 11/02/2016.

Therefore governments of affected states distribute information about the danger in lawyers' circles and create risk-awareness by means of appropriate, regular warnings and cooperation with the bar associations.[393]

5.1.2 The state sector

Yet all of this only affects the private sector. In order to be able to deduce a hybrid threat from it, the question arises as to the extent to which the state sector is affected and whether negative consequences arise for it. A state can be threatened in two ways by such cyber-attacks against law firms: indirectly and directly. Directly would actually imply that the state itself was a client of the law firm or the company represented by the law firm under attack was of relevance at a system level to the state under threat or was (part-) nationalised. An indirect threat is much more abstract; it resides in its nature that the aggressive actor intends there to be only indirect consequences.

The extent to which China really directly threatens the USA in the case mentioned here is, given the nature of the sources, indeterminable. But there are patterns mentioned in the following which, aside from preexisting opinions among U.S. security circles, lead to the conclusion that attacks on foreign law firms are orchestrated by Chinese central government. It must always be born in mind that China is, next to Russia, the most probable challenger to America's dominant position, yet nevertheless engages continuously in negotiations with the USA, not least because of the ongoing "*U.S.-China Strategic and Economic Dialogue*".

[393] Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31/01/2012. <http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-targetlaw-firms> accessed on 11/02/2016; FBI Warns Of Spear Phishing Attacks On U.S. Law Firms and Public Relations Firms. In: Dark Reading, 18/11/2009. <http://www.darkreading.com/vulnerabilities---threats/fbi-warns-of-spear-phishing-attacks-on-us-law-firms-and-public-relations-firms/d/d-id/1132421?>, accessed on 11/02/2016; Mintz, M.: Cyberattacks on Law Firms-a Growing Threat. In: Martindale-Hubell-Blog, 19/03/2012. <http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat>, accessed on 09/08/2014.

Thus any strengthening of the Chinese position indicates a weakening of the American one. In this case, the indirect (hybrid) threat to hegemony is a strengthened position of its challenger, regardless of who the direct target of the hybrid action is.

There are sufficient grounds to assume that the Chinese government fears excessive foreign influence in its territory, because the attacks are certainly not exclusively on U.S.-American law firms but more than often also directed against British and Canadian firms. Hybrid threats can also have unintended consequences, so it is necessary to think no longer in terms of action and reaction but rather in a networked manner. Therefore all that remains is to show patterns that suggest that cyber-activities can be probably attributed to China, by locating these activities in relation to Chinese interests.

China is currently experiencing a boom. The economy is growing, albeit with growth figures receding slightly from those of recent years, as is the case with the population. Political ambitions are being entertained to ascend to become a regionally predominant power in the Pacific in the medium term. On the one hand, the growing population must be supplied whilst, on the other, the Chinese government also sometimes resorts to repressive measures in order to keep unrest under control. Because of its size and booming activity, the Chinese economy has increasing demands in terms of healthcare, environmental technology and the food industry[394] as well as for raw materials along with communication and transport infrastructure.

In order to satisfy this demand, at least for the foreseeable future, China will be dependent on imports and thus on good relations with its strategic partners and neighbours. This is, however, a difficult balancing act, given that regional predominance is scarcely compatible with peaceful development.

[394] Shuanghui wraps up Smithfield deal, China’s largest US takeover. In: China Daily, 26/09/2013. <http://usa.chinadaily.com.cn/business/2013-09/26/content_16995767.htm>, accessed on 11/02/2016.

The new leaderhip in Beijing, which has been in office since November 2012, has therefore embarked on a more aggressive path than its predecessors in terms of foreign policy. For example, a national security commission was founded, and the Senkaku conflict with Japan was also escalated by China. Together with a more aggressive image for the People's Liberation Army, such political action makes it difficult to conduct diffident diplomacy. The consequences are worse relations with China's neighbours, who fear that Chinese ascendancy could be to their cost and are therefore inclined to turn to the USA as protecting power. China is using all means at its disposal to try to prevent this and has therefore created the *"peaceful development programme"*.[395]

5.1.3 Targeted attacks

This situation lays out the framework within which the picture of cyber-attacks is to be drawn. Reports of attacks on law firms are partly unambiguous, given that some law firms have confirmed attacks on them, but also partly limited to the existence of strong indications, like an abrupt strengthening of a formerly inadequate cybersecurity system or the frequent naming of a particular firm at relevant specialist events in the absence of any proof of an attack. Whether an attack was successful or not is essentially of no importance to the question over coordination. According to media reports, a variety of figures for the number of attacks exist: seven successful attacks on important Canadian firms in September 2010[396], 80 firms in New York in 2011[397], thousands of unsuccessful attempts in Ontario in 2013[398] etc.

[395] China's foreign policy faces acute challenges. In: The Daily Star, 25/07/2014. <http://www.dailystar.com.lb/Opinion/Commentary/2014/Jul-25/265049-chinasforeign-policy-faces-acute-challenges.ashx>, accessed on 09/02/2016; Paal, D.: Contradictions in China's Foreign Policy. In: Carnegie Endowment, 13/12/2013. <http://carnegieendowment.org/2013/12/13/contradictions-in-china-s-foreignpolicy>, accessed on 09/02/2016.

[396] Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, p. 48ff, here p. 50.

[397] Mandiant Corporation, quoted from M Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, p. 48ff, here p. 50.

Indeed it is possible to identify some attacked firms more precisely. One gains insight into the Chinese government's interest in them if one considers their areas of activity alongside the times of the cyber-attacks.

The first cyber-attacks on law firms can be traced to January 2010. The U.S.-American law firm that was attacked announced one week before that it would be representing the American company CYBERsitter in a 2.2 billion U.S. Dollar claim for damages against the Chinese government. The grounds were that CYBERsitter asserted that censorship filter programs, developed by the Chinese government and legally obligatory for users in China, contained over 3000 lines of plagiarised code.[399] This was therefore a matter of copyright. From an analytical point of view, there is still little indication of networked thinking; a private firm takes action against the government, which in turn presumably hacks the firm's representative.

The second case from January 2010 is similarly simple. An international law firm with roots in the USA advised the "1st Amendment Coalition", a group holding the view that China's Internet regulation constitutes a violation of WTO law[400]. Here too, China's reaction is linear and, as in the case described previously, can scarcely be considered a threat to state interest: a private interest group is of the opinion that the Chinese state is acting illegally and seeks to substantiate its claim in law.

[398] Cybercrime and law firms: The risks and dangers are real. In: LawPRO Magazine 2013 Vol.12 No.4, 2013, p. 6ff, here p. 6.

[399] China and the Law: Did Chinese Hackers Attack LA Law Firm? In: The Wall Street Journal Law Blog, 14/01/2010. <http://blogs.wsj.com/law/2010/01/14/china-and-the-law-did-chinese-hackers-attack-la-law-firm/>, accessed on 09/02/2016; L.A. Law Firm Reports Cyber Attacks. In: The Wall Street Journal, 15/01/2010. <http://www.wsj.com/articles/SB10001424052748704363504575002301498625456>, accessed on 09/02/2016.

[400] Kelly F. in an interview with Kaplan G., Australian Broadcasting Corporation, quoted by King & Spalding: The Great Wall of China. 27/01/2010. < http://www.kslaw.com/News-and-Insights/NewsDetail?us_nsc_id=150>, accessed on 09/02/2016.

Chinese hackers then attacked the group's legal representatives, whose specialties included industrial espionage[401].

Half a year later, in September 2010, the next and more comprehensive attack occured against Canadian government units, think tanks, and seven large law firms in Toronto[402]. In November 2010 there followed an offer that attracted much attention but which, following legal difficulties, was finally foiled in January 2011 on grounds of taxation and partly as a result of resistance from politicians and civil society. BHP Billiton, the world's largest mining company, attempted a hostile takeover of the Potash Corporation, the world's largest fertiliser manufacturer.[403] In November 2011, thus practically a year later, experts became convinced that the attack from September 2010 served only to conceal the actual objective, namely the two law firms that were representing the two parties in the Potash Deal[404]. According to this interpretation, of the seven law firms attacked, only two were really targets. The formerly Chinese-state-owned Sinochemgroup commissioned the Deutsche Bank and Citigroup in September 2010, i.e. in the month of the attack, to find out how the planned takeover might best be prevented. At the time of the attack, the Chinese economy was experiencing an elevated demand for agro-chemicals. Queries about this addressed to the Chinese embassy received no prompt answer.[405]

[401] Law Firms Under Siege. In: Dark Reading, 04/06/2011. <http://www.darkreading.com/attacks-breaches/law-firms-under-siege/d/d-id/1135516?>, accessed on 09/02/2016.

[402] Weston, Greg: Foreign hackers targeted Canadian firms. CBC news, 29/11/2011. <http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810>, accessed on 09/02/2016.

[403] Jones, Day: Potash Corporation of Saskatchewan successfully defends historic $43.1 billion hostile takeover bid. January 2011. <http://www.jonesday.com/potashcorporation-of-saskatchewan-successfully-defends-historic-431-billion-hostiletakeover-bid/>, accessed on 09/02/2016.

[404] Weston, Greg: Foreign hackers targeted Canadian firms. CBC news, 29/11/2011. <http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810>, accessed on 09/02/2016.

[405] Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31/01/2012. <http://www.bloom

To summarise: two foreign private corporate competitors want to close a deal between themselves and China sees its interests as endangered, so it tries to sabotage the deal. In comparison with the two previous cases, this is more properly rated as a threat to Canada, given that the entire Canadian economy was certainly subject to influence on the basis of the scale of the negotiations (40 billion $)[406]. Even though China was not affected *prima facie* by the negotiations, it had a significant interest in avoiding the possibility that its continuously growing population might be confronted by a shortage of food (Potash Corporation is the world's largest fertiliser producer).

In July 2011 there was another series of attacks. This time it was possible to determine precisely when the attacks occurred. They were distributed throughout the period from June 29th 2011 till July 21st 2011, albeit with no attack occurring at a weekend. Thus one may deduce that professional, full-time hackers were involved. Two of nine attacks in this period were directed against law firms, with somewhat more than a quarter of the victims being lawyers. One of the affected law firms advised U.S. companies, representing interests in questions of international trade and, moreover, had actively addressed the matter of Chinese export restrictions on raw materials with the Office of the United States Trade Representative and the WTO[407]. The individual lawyers affected were all active in international trade law. The affected lawyers in the other law firm worked on intellectual property and copyright and gave lectures about China.[408]

berg.com/news/articles/2012-01-31/china-based-hackers-target- law-firms> accessed on 09/02/2016.

[406] Ibid.

[407] Price A./Brightbill T./ElSabaawi L: WTO Panel Says China's Raw Materials Export Restrictions Violate WTO Obligations. Wiley Rein, 05/06/2011. <http://www.wileyrein.com/publications.cfm?sp=articles&id=7192>, accessed on 09/02/2016.

[408] Whiteaker, Chloe: China Hackers Activity Logged Reveals Multiple Victims Worldwide. In: Bloomberg Online, 25/07/2012. <http://go.bloomberg.com/multimedia/china-hackers-activity-logged-reveals-multiple-victims-worldwide/>, accessed on 04/08/2014.

In this case the attacks were therefore directed at law firms that could possibly hinder Chinese interests directly rather than just through representing their clients.

Subsequently there were repeated, smaller attacks, albeit with strategic objectives that could not be identified precisely. Four firms that conceded in October 2013 that they had repeatedly been the targets of attacks[409] had, however, been involved in notable activities during the preceding period.

Stewart Baker, formerly Assistant Secretary of the Department of Homeland Security, was quoted in the media in February 2013 in connection with U.S. government work relating to cyber-attacks and a firmer U.S. standpoint regarding China[410]. In March 2013 Reuters quoted Phil West, a former advisor to the Treasury Department, in an article that described a tax treaty between the USA and China as "elusive"[411]. In April 2013 Kuwait Petroleum invested in a joint venture with Sinopec, one of the largest Chinese petroleum corporations and located in Guangdong province[412], and was represented in negotiations by one of the four firms that were attacked. Also in April, Stewart Baker was again quoted, this time regarding the U.S.

[409] Greengard, Samuel: Law Firm Defends Itself Against Cyber-Threats. In: Baseline, 08/11/2013. <http://www.baselinemag.com/security/law-firm-defends-itself-againstcyber-threats.html>, accessed on 10/02/2016; Benzing, Jeffrey: Law Firms 'Low-Hanging Fruit' for Cyber Thieves. In: Main Justice, 01/11/2013. <http://www.mainjustice.com/2013/11/01/law-firms-low-hanging-fruit-for-cyber-thieves/>, accessed on 10/02/2016; Ames, Jonathan: Top City firm fights off cyber attack. In: The Lawyer, 28/10/2013. <http://www.thelawyer.com/analysis/the-lawyer-management/top-city-firm-fights-off-cyber-attack/3011549.article>, accessed on 10/02/2016.

[410] Steptoe & Johnson: Associated Press Quotes Stewart Baker on Chinese Cyberattacks on US. 05/02/2013, <http://www.steptoe.com/news-1333.html>, accessed on 10/02/2016.

[411] TempleWest, Patrick/Lee, Yimou: U.S.-China anti-tax evasion deal seen as crucial, but elusive. In: Reuters, 14/03/2013. <http://in.reuters.com/article/2013/03/13/usa-tax-fatca-idINL1N0BYH9520130313>, accessed on 10/02/2016.

[412] Ling S./Zhou O.: Petrodollars: the Sinopec-KPC refinery is hitting some rough spots. In: The Barrel, blog, 15/04/2013. <http://blogs.platts.com/2013/04/15/sinopec-kpc/>, accessed on 10/02/2016.

federal government ban on purchasing IT from Chinese (formerly) quasi-nationalised companies.

This ban is drawn into association with Chinese cyber-espionage.[413] In May 2013 one of the law firms attacked was advising PAI Partners regarding the sale of FTE Automotive GmbH to Bain Capital. The parties to the deal had agreed on secrecy of the precise purchase price.[414] In July 2013 Spreadtrum Communications, involved in a 1.78 billion $ takeover by Tsinghua Unigroup (a quasi-nationalised Chinese wireless communications manufacturer), was represented by one of the firms attacked[415]. Eric Emerson, a lawyer at that very firm who had already been quoted three times in the media since February regarding expert opinion about China, spoke in July 2013 in Washington about "Perspectives on the U.S.-China Investment Relationship"[416].

In September 2013 Shuanghui bought the world's largest pig-rearing company, Smithfields. This stands as the largest takeover by a Chinese company to date (4.7 billion $), and one of the firms attacked had a leading role in it[417].

[413] Steptoe & Johnson: Media Quotes Stewart Baker on US Ban on Chinese IT Equipment. 09/04/2013, <http://www.steptoe.com/news-1408.html>, accessed on 10/02/2016.

[414] Clifford Chance: Clifford Chance advised PAI Partners on the Sale of FTE Automotive GmbH. 14/05/2013. <http://www.cliffordchance.com/news/news/2013/05/clifford_chance_advisedpaipartnersonthesaleofftеautomotivegmbh.html>, accessed on 10/02/2016.

[415] Fenwick & West: Fenwick & West is Representing Spreadtrum Communications in its Acquisition by Tsinghua Unigroup for $1.78B. 12/07/2013. <http://www.fenwick.com/experience/Pages/Fenwick-Represents-Spreadtrum-Communications-in-its-Announced-Acquisition-by-Tsinghua-Unigroup-for-$1.78B.aspx>, accessed on 10/02/2016.

[416] Steptoe & Johnson: Perspectives on the US-China Investment Relationship, Global Business Dialogue Members' Lunch. 18/07/2013. <http://www.steptoe.com/newsevents-2477.html>, accessed on 10/02/2016.

[417] Allen & Overy: IFLR Americas' M&A Deal of the Year award for Shuanghui's acquisition of Smithfield Foods. 09/04/2014. <http://www.allenovery.com/news/

Regarding this, a lawyer from the same firm, whose lawyers had been repeatedly quoted in the press as experts, expressed the opinion that the U.S. government would probably approve this takeover[418]. In September 2013 another of the four law firms advised Carlyle Asia Growth Partners IV on a 365 million HK$ investment in Tenwow International Holdings, one of the largest convenience food producers in China[419], as well as AMP Capital on a joint venture with an affiliate of China Life Insurance (Group) Company, the world's largest insurance company (based on capital)[420]. In October 2013 the same law firm also advised Siemens on the sale of TLT-Turbo GmbH to Power Construction Corporation of China. The parties to the deal agreed on secrecy regarding the purchase price.[421]

One of the law firms affected has staff with a broad range of experience including government work and is openly critical of China in the media. The other three represented the opposing (i.e. non-Chinese) parties in negotiations with Chinese companies. The sectors involved – fuel, automotive industry, communication technology, food, healthcare and environmental technology – all fall within the strategic interests of the Chinese economy and therefore also the Beijing government, given the huge size of the population.

engb/articles/Pages/IFLR-Americas%E2%80%99-MA-Deal-of-the-Year-award-for-Shuanghui%E2%80%99s-acquisition-of-Smithfield-Foods-.aspx>, accessed on 10/02/2016.

[418] US likely to clear $4.7bn Smithfield deal. In: The Financial Times, 05/09/2013. < >, accessed on 10/02/2016.

[419] Clifford Chance: Clifford Chance advises Carlyle on HK$365 million cornerstone investment in Tenwow International Holdings. 30/09/2013. <http://www.cliffordchance.com/news/news/2013/09/clifford_chance_advisescarlyleonhk365million cornerstoneinvestmen.html>, accessed on 10/02/2016.

[420] Clifford Chance: Clifford Chance advises AMP Capital on China funds management joint venture with China Life. 05/09/2013. <http://www.cliffordchance.com/news/news/2013/09/clifford_chance_advisesampcapitalonchinafundsmanagementjointvent.html>, accessed on 10/02/2016.

[421] Clifford Chance: Clifford Chance advises Siemens AG on the sale of TLT-Turbo. 29/10/2013. <http://www.cliffordchance.com/news/news/2013/10/clifford_chance_advisessiemensagonthesaleoftlt-turbo.html>, accessed on 10/02/2016.

In all these cases it is therefore clear that the precisely determinable cyber-attacks were carried out on those firms that, at the time of the attack, were active in an area connected with China.

Whilst the cyber-attacks were originally targeted only on those law firms that were proceeding against China, others were quickly also attacked in order to conceal the true objectives.

Not just the number of targets but also the complexity of the attacks grew. An attempt was made to achieve the identified foreign-political objectives by means of an elevated level of creativity. Whilst the attacks were initially deployed directly against a judicial adversary of the Chinese State, more recently it can be stated that the targets of the cyber-attacks often only stood indirectly in the way of China's economic interests. Alongside the number of targets and complexity of the carefully directed attacks, their frequency also increased. Here it is worthy of note that the change of leadership of the Chinese government in November 2012 was accompanied by an interruption in the attacks and a swing towards more aggressive foreign policy[422]. The number of targeted attacks that can be verified by means of publicly available information (excluding feints) rose steeply immediately afterwards, over the period from January till March 2013. It was only possible to find data up until November 2013 that allow the inference of targeted attacks.[423]

[422] China's foreign policy faces acute challenges. In: The Daily Star, 25/07/2014. <http://www.dailystar.com.lb/Opinion/Commentary/2014/Jul-25/265049-chinas-foreign-policy-faces-acute-challenges.ashx>, accessed on 10/02/2016; Paal, D.: Contradictions in China's Foreign Policy. In: Carnegie Endowment, 13/12/2013. <http://carnegieendowment.org/2013/12/13/contradictions-in-china-s-foreignpolicy> accessed on 10/02/2016.

[423] Prepared by Christoph Cede, following analysis of 33 websites and exclusively open-source (!) announcements, observation period: June-July 2014.

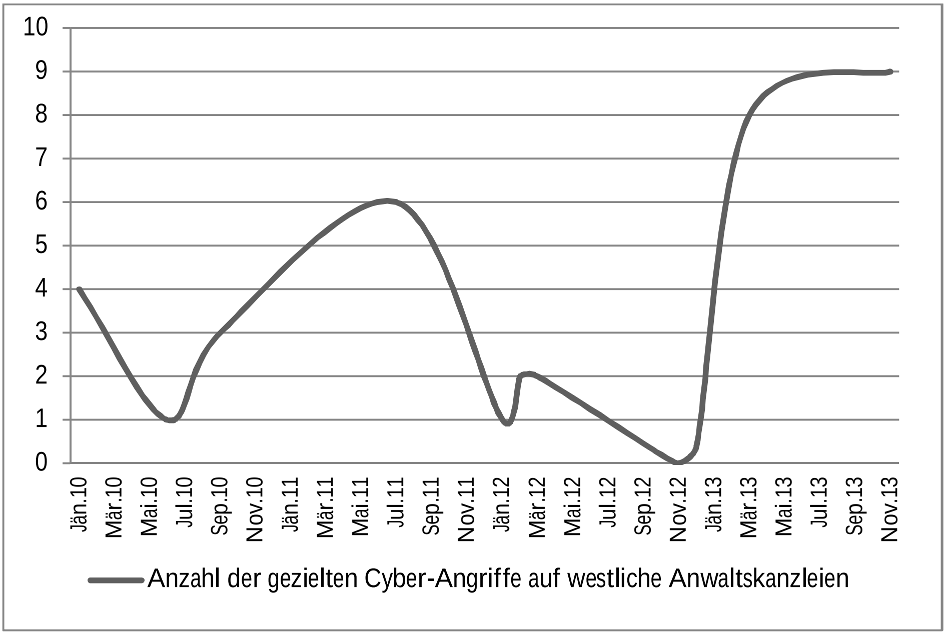


Tabelle 6: Targeted and verifiable cyber-attacks on western law firms *Christoph Cede*

All these circumstances suggest that behind these attacks is an actor who is favourably disposed towards the Chinese government and who, through the advantage he creates for China, indirectly compromises the USA in terms of its room to manoeuvre. Even though the attacks alone fall far short of the strategic threshold necessary for a hybrid threat, nevertheless, combined with skillful diplomatic moves and appropriately harmonised negotiations in the "*U.S.-China Strategic and Economic Dialogue*", they could threaten the USA.

5.1.4 Deductions

The question that arises for Austria and European small states is what lessons can be learnt from this. Firstly there is a need to clarify whether such attacks happen to Austrian law firms (the bar association answers no queries on this) and whether these could be traced in a similar manner.

With regard to law firms, the Austrian bar association will scarcely be able to take steps any different from those of larger states: inform, warn and call for cooperation. It is necessary to highlight the threat to data and call for raised security awareness. Ultimately, lost data could work to the disadvantage not only of law firms but also possibly of Austria in that, through a combination with some other means, the state could be subjected to a hybrid threat.

Decision-makers at a state government level (and in partially-nationalised businesses) should be aware of the risks, when law firms are involved in bilateral negotiations and, above all, directly in closing contractual deals.

If external legal counsel is engaged by the state to advise on specific matters, it seems advisable to pay particular attention to their level of security and to communicate this to the relevant law firms as an expectation. But measures to raise in-house security only offer protection to the extent that aggressors have not yet familiarised themselves with them. So in the long term there is a need to prepare strategies for how to deal with such a threat.

5.2 Projection of Soft Power via Social Networks in Hybrid Conflicts

Martin Staudinger

In March 2014 and over the following months, western-European journalists, who reported on the upheaval in the Ukraine and directly succeeding annexation of the Crimean peninsula by the Russian Federation, received numerous, fierce reactions. Not only through email and letters, but also via postings on the websites and Facebook accounts of their media businesses as well as other channels on the Internet, readers expressed opinions regarding the presentation of events; many of them applied sharp criticism, expressed incomprehension and resorted to personal attacks too.

"[I have not seen the likes of what's happening to us right now in the dispute about Russia and the Crimea in thirty years of conducting debate]", wrote Bernd Ulrich, head of politics at the German weekly newspaper "Die Zeit" on April 10th 2014:

> "Unless surveys are misleading, two-thirds of German citizens, voters and readers stand opposed to four-fifths of the political class – in other words, to the government, to the overwhelming majority of members of parliament and to most newspapers and broadcasters. But what does "stand" mean? Many are downright up in arms."[424]

Attempts to understand and explain this phenomenon at the time provoked another almost 750 comments, some of them furious.

A subset of the reactions, which puzzled not only Ulrich, could well have been genuine expressions of widely-held sentiment in Europe and were perceived as such. But subsequently there was a lot to suggest that a substantial other subset of the reactions were directed towards news coverage.

[424] How Putin Divides. In: Die Zeit Online, 10/04/2014. <http://www.zeit.de/politik/ausland/2014-04/germans-russia-media-putin>, accessed on 16/02/2016.

In its Internet edition, the “Süddeutsche Zeitung” spoke of “droves of paid manipulators” assigned to

> “[dominating opinion in the comment areas of large news portals, disrupting debate in social networks and breaking up communities on the opposing side. Protected by anonymity, they can scarcely be distinguished from normal debaters or simple provocateurs – so-called trolls.]”[425]

Supporting the supposition that many expressions of opinion about the Ukraine crisis originate from propagandists, there are not only indications; for example, the fact that, according to surveys by the Allensbach Institute at the time, only eight percent of Germans admitted having a “good opinion of [Russia’s President Vladimir] Putin” and 70 percent expressed a lack of understanding of the Russian president. This is also supported by independent media research results. The oppositional Russian newspaper “Novaya Gazeta” had already reported in 2012 on the “Internet Research Agency”, a company in the St. Petersburg suburb of Olgino, in which, of late, up to 600 staff were said to have been employed to “[manipulate opinion on the Internet to favour the Kremlin]”. In connection with the Ukraine crisis, this information was confirmed to the “Süddeutsche Zeitung” by one of the company’s top staff.[426]

> “[In the meantime, a director of the ‘Internet Research Agency’ decided on a headlong rush. By phone, Michail Burtschik confirmed the authenticity of the material to the Süddeutsche Zeitung, but didn’t want to say any more about the agency’s activities. In his blog, Burtschik now calls himself the ‘executive troll’ and stated that the activity was nothing special; ultimately journalists were also paid to write. As patriots, some were even proud to be called the ‘Trolls from Olgino’: ‘Better to be a troll and love your homeland than to scold the government anonymously’, wrote Burtschik (...)]”[427]

Taking a contrary position, the Ukrainian Crisis Media Center, based at the

[425] Putins Trolle [Putin’s trolls]. In: Süddeutsche Zeitung Online, 13/06/2014. <http://www.sueddeutsche.de/politik/propaganda-aus-russland-putins-trolle-1.1997470>, accessed on 16/02/2016.

[426] Ibid.

[427] Ibid.

Hotel Ukraina in Kiev, delivered the Ukrainian perspective of the crisis round the clock to the media and public, also using social networks like Facebook and Twitter.[428]

The emergence of social networks on the Internet, and their increasing use by broad sections of the population, also substantially changed the use of some aspects of soft power in conflicts.

According to a report in the "Huffington Post", General Valery Gerasimov, chief of the general staff of the Russian Federation, acknowledged this in an article published on February 27th 2013 in the Russian publication "Military-Industrial Kurier". This includes:

> "The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks. It is necessary to perfect activities in the information space, including the defense of our own objects."[429]

Actors on the offensive through state-, people- and terrorist-power make equivalent use of social networks like Facebook, Twitter, Instagram and YouTube, to some extent with the same or similar objectives. These might consist of securing prerogative of interpretation, image management, motivating pre-existing supporters or recruiting new ones, but also intimidating adversaries.

To date, all of this belonged to the range of tasks falling within propaganda. It is nevertheless possible to confirm a paradigm shift.

For the time being, the Internet makes it possible to reach a large number of recipients with relatively little effort and on short timescales.

[428] Author's personal perception.

[429] Top Russian General Lays Bare Putin's Plan for Ukraine. In: The Huffington Post, 09/02/2014. <http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html>, accessed on 16/02/2016;
Original source: <http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf>.

At the end of 2013 there were 2.8 billion Internet users worldwide.[430] According to findings of the opinion polling institute Bitkom, which specialises in the high-tech sector, in October 2013 two thirds of them, i.e. over 1.8 billion, were also active on social networks.[431]

According to enquiries by the U.S. software company Adobe, at the beginning of 2014 a total of 5.7 billion user profiles existed on the 21 largest networks worldwide.[432] Seen in terms of statistics, this implies that, on average, every Internet user is active on three networks. That means a considerable space for resonance.

But the actual paradigm shift arises from the possibility to individualise the exertion of influence at the same time as maximising publicity and potentially concealing the agenda.

After the end of the Cold War, initially of note was the increasing involvement of PR agencies in media handling of conflicts. To give some (non-exhaustive) relevant examples: the U.S.-American PR agency Hill & Knowlton which, during the second Gulf War, put forward to the world the false assertion that, during the invasion of Kuwait, Iraqi soldiers had snatched newborn babies from incubators at a hospital and thus killed them. Hill & Knowlton had been commissioned by the Kuwaiti government-in-exile to support a recapture of the emirate through publicity work.[433]

[430] Internet Usage Statistics. The Internet Big Picture. In: Internet World Stats. <http://www.internetworldstats.com/stats.htm>, accessed on 17/02/2016.

[431] Berg, Achim: press conference – Nutzung sozialer Netzwerke in Deutschland [use of social networks in Germany]. Bitkom, 31/10/2013. <http://www.bitkom.org/files/documents/BITKOMPK_Studie_Nutzung_Sozialer_Netzwerke_31_10_2013.pdf>, accessed on 17/06/2015.

[432] Jeremy Waite: Which Social Networks Should You Care About in 2014? 03/01/2014. <https://blogs.adobe.com/digitaleurope/2014/01/03/social-networks-care-2014/?PID=6149999>, accessed on 17/02/2016.

[433] Deception on Capitol Hill. In: The New York Times Online, 15/01/1992. <http://www.nytimes.com/1992/01/15/opinion/deception-on-capitol-hill.html>, accessed on 17/02/2016.

During the Balkan wars, the agency Ruder Finn was commissioned to undermine Serbia's position.[434]

In the war in Georgia in 2008, "[the Brussels-based PR agency aspect communications, which has acted for the Georgian government since November 2007, supplied the media on a minute-by-minute basis with press releases translated into English practically in real time]".[435]

During that period, Russia's interests were represented by gplus europe, a subsidiary of the New York PR giant, Ketchum.[436]

Before social networks were established, like all others going on the offensive with campaigns (information and disinformation), manipulation, propaganda and mobilisation, PR agencies were obliged to a large extent to make use of traditional media which, at the same time, themselves exercised a filtering function or had recognisable party affiliations.

An actual example: readers' letter campaigns to influence public opinion were relatively easy to identify as such. Moreover editorial decisions were required on whether or not to publish letters along with moderation of the relationship between various points of view. The identities of authors or simply their true existence could be checked with relatively little effort.

On the Internet this filter function is *de facto* disabled. Social networks allow Internet users to publish content more or less without limitation.

[434] Schmidt, Christian: Kriegs-PR und Propaganda? Zum jüngsten Jugoslawienkrieg [war-PR and propaganda? On the latest war in Yugoslavia]. Term paper, Institute of Communication and Media Studies, University of Leipzig, 2000.

[435] Staudinger, Martin/Szyszkowitz, Tessa: Der Krieg nach dem Sieg [war after victory]. In: Profil 37/08, 06/09/2008, p. 68. <http://www.profil.at/home/der-krieg-sieg-218312>, accessed on 17/02/2016.

[436] Die Strategen der Wortschlacht [strategies of verbal battle]. In: Süddeutsche Zeitung Online, 17/05/2010. <http://www.sueddeutsche.de/politik/pr-im-kaukasus-konflikt-die-strategen-derwortschlacht-1.707833>, accessed on 17/02/2016.

Postings on Facebook can only be deleted manually by the owner of the corresponding account, for example.

Where classical media do allow comments on their reporting on their websites, only by engaging moderators is it possible to select material before publication or remove it again afterwards. This is an outlay, in terms of time and costs, that many media have often foregone in the past in order to encourage traffic and generate advertising revenue.

At the same time this means that comments on media reporting can be made immediately with full publicity, a circumstance that, in itself, should not present a problem. However, this can easily be misused for campaigns, propaganda, manipulation and other offensive methods to exert soft power, and was indeed in recent times.

Meanwhile, addressees can be contacted individually via these social networks. For example, they can be confronted directly with content or, if necessary, they can also be pilloried in public. This can just as much target journalists on account of their reporting as it can authorities or those with political responsibility.

Applying pressure in this manner can prove effective not only on account of the maximisation of publicity, but also due to perception by the addressees. Anyone confronted by a large number of deprecatory, critical or denunciatory comments brought into the space for resonance mentioned above, might easily gain the (possibly false) impression of themselves being in a minority position or find themselves misguided into wrongly assessing the actual majority views among the public at large. A few weeks ago, “Die Zeit” summarised a further aspect thus:

> “Authoritarian states like China and Russia have further developed their propaganda strategy. Not only do they efficiently control their national media, they influence Western public with TV programmes, blogs and social media. This is an important change in tactics, given that self criticism is part of Western societies’ nature, which is one of … [their] … great strengths,

> this self-criticism is now being viciously strengthened from somewhere else and as a result it is suffering a self-destructive slide."[437]

It is also entirely possible to disseminate an agenda and, at the same time, to cover up. Actors are not recognisable as such without effort. They can hide behind apparently disinterested identities – e.g. concerned citizen.

All of this entails the possibility of feedback to political systems, above all if they are democratically structured and consequently receptive to the (often imagined) reaction of the electorate.

At the extreme end of the broad spectrum of soft power projection via new media are the activities of the so-called "Islamic State" (IS, "addaula alislāmiyya" in Arabic, known till mid July 2014 as "ISIS" – Islamic State of Iraq and (greater) Syria). This Salafi jihadist organisation, whose objective is the creation by force of a caliphate, starting in Syria and Iraq but following with the Lebanon, Israel, Palestine and Jordan, is listed as a terrorist group by the USA[438], the UN Security Council[439], Australia[440] and the Public Prosecutor General of the German Federal Court of Justice[441] amongst others.

[437] The world is going crazy – and what are we doing? In: Die Zeit Online, 02/09/2014. <http://www.zeit.de/2014/36/war-conflict-russia-iraq-ukraine/seite-3>, accessed on 17/02/2016.

[438] US Department of State, Bureau of Counter Terrorism: Foreign Terrorist Organizations. <http://www.state.gov/j/ct/rls/other/des/123085.htm>, accessed on 17/02/2016.

[439] UN Security Council, Security Council voices great concern over reported seizure of oilfields by terrorist groups operating in Syria, Iraq. SC/11495, 28/07/2014. <http://www.un.org/press/en/2014/sc11495.doc.htm>, accessed on 17/02/2016.

[440] Australian Government, Australian National Security: Listed terrorist organisations. <http://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/default.aspx>, accessed on 17/02/2016.

[441] Cf. Federal Ministry of the Interior: Verfassungsschutzbericht 2013 [2013 Annual Report on the Protection of the Constitution], p. 192ff, here above all p. 209ff. <http://www.verfassungsschutz.de/embed/vsbericht-2013.pdf>, accessed on 17/02/2016.

IS is highly active on social networks. The "New York Times" reported on June 28th 2014:

> "The extremist group battling the Iraqi government, the Islamic State in Iraq and Syria, may practice a seventh-century version of fundamentalist Islam, but it has demonstrated modern sophistication when it comes to using social media, particularly Twitter and other sites like WordPress and Tumblr. On Twitter, ISIS has hijacked World Cup hashtags, flooding unsuspecting soccer fans with its propaganda screeds. It has used Facebook as a death-threat generator; the text-sharing app JustPaste to upload book-length tirades; the app SoundCloud for jihadi music; and YouTube and Twitter for videos to terrify its enemies."[442]

> "ISIS, as well as its fighters and supporters, quickly adopted these tools and has been utilizing the latest Internet technologies and social media outlets to maintain massive, sophisticated online media campaigns used to promote jihad, communicate, recruit and intimidate",

quoting Rita Stern, analyst in the SITE Intelligence Group, in the article cited above.[443]

Even though only a few really definite numbers are available to date, there are many indications that the "Islamic State" is achieving really effective recruitment and intimidation with the aid of social networks. For example the case of a jihadist with Tunisian roots attracted attention in Austria in the summer of 2014 when he boasted on Facebook that he had taken part in executions by IS militia.[444]

[442] Iraq's Sunni Militants Take to Social Media to Advance Their Cause and Intimidate. In: The New York Times Online, 28/06/2014. <http://www.nytimes.com/2014/06/29/world/middleeast/iraqs-sunni-militants-take-to-social-media-to-advance-their-cause-and-intimidate.html>, accessed on 17/02/2016.

[443] Ibid.

[444] Dschihadist aus Wien mutmaßlich an Gräueltaten in Syrien beteiligt [jihadist from Vienna presumed to have taken part in atrocities in Syria]. In: Profil Online, 26/08/2014. <http://www.profil.at/articles/1435/982/377621/dschihadist-wien-graeueltaten-syrien>, accessed on 17/02/2016.

Worthy of note in this context is the fact that IS acts of violence, like the execution of unarmed prisoners, are not kept secret, as is typically the case with other warring parties. Quite the contrary; they are broadcast aggressively, presumably also in order to make themselves more attractive to new fellow combatants by demonstrating exceptional brutality.

The second supposed objective, intimidation, is not only directed at the immediately accessible vicinity of the Islamic State, but also at the international community.

It is thereby possible to suggest for example, to the governments, authorities and the peoples of other states, that IS already has a large following abroad, something that again might be capable of raising its attractiveness to potential followers.

Once again it is the social networks, by means of which photos, videos, audio files and other information can be delivered quickly and directly to a large group of recipients.

Summary

As a result of the emergence of social networks, the deployment of offensive means like campaigns (information and disinformation), manipulation, propaganda and mobilisation in hybrid conflicts can take advantage of new, extremely effective channels of distribution, in which it is scarcely possible to control, filter or even prevent the flow of information.

As a consequence of this, and the fact that it is possible simultaneously to both conceal an agenda and maximise its effect on the public through social networks, many possibilities arise for exerting influence on the population, the media and thus indirectly or directly on those with political responsibility, possibilities that may be difficult to identify or counter in individual cases.

5.3 Power Projection by Pipeline: Russia, Sweden, and the Hybrid Threat from the Nord Stream Project, 2005-2009

Michael Fredholm

By late 2005, Sweden suddenly faced what it perceived as a hard security threat, in the unexpected form of a Russian pipeline project across the Baltic Sea which, it was suspected, could be used as a sensor platform for Russian military intelligence. The pipeline would be ideally located for use as a tripwire sensor chain through which Russia could monitor all movements of aircraft, surface vessels, and submarines across the Baltic. However, the pipeline project was a commercial venture, which could not be opposed through regular security strategies due to international law. For this reason, the Ministry of Defence commissioned a study of the implications of the project and an inter-ministerial working group from the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment was put together to address the threat and assess counterstrategies to contain it.[445]

When faced with Swedish opposition, Russia responded with its own multidimensional counter-counterstrategy, which for reasons which will be explained included several major EU member states. In effect, Russia used hybrid means to influence the media, society, and ministries of neighbouring states to gain permission for a strategic industrial infrastructure project. There were elements of what used to be known as an influence campaign in these efforts, but a broad spectrum of actors was used to achieve the objective of building the pipeline, which corresponded to Russia's, not Sweden's, strategic interests. In effect, the two sides can be said to have lined up their respective principal powers as follows:

[445] Swedish state television eventually exposed an internal Swedish government document on the working group's suggested strategies against the proposed pipeline. Sveriges Television (SVT), Nyheter, 07.12.2006. The internal document was a Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006.

Russian Actors	Task	Swedish Actors	Task
Russian President	Decision-making	Ministry of Defence	Coordination
State-controlled Firm: Gazprom	Coordination	Ministry of Justice	EIA Approval (legal issues)
State-controlled Consortium: Nord Stream AG	Pipeline construction	Ministry of Environment	EIA Approval (environmental issues)
Intelligence Services	Intelligence collection	Intelligence Services	Intelligence collection
State Institutions	Seabed Survey	Ministry of Defence	Upholding state sovereignty
Naval Forces	Support to Seabed Survey	Ministry of Defence	Upholding state sovereignty
Diplomatic Power - Russia - Germany - Britain - France - Netherlands - Denmark	Political support: Continuous Continuous Initially Limited Limited Limited	Foreign Ministry	Political support
Media Power - Nord Stream AG - State Media - PR Agencies	Lobbying Media campaigns Recruitment of policy makers	FOI (Think Tank) Media Houses	Media campaigns Media campaigns

Table 7: Russian and Swedish Actors
Michael Fredholm

To the Swedish government, the natural gas pipeline project was perceived to be the very embodiment of a hybrid threat. With a hybrid threat defined as

> "a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests,"[446]

this was hardly surprising. As a commercial endeavour, the proposed pipeline would have to be treated as any other commercial project. Yet, foreign state organizations (the Russian diplomatic corps, aided to a certain extent primarily by its German counterpart; the Russian Navy; Russian state-controlled commercial enterprises such as Russia's natural gas pipeline export monopoly Gazprom; and much of the Russian media) were deeply involved in promoting the project.

The proposed pipeline was perceived as a threat to several Swedish core interests. Sweden's Defence Minister Mikael Odenberg summarized the hybrid nature of the threat in a national public radio interview: "the gas pipeline brings implications for energy policy, environmental policy, as well as security policy."[447] The Swedish government was particularly concerned over three core interests: the desire, based on environmental reasons, to gradually end European reliance on hydrocarbons as a key source of energy; the ambition (again for environmental reasons) to protect the Baltic Sea environment from the effects of pollution, the disturbing of old munitions and hazardous materials on the seabed, and if possible through a reduction in the overall level of shipping; and the desire to minimize naval activities in the Baltic (and, one could easily argue, in particular the presence of Russian naval units). In addition, the Swedish government felt duty-bound to

[446] As defined by the National Defence Academy (Landesverteidungsakademie), Vienna: "Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen."

[447] Sveriges Radio (Sweden), 14.11.2006.

support the views of Poland and the Baltic states, which opposed the project for reasons of their own, mainly having to do with their relations with Russia and Poland's role as a transit state for Russian natural gas supplies to Western Europe. Moreover, the proposed pipeline was regarded as a hard security threat in and of itself, since the Swedish Ministry of Defence realized at an early stage that it might be used as a platform for Russian military intelligence collection against Swedish targets. Additionally, the means eventually employed by the pipeline consortium to promote the pipeline project were also perceived as threatening to Swedish political culture. Here was indeed a commercial project which violated Sweden's core interests, yet it was beyond the control of the Swedish government-something hitherto almost unheard of so close to Sweden's borders. Instead it was regarded as sponsored by two neighbouring great powers, Germany and Russia, both of which had their own agendas and their own core interests which in this particular case conflicted with those of several smaller neighbours, among them Sweden.

This paper is divided into two parts. The first will describe the background of the Nord Stream pipeline and primarily serves to summarize the evidence for the pipeline project being a Russian government initiative and not a straightforward private business venture, as was generally argued by its proponents. In fact, to counter the response that the Swedish perception of the pipeline project was an unfortunate overreaction to a mere commercial venture, and an international one at that, it will be necessary to give a lengthy (and to the non-expert, admittedly somewhat tedious) description of the Russian energy sector and Russian energy policy. In addition, this part of the case study serves to illustrate the difficulty in recognizing and pinning down state participation in hybrid power projection employing commercial entities.

Those who wish may skip the first part and go straight to the second which will examine the pipeline project in its role as a hybrid threat to Swedish core interests. This part will describe the variety of actors involved, and their offensive means to promote the venture. In addition, it will examine the defensive means, also of a hybrid nature, employed by Swedish state actors in their attempt to thwart the project, an attempt which ultimately failed, yet succeeded in eliminating or at least reducing the project's potential to threaten Sweden's national security interests. On the surface, both the Swedish and Russian sides presented their cases as overt and transparent, and themselves as studiously reasonable and legalistic, yet both sides engaged in activities which could only be interpreted as hostile to the other. The devil was in the details, and a full description of the events which accompanied the Nord Stream project is necessary to perceive the hybrid means employed by both sides to enforce their will.

5.3.1 Part 1: The Pipeline Project as a Russian Government Initiative

National and Commercial Interests in the Pipeline Project

A major energy infrastructure project such as the Nord Stream pipeline cannot be understood without an analysis of the national and commercial interests of the states and corporations involved. For Russia, the pipeline project was the natural outcome of its national energy strategy.[448]

Few governments wish to be dependent on forces outside their control, even if the dependence is mutual. This is particularly noticeable within the field of energy security. While Russia is dependent on revenues from its energy exports, many European countries are equally or more dependent on Russia as a supplier of natural gas in particular. When possible, the Russian state strives, through its energy policy, to avoid dependence on other states and at the same time to dominate its domestic market as well as, when possible, the international market. Russia sees a particular strategic need to control the export and transit means for its exports to the international market. Russia thus works to create export infrastructure on Russian

[448] Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006; Fredholm, Michael: Strategies of Energy and Security in Contemporary Eurasia: Vulnerabilities and Opportunities in Russia's Energy Relationships with Europe, Central Asia, and China. In: Sreemati Ganguli (ed.): Strategising Energy: An Asian Perspective. New Delhi 2014, p. 163ff.

territory or across international waters that will eliminate the need to transit energy deliveries through other states.

Besides, state control over much of the Russian energy infrastructure means that Russia finds its energy policy a vital component in various issues of national security policy. The Russian desire to avoid dependence, for instance, makes its leaders preoccupied with a wide range of perceived strategic threats in the same way that some European Union (EU) countries instead perceive Russia as a threat. Russia will under no circumstances accept a position of dependence towards any other country, considering this a threat to its own national security. The Kremlin is no more immune to the demands of national security than the countries of the EU, or for that matter any other country.

Under the leadership of Vladimir Putin and Dmitry Medvedev, Russia developed, approved, and published its energy strategies in documents which carried legal status. The 2003 Russian energy strategy expressed key goals for Russia within the energy sector.[449] The results of its direction could be seen in several subsequent infrastructure projects carried out within the state-controlled Russian energy firms.[450] In addition, Russia, as a state, tends to take legislation such as the energy strategy seriously and tends to follow official policy expressed therein.[451]

The 2003 Russian energy strategy concluded that the goals of the Russian energy policy with regard to foreign countries included the need to strengthen the position of Russia in the global energy market and maximize

[449] Energeticheskaya strategiya Rossii na period do 2020 goda ("Energy Strategy of Russia to the Year 2020"), Government of the Russian Federation Decree No. 1234-r, 28.08.2003. Approved on 23.05.2003 and confirmed by the Russian government on 28.08.2003.

[450] Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005.

[451] See, e.g. Fredholm, Michael: Russia and Central Asian Security. In: Schlyter, Birgit N. (ed.): Prospects for Democracy in Central Asia. Istanbul: Swedish Research Institute in Istanbul Transactions Vol. 15, 2005, p. 97ff; on the Russian National Security Concept and Foreign Policy Concept, pieces of legislation enacted for similar reasons as the energy strategy.

the efficiency of the export possibilities of the Russian energy sector, and to ensure that Russian companies had equal access to foreign markets, technology, and financing.[452] Russia would use its unique geographical and geopolitical location. The energy factor would be a fundamental element within Russian diplomacy, for the foreign policy realization of the energy strategy and through diplomatic support to the interests of the Russian energy companies abroad. The energy strategy occasionally used language reminiscent of military strategy: the state would support the Russian companies in the struggle for resources and markets.[453]

Parts of the conclusions of the 2003 energy strategy, primarily those concerned with foreign markets, sounded alarming to Russia's neighbours.[454] The strategy listed the objective of securing Russia's political interests, in Europe and the neighbouring countries and within the Asia-Pacific region with natural gas, and throughout the entire world with oil.[455] However, it also contained the objective to remain a stable and reliable partner for the European countries and for the whole world community with regard to the export of energy.[456]

But was Russia a stable and reliable partner? Many have argued the opposite. In fact, Russia has often been accused of using its "energy weapon" against the importing countries to secure advantages of various kinds. Accusations have been many and varied, but they can be summarized as follows. Russia is said to wish to secure political dominance over neighbou-

[452] Energeticheskaya strategiya (2003), p. 40f.

[453] Ibid., p. 42f. It was not only the energy strategy that occasionally used language reminiscent of military strategy. At the 3rd Russian Petroleum & Gas Congress in Moscow on 21-23.06.2005, Semyon Vainshtok, then president of the Russian oil pipeline monopoly Transneft, quoted the famous 18th-century field marshal, Count Alexander Suvorov, to make a point.

[454] Yet, it should in all fairness be pointed out that the 2003 strategy devoted the bulk of its text to domestic Russian concerns. In addition to several references to energy security, the energy strategy also, for instance, indicated the need for environmental security. Energeticheskaya strategiya (2003), p. 26.

[455] Ibid., p. 61 and 71.

[456] Ibid., p. 41.

ring countries; secure an economic monopoly there; and limit the West's influence in Eastern Europe.[457]

Yet, from the Russian point of view, it was Russia, not the EU states, that was vulnerable to foreign policy pressure in the energy field. This was intimately linked to Russia's role as an exporter, because Russia itself depended on transit routes to move the energy to its destination. In other words, Russia regarded itself as suffering from transit dependence. This expressed itself in the energy strategy, which singled out foreign threats (geopolitics, macroeconomics, and business conditions) to Russian security, and furthermore indicated the need to have export port terminals not under the control of foreign powers.[458] Transit dependence means dependence on a foreign power, thus making Russia vulnerable not only to swings in business conditions but more importantly, to economic or political blackmail—making Russia the victim of precisely the policy of which others have accused Russia.

By laying a natural gas pipeline to Germany across the Baltic Sea, Russia wanted to escape transit dependence. Besides, pipelines are both cheaper and environmentally safer than other modes of shipping. However, the investment cost to build a pipeline is huge. Furthermore, when a pipeline has been built, it cannot be moved. To invest in a pipeline leading to a single customer makes the supplier vulnerable to demands from the customer to re-negotiate the price of energy or cancel imports, after the investments have already been made and the project is committed. This was the lesson Russia learned with regard to the Gazprom-sponsored gas pipeline to Turkey known as Blue Stream. This pipeline began operations in December 2002, but as early as March 2003, the Turkish side suspended imports (reportedly because of this country's recession) in order to re-negotiate the agreement in its favour. Geopolitical factors also complicated the deal, be-

[457] See, e.g. Hedlund, Stefan: Russia as a Neighborhood Energy Bully. In: Russian Analytical Digest 100 (26.07.2011), p. 2ff.

[458] Energeticheskaya strategiya (2003), p. 17 and 68.

cause of the Turkish support for the American-sponsored South Caucasus Pipeline from Azerbaijan to Turkey.[459]

A key strategic concern when projecting an international pipeline is thus whether the pipeline will connect directly to the end consumer, or whether it will pass through transit states. If so, will political decisions or the international context affect how the pipeline can be used, at present or in the future? Because of perceived problems in its relations with the present transit states (primarily Poland, Ukraine, and Belarus), Russia was in the process of developing a system of natural gas pipelines (Nord Stream across the Baltic and South Stream across the Black Sea) that would bypass the transit states and instead deliver gas straight to the West European markets. From the point of view of state power, these pipeline projects were often regarded as hostile to the transit states through which the Russian energy exports to Western Europe so far flowed. Several of them were not only transit states but also, in their turn, dependent on imported Russian energy. Would Russia use threats of the suspension of energy exports as a means to impose its will on other countries, and if so, would Russia be successful? In the 1990s, a few cases had occurred in which Russia attempted to gain concessions, for instance from Lithuania, Ukraine, and Moldova. However, none of these attempts were successful. Russia gained nothing from its attempts.[460] Despite frequent claims to the contrary, there were no similar cases since the 2003 formulation of an energy strategy—with one exception. Russia repeatedly used energy deliveries as a foreign-policy instrument against one particular foreign state, Belarus.[461] This was perhaps not surprising. First, Belarus was a state that since the signing of a treaty on 8 December 1999 envisioning greater political and economic integration was formally united to Russia in a two-state union. Second, Belarus had for

[459] Torbakov, Igor: Russian Gas Company Makes Concessions in Bid to Resolve Pipeline Dispute with Turkey. In: Business & Economics, 09.07.2003.

[460] Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005.

[461] See, e.g. IWPR's Belarus Reporting Service 53, 02.03.2004, for one case among many. See also Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok. Moscow: Kommersant/Eksmo 2009, 39ff.

domestic political reasons no support whatsoever to expect from the West, even if it cried foul.

There were, however, frequent commercial disputes, in which politics at times played a role. Several disputes involved Ukraine. The trade in natural gas from Russia and Turkmenistan to Ukraine was characterized by opaque relationships, secret contracts, and hidden beneficiaries, which, most observers concluded, engendered substantial corruption, with serious losses to both the Russian and Ukrainian states as well as consumers and shareholders there and elsewhere in Europe.[462]

Some political analysts in Europe and elsewhere went further and claimed that what Russia really wanted was to limit the growth of democracy in Eastern Europe and use Eastern Europe as a first step in the creation of a new global empire.[463] Such arguments were firmly rooted in the field of politics. Ultimately, this interpretation of Russia's energy export policy became an issue of faith. Either you believed in the threat, or you did not. It was hardly coincidental that the most extreme views on Russia as an energy supplier, whether positive or negative, tended to be found in those countries that by force of geography and history depended on Russian natural gas supplies and lacked most or all other options.

Sweden was among those neighbouring countries which to some extent were alarmed by the 2003 Russian energy strategy. Sweden accordingly paid a certain level of attention to the developments of the Russian energy sector. Sweden was not a transit country, nor was Sweden dependent on Russian energy. Natural gas provided only approximately 2 per cent of Sweden's total energy consumption, and all gas deliveries came from Denmark.[464] Sweden imported Russian crude oil and petroleum products, as

[462] Fredholm, Michael: Natural-Gas Trade between Russia, Turkmenistan, and Ukraine: Agreements and Disputes. Asian Cultures and Modernity Research Report 15. Stockholm University 2008.

[463] See, e.g. Cohen, Ariel: Rethinking Reset: Re-Examining the Obama Administration Russia Policy. Testimony before the U.S. House of Representatives. Committee on Foreign Affairs, 07.07.2011.

[464] Energimyndigheten (Swedish Energy Agency): Europas naturgasberoende: Åtgärder för tryggad naturgasförsörjning. Eskilstuna 2006, p. 23ff; Energimyndigheten: Hur trygg är vår

well as some electricity, but had several sources of supply and was in no way dependent on deliveries from Russia.[465] Then why was Sweden so concerned? The explanation can be found in the project which was first called North Transgas but soon would become known as the North European Gas Pipeline (NEGP) and eventually-Nord Stream.

North Transgas and the North European Gas Pipeline Project

The idea to build a northern natural gas export pipeline from Russia across the Baltic Sea originated in Finland and had been discussed since 1993.[466] Finland, already dependent on Russian natural gas supplies, saw itself as a future transit country and wished to host a major export pipeline from northwestern Russia to Germany. A feasibility studies for such a venture was carried out in 1997-1999, when Gazprom and the Finnish firm Fortum (then Neste Oy) set up a parity joint venture, North Transgas Oy, to study the expediency of building such a pipeline.[467] Sweden was regarded as an important market as well. On 3 December 1997, Russia and Sweden, represented by Russian First Deputy Prime Minister Boris Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Anders Sundström, respectively, signed a protocol about Sweden's involvement in the construction of the pipeline.[468]

Little came out of this joint venture, yet work continued in Russia. Although Gazprom was organised as a joint-stock company and despite having some limited foreign ownership, Gazprom in many ways operated as a

energiförsörjning? En översiktlig analys av hot, risker och sårbarheter inom energisektorn år 2006. Eskilstuna 2007, p. 25.

[465] See, e.g. Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 41ff.

[466] Sinijärv, Riivo: The NEGP. Estonian Perspective. In: Baltic Mosaic. St. Petersburg Winter-Spring 2006), p. 6ff, here 6. Also noted by Jonathan Stern in Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 30. Stern may refer to the same source.

[467] NEGP web site <www.negp.info> (defunct), last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), p. 30; Neft' i kapital 10, 2004, p.113; Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15.

[468] ITAR-TASS, 03.12.1997; Izvestiya, 17.11.1998.

government agency, combining commercial and regulatory functions.[469] Envisaged as a new route for Russian natural gas exports to Western Europe, it was eventually decided in Moscow that the projected pipeline system would pass beneath the Baltic Sea from, not Finland, but Russia's Portovaya Bay near Vyborg in the Gulf of Finland to Synergiepark Lubmin, near Greifswald on the coast of Germany. The ambitious plan at that time included branch lines to be built to feed natural gas to consumers in Finland, Sweden (with an entry point at Nyköping), and the Russian Kaliningrad enclave.[470] Yet, the main beneficiaries of the gas supplies would be Germany, the Netherlands, and ultimately Britain. In Germany, two projected pipelines would receive the gas and move it further. One was the Norddeutsche Erdgas-Leitung (NEL) to Rehden in Lower Saxony. The other was the Ostsee-Pipeline-Anbindungs-Leitung (OPAL) to Olbernhau near the Czech border (and on to Brandov in the Czech Republic).[471] However, the final terminus of the projected pipeline would be Britain, accessed through the Interconnector pipeline from Zeebrügge (Belgium) to Bacton (UK) or, eventually, the BBL pipeline from Balgzand (Netherlands) to Bacton (UK).[472] Other countries including Denmark would receive gas as well.

[469] See, e.g. Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

[470] See, e.g. Izvestiya, 17.11.1998; International Energy Agency (IEA): Russia Energy Survey 2002. Paris 2002, 139. On Nyköping, see Nord Stream AG, Project Information Document – Swedish Version (November 2006), dated 24.10.2006, p. 26. This was the document submitted with the notification to the littoral states of the Baltic Sea on 14.11.2006.

[471] Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 247; Nord Stream AG, Project Information Document – Swedish Version (November 2006), dated 24.10.2006, p. 8. This was the document submitted with the notification to the littoral states of the Baltic Sea on 1411.2006. Both pipelines would be owned and managed by E.ON Ruhrgas and Wingas GmbH, the latter a joint venture between Wintershall and Gazprom. See also Wingas Transport GmbH & Co. KG, press release, 08.10.2007.

[472] See, e.g. Northwest Russia Commercial News Update <www.bisnis.doc.gov>, 1-31.12.2002. On the Zeebrügge-Bacton Interconnector, see the firm's web site, <www.interconnector.com>. On the Balgzand-Bacton-Line (BBL), operational since 2006, see the firm's web site, <www.bblcompany.com.> Gasunie has a 60 per cent share in BBL, while Belgian gas transport company Fluxys and E.ON Ruhrgas each

In December 2000, the European Commission accordingly awarded the project Trans-European Network (TEN) status, which would assist in attracting funding from international financial institutes including the European Bank for Reconstruction and Development (EBRD) and European Investment Bank. In January 2001, the chairmen of Gazprom and Fortum submitted a joint letter to the prime ministers of Finland and Russia, requesting support of both governments and the EU for the pipeline project. Two German companies, Ruhrgas and Wintershall, were invited into the project and an agreement between the participating companies on a joint study of the project to build the pipeline was signed in Moscow in April 2001.[473] Cooperation between Ruhrgas and Gazprom went back to 1970 when Ruhrgas, together with several other German industrial companies and banks, helped construct natural gas pipelines to acquire gas from Siberia for sale to Western Europe.[474] Wintershall and Gazprom had begun working together in 1990, when the Soviet Union and the Federal Republic of Germany signed an international agreement for cooperation in the gas industry.[475]

During the Russia-EU summit in Brussels on 11 November 2002, a working meeting took place between Alexei Miller, Gazprom Chief Executive Officer (CEO),[476] and François Lamoureux, Director-General of the European Commission Directorate-General for Transport and Energy (DG TREN). As a result, DG TREN again recognized the pipeline project as a priority project within the framework of the energy dialogue between Russia and the EU. On 18 November, the Gazprom board decided to begin

have 20 per cent shares. Gazprom has an option to buy a 9 per cent stake in BBL, with the shares coming from Gasunie, leaving the latter with a majority 51 per cent. See, e.g., Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 121.

[473] NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), p. 31.

[474] Russian Petroleum Investor 14: 5 (May 2005), p. 53; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15.

[475] Russian Petroleum Investor 14: 5 (May 2005), p. 54.

[476] Miller's formal title was chairman of the management committee of Gazprom.

execution of the pipeline construction project.[477] On 21 November, Miller met Leningrad Region governor Valery Serdyukov. The sides agreed to set up a joint working group consisting of authorized representatives of the Leningrad regional administration and two Gazprom subsidiaries, OOO Lentransgaz and OAO Giprospetsgaz, to coordinate the pipeline project on the territory of the Leningrad region. Then Miller travelled abroad. On 25 November, Miller met with Finnish Prime Minister Paavo Lipponen and Fortum chairman Matti Vuoria in Helsinki. On 26 November, Miller met with Dutch Prime Minister Jan Peter Balkenende and George Verberg, CEO of national gas company Nederlandse Gasunie, in The Hague. On 28-29 November 2002, Miller made an official visit to London at the invitation of the British government. He met with the British Minister for Energy, Brian Wilson, as well as the heads of British Petroleum, Royal Dutch/Shell, Centrica, and Goldman Sachs. In all these meetings, the pipeline project was one of the projects under discussion.[478]

Miller also attempted to sell the idea of the pipeline project in Sweden. On 28 March 2003, Miller met Swedish Minister for Industry (Enterprise), Employment and Communications Leif Pagrotsky in Stockholm, discussing the possibility of supplying Russian natural gas to Sweden.[479]

On 30 June 2003, in the presence of Russian President Vladimir Putin and British Prime Minister Tony Blair, a memorandum on cooperation with regard to the pipeline project was signed with Britain.[480] And late in 2003, Gazprom established a foothold in the British gas market when Wingas (a joint venture of Gazprom and Germany's Wintershall) created a joint venture on a parity basis, HydroWingas Ltd., to market natural gas in Britain.[481]

Having gained international support, Gazprom and key Russian ministries involved in the project then prepared a new feasibility study on the

[477] Northwest Russia Commercial News Update. December 2002, p. 1ff. <www.bisnis.doc.gov>; Russian Petroleum Investor 13: 4 (April 2004), p. 31f.

[478] Russian Petroleum Investor 13: 4 (April 2004), p. 32.

[479] Interfax, 31.03.2003.

[480] NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), 32.

[481] Russian Petroleum Investor 13: 4 (April 2004), 32f.

construction of the pipeline. The resulting proposal of the Russian Energy Ministry and Gazprom was examined by the Russian government. On 16 January 2004, Russian Prime Minister Mikhail Kasyanov signed decree No. 64-r of the Russian government to approve the proposal to build what was now referred to as the North European Gas Pipeline (NEGP). The Russian government charged the Energy Ministry with the preparation, with Gazprom's direct participation, of the necessary documentation for the construction of the pipeline. The Russian government assigned to the Russian Federation State Committee for Construction and the Housing and Utilities Sector (Gosstroy) and Russian Ministry of Natural Resources the task of ensuring, jointly with interested federal bodies of executive authority, the state expert examination of this documentation, and the environmental impact upon the regions that would be traversed by the pipeline.[482]

It was thus clear from the outset that the northern gas export pipeline project was a Russian government initiative. There were commercial incentives as well, and foreign participation, but as envisioned in the recently adopted energy strategy, it was the Russian state which took the initiative, not the private sector. It was also representatives of the Russian state who henceforth began to promote the project, among them notables such as Viktor Kalyuzhny, Deputy Minister of Foreign Affairs of the Russian Federation and Special Presidential Envoy for the Caspian Sea (and before that Minister of Fuel and Energy from 1999 to 2000), who declared that the NEGP would dramatically increase Russia's gas export potential.[483]

Even at this moment of perceived success, storm clouds were gathering over the project. On 4 February 2004, a Gazprom board meeting addressed the strategic issue of how to build an export policy in the face of the new conditions imposed by the EU, which simultaneously aimed to protect the energy security and labour markets of the member states and split up the major energy companies in order to liberalize the market. The EU accordingly demanded that companies such as Gazprom too would adhere to the

[482] Ibid., p. 30f.

[483] Kalyuzhny, Viktor, Deputy Minister of Foreign Affairs of the Russian Federation and Russian Special Presidential Envoy for the Caspian Sea, Statement at the Caspian & Black Sea Oil & Gas Conference 2004, Istanbul, 26.02.2004.

new policies, which conflicted with Gazprom's monopoly position. At issue were both the new policies for the EU internal market and concerns that Gazprom's dominant position would make EU member states dependent on Russia. The Gazprom board of directors reportedly concluded that the solution would be for Gazprom, jointly with the Russian government, to "persuade" the EU to cooperate and not to reduce Russian gas imports.[484] It would soon become clear that the Gazprom board and indeed the Russian government in its enthusiasm and belief in its influence with EU leaders underestimated the problem.[485]

On 11 February 2004, Gazprom CEO Miller held a Gazprom conference in Moscow on the implementation of the NEGP construction project. It was decided to go ahead and draft a detailed feasibility study. It was also decided to retain Dresdner Bank (Germany) and ABN Amro (Netherlands) as financial consultants to work on the NEGP project and the British law firm Linklaters as a legal consultant. It was also decided to conduct a tender to select an engineering consultant for the project.[486]

[484] Russian Petroleum Investor 13: 4 (April 2004), p. 35f. The board also decided to develop a strategy for the expansion of the EU and Russia's entry into the World Trade Organization.

[485] The Russian side was enthusiastic and on 05.02.2004 addressed the NEGP project issues at a meeting with François Lamoureux, DG TREN, according to Viktor Khristenko, then Russia's deputy prime minister and subsequently minister of industry and energy. Russian Petroleum Investor 13: 4 (April 2004), 37. On 06.02.2004, Khristenko gave a briefing in Moscow that the first-phase feasibility study on the NEGP would be completed before year-end 2004. He also said that a consortium of Gazprom and Finland's Fortum soon would sign a contract with the European Commission to develop a feasibility study on the pipeline. Ibid., p. 36.

[486] Ibid., p. 33 and 36. The deal with Dresdner Bank had been finalized on the day before, on 10.02.2004, when Miller met in Moscow with Herbert Walter, chairman of the Dresdner Bank board of managing directors, the two agreeing that the bank would act as a financial consultant on the project. Reuters, 10.02.2004. Finally, having carried out this preparatory work, an investment decision on the NEGP would be made in the fourth quarter of 2004. This date was later postponed, however. In the fall of 2004, Gazprom announced that it would decide whether to invest in the construction of the NEGP in the first quarter of 2005. Russian Petroleum Investor 14: 4 (April 2005), p. 42.

Gazprom planned to launch construction work in 2005, estimated that the NEGP would be commissioned in 2007-2008, and would be able to supply 20 to 30 billion cubic meters (bcm) of gas per year.[487] There was a considerable demand for these supplies in Germany and Britain, both of which needed additional gas imports. Several international energy companies, including Ruhrgas and Wintershall (both of Germany), Gasunie (The Netherlands), Royal Dutch/Shell (Britain/Netherlands), Total (France), and British Petroleum and Centrica (both of Britain), displayed an interest in the NEGP project.[488] But Gazprom wanted more than investments and had additional criteria when it came to the selection of project participants. Gazprom wanted partners which could facilitate gas sales in new markets and closure of long-term contracts for gas purchase at fixed prices.[489] What Gazprom wanted was security of supply, which indeed is the goal of most energy producers. Gazprom defined this as (1) physical security (reliable infrastructure, sufficient resource base); (2) economic security (stability); (3) legal security, and (4) secure demand (long-term projects and contracts).[490] The need for a secure demand derived from the very substantial investment costs required for construction of new energy infrastructure.

Vladimir Putin's Views on Russian Energy Policy

As had become clear from the conclusion by the Gazprom board of directors that Gazprom, jointly with the Russian government, had to "persuade" the EU to cooperate, the project was to a considerable extent not only initiated by but also dependent on the Russian state. This was no coincidence. It also conformed to the views expressed by Russia's President Putin.

Until mid-2003, Russian energy policy remained the composite product of many disparate actors, both within the state structures and the Russian pri-

[487] Russian Petroleum Investor 13: 4 (April 2004), p. 30 and 35.

[488] NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), 32 and 34.

[489] Russian Petroleum Investor 13: 4 (April 2004), 34.

[490] Tsygankov, Stanislav (Head of the Department for Foreign Economic Activities, Gazprom), "Export Strategy for Russian Gas: Securing a Reliable Supply," 7th Russian Petroleum & Gas Congress, Moscow, 25.06.2009.

vate sector. Until the spring of 2003, energy company executives even took part in the decision-making process at government level.[491] Unlike Boris Yeltsin before him, Putin attempted to limit the opportunities for the business oligarchs to enjoy direct presidential access. He preferred that a redefined version of the Russian Union of Industrialists and Entrepreneurs function as business advisory board for the Presidency.[492] Policy was soon settled in favour of state control, as described in the 2003 energy strategy.[493] This certainly included major export pipelines. Vladimir Putin stated, on 29 April 2004, that he did not intend to end state control over pipeline transportation, the key factor in Russian oil and natural gas transportation. "At the moment I consider that there are no grounds for the state to give up its control over pipeline transportation. But this does not hinder private investment, which will be welcomed." Putin continued that "private investment is possible with continued state control and state ownership of pipeline transport".[494]

Putin's opinion on this matter was well known, as was the fact that he considered natural gas a key strategic commodity. Already in October 2003,

[491] See, e.g., Interfax, 20.12.2002, on the Russian president's regular contacts with top Russian businessmen. An earlier example is provided by the 1995 energy strategy, which was drafted by a number of commissions that included, in addition to various government appointees, A. F. Dyakov, president of UES, V. D. Chernyayev, president of Transneft, V. I. Ott, vice-president of Rosneft, R. I. Vyakhirev, president of Gazprom, V. Yu. Alekperov, president of LUKoil, and V. A. Fedorchenko, president of the East-Siberian Oil and Gas Company. For further information, see Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

[492] Shevtsova, Lilia: Putin's Russia. Washington, DC 2003, p. 180.

[493] For further information, see Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

[494] Interfax, 29.04.2004.

Putin reportedly told visiting German Chancellor Gerhard Schröder in Yekaterinburg:

> "The gas pipeline system is the creation of the Soviet Union. We intend to retain state control over the gas transportation system and over Gazprom. We will not divide Gazprom. And the European Commission should not have any illusions. In the gas sector, they will have to deal with the [Russian] state."[495]

Putin's views on state planning and the importance of the energy policy for Russia's foreign relations went years back, to the time before he became president of Russia. Indeed, these views formed the key part of the candidate of sciences dissertation in economics that Putin defended in June 1997 when he was still a senior official. The dissertation was written on the topic of "strategic planning of the reproduction of the mineral raw materials base of the region under conditions of the formation of market relationships" at St. Petersburg's well-known State Mining Institute.[496] What seems to have been either an abstract or a further development of the dissertation was published in January 1999 as an article on "mineral raw materials in the strategy for development of the Russian economy" in the journal of the institute, his being the lead article in an issue devoted to the fuel and energy complex.[497]

[495] Felgengauer, Pavel: Oborona neftegazovoy truby. In: Novaya Gazeta 76.

[496] Putin, Vladimir: Strategicheskoye planirovaniye vosproizvodstva mineral'no-syr'yevoy bazy regiona v usloviyakh formirovaniya rynochnykh otnosheniy (Sankt-Peterburg i Leningradskaya oblast'). St. Petersburg 1997. On the State Mining Institute, see its web site, <www.spmi.ru>.

[497] Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 3ff. The article has since been translated into English and re-published in Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 48ff. See also Balzer, Harley: The Putin Thesis and Russian Energy Policy. In: Post-Soviet Affairs 21:3 (2005), 210ff. Putin's dissertation and journal paper were first brought to public light in Olcott, Martha Brill: The Energy Dimension in Russian Global Strategy. Vladimir Putin and the Geopolitics of Oil (Houston, Texas 2004), p. 16. Olcott doubted whether Putin wrote the dissertation himself or relied on a ghost writer, but she did not doubt that he stood for the views presented therein.

In his dissertation, Putin outlined his belief that state planning must be the key to the management of Russia's natural resources:

> "The main result of the dissertational work is that normative methodological recommendations on the creation of a system of strategic planning can be developed, corresponding to and based on the received scientific results. These recommendations will arm the state organs at all levels with an instrument with which to realize the strategic goals in developing the mineral raw materials complex."[498]

"Sustainable development of Russia's economy in the near term must be based on systematic growth in her developed sectors, and, most of all, on her mineral resource potential," Putin noted. He continued: "The main reserve to, in the near future, make Russia a great economic power with a high living standard for the majority of the population is maximum support for the fatherland's processing industry based on the extractive complex."[499] Putin also concluded that the strategic goal of state policy with regard to decisions about domestic and foreign economic policy must be "aimed at furthering the geopolitical interests and maintaining the national security of Russia."[500] Putin did not believe in globalization or global market forces, at least not at this particular stage in Russia's economic development. State planning must be at the core of Russia's resource management, he concluded. Russia's mineral resources would serve as the basis for Russia's economic development and as a guarantee for the country's economic security. This demanded what Putin described as the "creation, with full support from the state, of large financial-industrial groups-corporations with an interbranch profile that will be able to compete with Western

[498] Putin, Vladimir: Strategicheskoye planirovaniye vosproizvodstva mineral'no-syr'yevoy bazy regiona v usloviyakh formirovaniya rynochnykh otnosheniy (Sankt-Peterburg i Leningradskaya oblast'). St. Petersburg 1997, p.175.

[499] Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 3; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 49.

[500] Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 7; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 53.

transnational corporations."[501] State-sponsored foreign investment in Russia's extractive industries would also be needed, Putin noted, but the Russian state must under no circumstances lose control of the country's resources. A key demand, in Putin's words, was to "ensure that national interests are maintained when attracting foreign investment."[502]

Incidentally, Putin's views on Russian energy security would seem to correspond to his thoughts on global energy security. In February 2006, when Russia had assumed the presidency of the Group of Eight (G8, consisting of Britain, the United States, Russia, France, Germany, Japan, Italy, and Canada), Putin concluded that "all it takes is for mankind to create a balanced [energy security] potential in order to provide every state with sustainable energy supply, and international cooperation opens all avenues for that."[503] In other words, energy security was the business of states and the appropriate state organs, not privately owned corporations.

As president, Putin began to realize his vision for Russia. The natural monopolies including the energy sector, of which Gazprom was a key component, were being put under the personal authority of representatives of the Russian state in the form of members or chairmen appointed to the boards of directors. Since these representatives were generally regarded as Putin's men and came from Putin's own staff, the Presidential Administration, it was clear that not only was Putin strengthening state control over the natural monopolies, he was also strengthening direct presidential control.[504]

[501] Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 6; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 51.

[502] Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 8; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 54.

[503] Putin, Vladimir: 'Energy Egotism Is a Road to Nowhere'. In: Wall Street Journal, 29.02.2006.

[504] Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005 Policy.

Examples of his appointees included both Alexei Miller, a friend of Putin from St. Petersburg, who was appointed CEO of Gazprom in May 2001,[505] and Dmitry Medvedev, the Head of the Presidential Administration, who was appointed Chairman of Gazprom in June 2002.[506] Among other Gazprom board members with direct links to the Russian top leadership were, by 2004, German Gref, Minister for Economic Development and Trade of the Russian Federation; Viktor Khristenko, Minister of Industry and Energy of the Russian Federation; Farit Gazizullin, Minister for Property Relations of the Russian Federation; Igor Yusufov, Special Representative of the President of the Russian Federation for International Energy Cooperation, Ambassador-at-large of the Ministry of Foreign Affairs of the Russian Federation; and (until 25 June 2004) Alexandra Levitskaya, First Deputy Head of the Secretariat of the Presidential Administration.[507]

The Putin-Schröder Concord

On 8 July 2004, during German Chancellor Gerhard Schröder's visit to Moscow, Germany's largest electricity and gas concern, E.ON AG, and Gazprom signed a memorandum of understanding with regard to a variety of areas of energy sector cooperation including the construction of the NEGP. This strategic alliance was hardly surprising. E.ON was now Gazprom's largest foreign investor, having in February 2003 acquired Ruhrgas AG (and had on 1 July 2004 changed the firm's name to E.ON Ruhrgas AG; E.ON Ruhrgas thus controlled directly and through Gerosgaz, a joint venture with Gazprom subsidiary Gazexport, 6.43 per cent of Gazprom's

[505] Upstream, 17.06.2005, p. 32.

[506] Gazprom web site, <www.gazprom.ru>. Medvedev was chairman of the board of directors of Gazprom also in 2000-2001, as well as deputy chairman of the board of directors of Gazprom from 2001 to June 2002. Russian President's official website, <www.kremlin.ru>, last accessed in September 2008.

[507] Gazprom Annual Report 2004, dated 17.05.2005. Inside observers concluded that even though the election of Gazprom's new board of directors was scheduled for 25.06.2004, it virtually took place at the 04.02.2004 Gazprom board meeting, with the main proposed candidates from the government already selected to the 2004 board of directors. Russian Petroleum Investor 13: 4 (April 2004), p. 36.

shares).[508] The foundation for cooperation between Gazprom and E.ON thus became Ruhrgas, which had worked with Gazprom since 1970.[509]

Yet negotiations continued with Wintershall as well. Wintershall AG was a fully owned energy sector subsidiary of the chemical concern BASF AG. On 11 April 2005, at the Hannover International Trade Fair, Gazprom CEO Alexei Miller and BASF Chairman of the Board Jürgen Hambrecht signed a memorandum of understanding with regard to natural gas production in Russia and elsewhere. As part of the agreement, Wintershall AG would receive a 49 per cent interest in a joint venture to construct the first phase of the NEGP.[510] On the same day in Hannover, Miller also met with the CEOs of E.ON and E.ON Ruhrgas, Wulf Bernotat and Burckhard Bergmann. The three company heads continued work on details of the memorandum of understanding signed in the summer of 2004. It had become apparent that the deal was a complex one that also included investments in the Russian gas industry. It was clear that BASF had reached an agreement first, but E.ON was still interested in the project. At the Hannover press conference Miller noted: “Now E.ON knows that it has a serious foreign competitor”.[511]

On 15 February 2005, after a meeting with German Chancellor Schröder, Miller had announced that the NEGP would be in operation by 2010.[512] Finland and Fortum were now out of the picture, and so was the Finnish vision of turning Finland into a transit state. On 17 May 2005, the Gazprom board of directors approved the acquisition of the remaining 50 per cent interest in the joint venture North Transgas Oy, owned by Fortum Heat and Gas Oy. Fortum explained its withdrawal from North Transgas Oy as part of a “restructuring of its gas assets”.[513] In reality, Fortum had lost interest in the project. As the hope for Finland to become a transit

[508] Russian Petroleum Investor 13: 9 (October 2004), p. 26ff, on 26.

[509] Russian Petroleum Investor 14: 5 (May 2005), p. 53.

[510] Ibid., p. 49 and 54.

[511] Ibid., p. 50.

[512] Ibid., p. 55.

[513] Fortum Corporation Interim Report, January-June 2005. Russian Petroleum Investor 14: 10 (November / December 2005), p. 48.

country had evaporated, Fortum had acquired new priorities. Besides, the German firms had taken a firm lead as foreign partners in the fundamentally Russian project.

On 8 September 2005, Russian President Vladimir Putin and German Chancellor Gerhard Schröder met in Berlin. During the meeting, Alexei Miller, Gazprom CEO, Jürgen Hambrecht, chairman of the board of BASF AG, and Wulf Bernotat, chairman of the board of E.ON AG, signed an agreement in principle to construct the NEGP. The parties would create a Russian-German joint venture, the North European Gas Pipeline Company (NEGPC) as the operator of the project. Gazprom would hold 51 per cent interest in the joint venture, and the German companies would each hold 24.5 per cent (through E.ON Ruhrgas AG and Wintershall Holding GmbH, respectively). It was now confirmed that the pipeline would allow Russia direct access to western EU markets, bypassing existing transit countries. Both the Russian and German sides regarded as a key prerequisite of the project that natural gas delivery through NEGP to the consumer would not be contingent on the political will of the transit countries, Poland, Ukraine, and Belarus. There would also be no transit fees as were paid when moving natural gas through other countries.[514] On 16 September 2005, Gazprom CEO Miller signed an order for the investment phase of the NEGP project.[515] Preparations for construction began, in particular in the Vologda and Leningrad Regions which in any case needed further natural gas infrastructure for their own use.[516]

Now Britain, then already a net importer of natural gas, felt left out. Two years had passed since the Putin-Blair meeting when a memorandum of cooperation had been signed. On 13 September 2005, the British Minister for Energy, Malcolm Wicks, speaking at a meeting of the Association of European Businesses in Moscow confirmed that Britain remained inte-

[514] Russian Petroleum Investor 14: 10 (November / December 2005), p. 46 and 51.

[515] Ibid., p. 46.

[516] Ibid., p. 49.

rested in Russian natural gas supplied via the NEGP. He also argued for British companies to participate in the project.[517]

It was really only from the September 2005 Schröder-Putin summit that the neighbouring countries began to comment on the project. Having been quite deliberately shut out of the project and at risk of losing both transit fees and political influence over the Russian gas trade with Western Europe, Poland and Ukraine opposed the construction of the NEGP. So did the Baltic states. Political leaders from the Baltic states and Poland, including Latvian Prime Minister Aigars Kalvītis, made attempts to persuade the EU that the decision by Russia and Germany to build the NEGP across the Baltic Sea was "ill-conceived" and that the project should not be implemented. Polish President Aleksander Kwaśniewski had by then already opposed the project, claiming that he was bewildered that Russia and Germany would carry out such a large-scale project while ignoring the economic interests of other EU member states. Kwaśniewski also argued that the NEGP project was environmentally disruptive, as well as "ineffectual from economic and political perspectives" and "a bad project". Others including Lithuania's Prime Minister Algirdas Brazauskas argued that construction of the NEGP would turn into an environmental catastrophe for the Baltic Sea and that Second World War-era chemical weapon caches on the Baltic seabed would be disturbed by the construction work and cause an ecological disaster.[518] In a controversial statement at a conference in Brussels on 30 April 2006, Polish Minister of National Defence Radosław Sikorski said the oil pipeline deal was in the Molotov-Ribbentrop tradition, in comparison to the 1939 Molotov-Ribbentrop non-aggression pact between the Soviet and Nazi German foreign ministers dividing Poland between the two countries.[519] Some even began to refer to the project as the Putin-Schröder pact.[520]

[517] Ibid., p. 52.

[518] Ibid., p. 51.

[519] BBC News, 30.04. 2006; Der Spiegel Online, 01.05.2006.

[520] Sinijärv, Riivo: The NEGP. Estonian Perspective. In: Baltic Mosaic. St. Petersburg Winter-Spring 2006), p. 7.

However, in Finland comments were muted. Since neither Sweden's government nor industry had yet been formally invited to participate, there were few immediate comments there either.

On 9 December 2005, construction work on the project began in the form of the welding of the first joint of NEGP, in the area of the Babayevo village in the Vologda Region. Among those attending the ceremony were Russian Prime Minister Mikhail Fradkov, Minister of Industry and Energy Viktor Khristenko, German Minister for Economy and Technology Michael Glos, Gazprom CEO Miller, and the chief executives of the German firms E.ON AG and BASF AG, Wulf Bernotat and Jürgen Hambrecht. The new German Chancellor Angela Merkel declined to participate.[521]

After the ceremony, it was announced that German ex-Chancellor Gerhard Schröder would become the future chair of the North European Gas Pipeline Company (NEGPC) shareholders' committee (board of directors). It also became know that Matthias Warnig, chairman of the Board of Directors of Dresdner Bank ZAO in the Russian Federation, had been proposed as managing director of the NEGPC.[522] Neither appointment was totally unexpected, and the choice of Schröder had been preceded by rumours to that effect since 10 October.[523]

The appointment of Schröder caused a heated debate in Germany. While the energy industry generally considered the appointment a boon which would guarantee good relations with Gazprom and Russia, much of the media regarded the appointment as a disgrace or worse.[524]

As agreed, the joint Russian-German venture NEGPC was established in Zug, Switzerland, on 5 December 2005. Gazprom held 51 per cent in the joint venture and BASF and E.ON each had a 24.5 per cent stake. Zug was

[521] NEGP Press Release, 09.12.2005; Russian Petroleum Investor 15: 2 (February 2006), p. 12.

[522] Russian Petroleum Investor 15: 2 (February 2006), p. 10; Russian Petroleum Investor 15: 6 (June/July 2006), p. 26.

[523] Roth, Jürgen: Der Deutschland-Clan: Das skrupellose Netzwerk aus Politikern, Top-Managern und Justiz. Frankfurt am Main 2006, ch.7.

[524] Russian Petroleum Investor 15: 2 (February 2006), p. 10.

reportedly chosen because of its favourable taxation legislation.[525] Since Gazprom remained controlled by the Russian state, the project thus retained its character of a Russian state project although with, in the words of Putin, foreign investment. On 30 March 2006, the first official meeting of the shareholders' committee of the NEGPC was held at the Gazprom headquarters in Moscow. Gazprom proposed, and the committee elected, Gerhard Schröder as chairman.[526]

As managing director of the NEGPC, the Shareholders' Committee, as expected, appointed Matthias Warnig.[527] During the last decade of the Cold War, Warnig had been a Ministry for State Security (Ministerium für Staatssicherheit, MfS, since commonly known as the Stasi) officer in Dresden, at the same time when Vladimir Putin served there as a representative of the Soviet security service, the Committee for State Security (KGB). Putin served in East Germany with the KGB from 1985 to 1990.[528] Warnig served with the Stasi from 1975 but was on duty in West Germany from 1986 to August 1989. Although Warnig and Putin claimed not to have met before St. Petersburg in October 1991, they had certainly been good friends for more than a decade.[529] Warnig's background too was duly noted by foreign observers, in Sweden and elsewhere.[530]

[525] Saar-Echo (Germany), 14.12.2005. Zug was already the home of another Gazprom joint venture, RosUkrEnergo. Fredholm, Michael: Natural-Gas Trade between Russia, Turkmenistan, and Ukraine: Agreements and Disputes. Asian Cultures and Modernity Research Report 15. Stockholm University 2008.

[526] Russian Petroleum Investor 15: 6 (June/July 2006), 26; Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006).

[527] Russian Petroleum Investor 15: 6 (June/July 2006), p. 26.

[528] The Telegraph (UK), 27.02.2005; St. Petersburg Times (Russia), 01.03.2005; Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 145.

[529] Die Welt (Germany), 03.08.2014; Der Spiegel (Germany) 35, 2008, p. 81. However, Roth refers to a former Stasi officer who claimed that Putin and Warnig met already in East Germany. Roth, Jürgen: Der Deutschland-Clan: Das skrupellose Netzwerk aus Politikern, Top-Managern und Justiz. Frankfurt am Main 2006, ch.7.

[530] Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 21. According to one of the U.S. State Department cables exposed by Wikileaks, Ambassador John R. Beyrle at the U.S. Embassy in Moscow in 2009 apparently advised that "given

Moreover, although an office opened in Zug on 4 October 2006, the shareholders' committee decided to open a NEGPC branch office in Moscow as well.[531] It later became clear that important activities took place in Moscow, not Zug. Yet the consortium claimed that more than three quarters of the total staff of about 70 would work in Zug.[532] The same importance to the Moscow link seems to have applied to the appointment of Warnig, who in a meeting with the U.S. Ambassador in Moscow reportedly described himself as a "de facto employee of Gazprom."[533]

5.3.2 Part 2: The Pipeline Project as a Hybrid Threat

The Swedish Government's Reaction

As noted, the Swedish government perceived the proposed NEGP as a threat to several Swedish core interests: the desire to gradually end European reliance on hydrocarbons as a key source of energy; the ambition to protect the Baltic Sea environment; and the desire to minimize naval activities in the Baltic. In addition to these laudable goals, there was the military dimension, the hard security threat, which in effect would overshadow the others.

It was known that a pipeline such as the NEGP might be used as a sensor platform for Russian military intelligence collection against Swedish targets. This was not a mere hypothetical scenario, nor was the installation of sen-

Warnig's reportedly close friendship with Prime Minister Putin, we recommend the Department facilitate Mr. Warnig's meeting requests." Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

[531] Russian Petroleum Investor 16: 1 (January 2007), p. 31; Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006). Apparently "a handful of employees" had met in Zug to establish a headquarters already in August 2006. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 4 and 21. They included Matthias Warnig and other senior managers. Kommersant (Russia), 30.08.2006.

[532] Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006), p. 5.

[533] According to one of the U.S. State Department cables exposed by Wikileaks. Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

sors only a precaution against terrorism, as the Russian side from time to time claimed.[534] As early as 2004, the Russian Baltic Fleet had implemented plans to install a radar station on an oil platform at the Kravtsovskoye deposit (known as D-6), located 22 km from the shore of Kaliningrad, to which the platform was connected with a pipeline, on the Baltic shelf and owned by the Russian oil company LUKoil-Kaliningradmorneft. This facility had been announced as the Baltic Fleet's first sea-based radar station and, due to the platform's position in the Baltic Sea, was described as a significant addition to the Baltic Fleet's surveillance capability.[535] Plans for integrated systems for monitoring air, surface, and underwater movements had already been announced in 1999, with the stated intention of guarding and defending littoral territories and sea zones against intrusion by submarines and surface ships as well as against saboteurs and terrorists from "groups of people or enemy states" through the use of a variety of sensor systems including over-the-horizon target acquisition radar, optronic surveillance systems, electronic reconnaissance systems, and sonar and electromagnetic surface and underwater target acquisition systems.[536] Besi-

[534] Hinted at by Russian defense minister Sergei Ivanov already on 15.05.2006 in his comment that the Northern Fleet would be vested with the task of anti-terrorist defense and of providing security for the routes of transportation of Russian hydrocarbon resources to world markets. ITAR-TASS, 16.05.2006.

[535] ITAR-TASS, 12.06.2004.

[536] Baranenko, Anatoly/Belyayev, Vladimir/Klimov, Sergei/Kuzmenko, Anatoly/Sokolov, Sergei and Shcherbakov, Nikolai: Protection of 200-Mile Zone, a Priority Task of Coastal States. In: Military Parade: The Magazine of the Military Industrial Complex 31, January-February 1999, p. 48ff. The authors were distinguished, with Rear Admiral Baranenko the head of the Radio-electronic Warfare Center at the Naval Academy, Kuzmenko the Chief Expert of the Navy Directorate of the Rosvooruzhenie state enterprise, and the others affiliated to the Altair state research and production association. Additional information on the technology was published by Rear Admiral Baranenko in Soloviev, Igor/ Korol'kov, Grigoriy and Anatoly, Baranenko: Morskaya radioelektronika: Spravochnik. Politekhnika, 2003, ch. 2. See also Baranenko, A./Karpov, M./Demidovich, A. and Makarov Yu: BSN kak element boyevogo obespecheniya VMF (Shore observance system as an element of the Navy's combat support). In: Morskoy Sbornik: Zhurnal Boyenno-Morskogo Flota 1836 (November 1999), p. 58f. Written by a group of naval officers including Rear Admiral Baranenko, this article provides additional historical and technical information.

des, using underwater sensor chains as tripwires for monitoring submarines was not a new idea. During the Cold War, the United States and NATO had relied on its Sound Surveillance System (SOSUS), which consisted of seabed-mounted hydrophone arrays connected by underwater cables to facilities ashore, to detect Soviet ballistic missile submarines, in particular those which from bases in the Barents and White Seas aimed to gain access to the North Atlantic by rounding northern Norway and steering south through the Greenland-Iceland-United Kingdom (GIUK) gap.[537]

But cooperation between Russian military and energy sector actors went far beyond sensor platforms. On 27 September 2004, LUKoil and the Russian Ministry of Defence had signed a broad cooperation agreement on the provision of technical and financial assistance to a range of defence establishments, including the Rear Services and Transport Military Academy in St. Petersburg, the military hospital in Khimki outside Moscow, and the main personnel department of the Ministry of Defence. LUKoil would, in addition to continuing to supply the armed forces with fuel and lubricants, also attempt to find employment for those who were discharged from military service.[538] Meanwhile, Gazprom was developing a cooperation program with the Russian Navy, in which naval vessels and infrastructure would be used in the development and transportation of liquefied natural gas (LNG) in the Barents Sea, and naval cooperation would be sought in the preparations for the construction of the NEGP. Gazprom had already begun its naval cooperation program on 19 October 2002, when Gazprom and the Russian Navy signed a protocol on intentions to promote interaction and long-term cooperation in Russian oil and natural gas offshore exploration and development. During 27-30 September 2004, Gazprom experts and Navy officers had jointly visited the Northern Fleet facilities, inspecting potential building sites for a gas liquefaction plant, and in January 2005, possible building sites had been examined by OAO Giprospetsgaz, the Gazprom subsidiary which also appeared in relation to the NEGP pro-

[537] Whitman, Edward C.: SOSUS: The ‘Secret Weapon’ of Undersea Surveillance. In: Undersea Warfare: The Official Magazine of the U.S. Submarine Force 7: 2 (Winter 2005).

[538] ITAR-TASS, 27.09.2004.

ject in the Baltic. Gazprom announced its intention to cooperate with the Navy in the construction of the NEGP in March 2005.[539]

The dilemma for the Swedish government was how to act on the information that the pipeline project had the potential to be used as a sensor platform. Several powerful neighbours, including Russia and Germany, were determined to carry out the pipeline project. Another powerful European state, Britain, supported the project. And despite the military dimension, the pipeline was in its setup a commercial project.

Because of this dilemma, the Swedish government had to handle the situation in multiple dimensions. First, after the September 2005 agreement to build the NEGP, the Swedish Ministry of Defence sponsored the first of several studies on the project. These were prepared by the FOI, an assignment-based authority under the Ministry of Defence. This meant that the FOI conducted research on a fee basis, on topics chosen by whichever branch of government had sponsored the assignment. The FOI conducted research independently and it would be both incorrect and unfair to suggest that the FOI produced research results merely to satisfy the sponsor's preconceptions. Yet, since the sponsor initiated and paid for the assignment, it was only natural that the sponsor also suggested avenues of research. The FOI categorized the project as "Policy support to the Government (Defence)" and described it as a security, safety and vulnerability analysis.[540] In addition, the aforementioned inter-ministerial working group from the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment was set up in the first half of 2006.[541] This resulted in a memorandum on the pipeline project, dated 15 March 2006.[542]

[539] Gazprom press release, 18.03.2005; Gazprom 4 (April 2005), p. 5.

[540] Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 2.

[541] Sveriges Television (SVT), Nyheter, 07.12.2006. The internal document, published by Swedish state television, was a Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006.

[542] Näringsdepartementet (Ministry of Industry (Enterprise)), Naturgasledning i Östersjön - North European Gas Pipeline, Memorandum, 15.03.2006.

The Ministry of Defence took the lead in coordinating defences. In late 2006, after several months of deliberation, the Ministry of Defence requested seven agencies under its authority to investigate and assess the security, defence, and environmental implications of the pipeline project, including the possible implications of Russian naval vessels in the area and the potential to use the pipeline and its offshore platform for intelligence collection. The seven, which included the Armed Forces (which incorporated the Military Intelligence and Security Service, MUST), the national signals intelligence agency (FRA), the Emergency Management Agency (KBM), the Rescue Services Agency (SRV), the Coast Guard (KBV), the National Defence College (FHS), and the Defence Research Agency (FOI), were asked to provide written responses by 9 February 2007 and were also invited to a first hearing on 6 December 2006.[543]

By then, the pipeline issue was also being debated in the media. A key role came to be played by the FOI. The FOI studies were highly critical of the pipeline project. Even in the first FOI study of the NEGP, it was noted that the construction of the NEGP was assessed as increasing Russian leverage on the neighbouring states. The bypassed states (Poland, the Baltic states, Belarus, and Ukraine) would become more vulnerable to Russia if Russia chose to act coercively. In addition, the study concluded, the states which supported the project and would benefit from it (primarily Germany, Denmark, the Netherlands, and Britain) were at risk of becoming more sensitive to Russian pressure, if Russia chose to apply it. The FOI was concerned that the NEGP would become a tool for Russia to impose its will on its near neighbours, which would affect Swedish national security.[544] These concerns were duly noted by the Swedish Ministry of Defence. In

[543] Försvarsdepartementet (Ministry of Defense): Inbjudan till hearing samt anmodan att lämna upplysningar m.a.a. den föreslagna rysk-tyska gasledningen Nord Stream, reference FÖ2006/2715/MIL, dated 17.11.2006. Released by the Ministry of Defense on 12.07.2014. The Swedish names of the latter agencies were Krisberedskapsmyndigheten (KBM), Statens räddningsverk (SRV), Kustbevakningen (KBV), Försvarshögskolan (FHS), and Totalförsvarets forskningsinstitut (FOI). The initiative was also announced in Riksdag & Departement 34, 2006, p. 7.

[544] Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 30ff.

effect, Sweden worried that its neighbours would fall prey to appeasement politics in the event of future Russian aggression.

And then there was the sensor issue. The first FOI study in June 2006 raised the alarm in public for a direct Russian threat emanating from the proposed pipeline. The study noted that "[i]t can also be assumed that the NEGP have a military dimension, e.g. concerning military protection of the pipeline and usage of the infrastructure for military or intelligence purposes."[545] The second FOI study, published in early 2007, was yet more outspoken. The study concluded that the prospects for using the offshore compressor platform then planned for the pipeline as well as the pipeline itself "as platforms for active and passive sensors are rather good" and that "Russia would get a competitive intelligence edge concerning all subsurface, surface and aerial monitoring in the Baltic Sea."[546]

This issue was also raised in one of Sweden's leading dailies, *Svenska Dagbladet*. In November 2006, three days before the Ministry of Defence requested its ancillary agencies to investigate and assess the pipeline issue, the newspaper referred to an anonymous source with inside knowledge of the Swedish government's work with regard to the project. This source volunteered information that the pipeline and platform could be used as a structure on which to mount underwater sensors. The pipeline, which would traverse the entire Baltic Sea, would then become a tripwire which would register the movements of all vessels in its vicinity. It would in effect be impossible for Swedish or other military vessels, even submarines, to move without the Russian military registering each and every movement near or across the pipeline. The Russian capacity for early warning would be tremendous, and the capability of the Swedish navy to move undetected in times of crisis would in effect evaporate. Whether this leak from inside the Swedish government was intentional or not, the technical feasibility of using the pipeline as a sensor mount was confirmed by Rear Admiral Emil Svensson, head of underwater systems at the Swedish Defence Materiel

[545] Ibid., p. 32.

[546] Larsson, Robert L.: Nord Stream, Sweden and Baltic Sea Security. Stockholm: FOI, March 2007, p. 37 and 49.

Administration (FMV).[547] In light of this, the appointment of Warnig as managing director of the NEGPC appeared ominous. Even though by then he had long experience as a businessman, his Stasi background and known friendship with President Putin suggested that he might not be averse to letting intelligence sensor operators into the project.

Besides, Russian President Vladimir Putin had unexpectedly spoken out in terms that seemingly supported the Swedish concern over national security issues. On 25 October 2006, Putin said in a TV interview that the Russian navy would have to protect Russia's economic interests in the Baltic. Like in many other countries, including Britain, he noted, the navy would have to carry out purely economic tasks in addition to military ones. In this context, Putin specifically mentioned the pipeline project as "one or our most important priorities" and also spoke about involving the Russian Baltic Fleet in efforts to tackle a series of tasks in building the pipeline, since nobody knew the conditions of the Baltic better than the naval personnel.[548] These remarks were widely reported by the Swedish media.[549]

In fact, the Russian president echoed earlier comments by the Russian defence minister, Sergei Ivanov. In October 2005, he had concluded that military security was needed to protect offshore rigs, offshore operators, and for "supplying special services during the development and operation of offshore shelf deposits."[550] On 15 May 2006, speaking about the Northern Fleet, Ivanov had concluded that

[547] Svenska Dagbladet (Sweden), 14.11.2006.

[548] Pryamaya liniya s Prezidentom Rossii Vladimirom Putinym, 25.10.2006, TV transcript <www.liniya2006.ru>. The TV interview covered a large variety of topics and the pipeline issue was only one among many; yet it was only the pipeline-related comment which was noted in the Swedish press. Eventually, from December 2008 to February 2009 and from May 2009 to January 2010, the Baltic Fleet indeed cleared munitions identified in Russian waters in support of the pipeline project. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 45.

[549] See, e.g. Svenska Dagbladet (Sweden), 14.11.2006.

[550] ITAR-TASS, 28.10.2005.

> "the state already has serious plans to develop large oil and gas fields in the Barents Sea. The Northern Fleet has a detailed knowledge of these plans because the fleet will definitely be vested with the task of anti-terrorist defence and of providing security for the routes of transportation of Russian hydrocarbon resources to world markets."[551]

Then, on 30 July 2006, Ivanov stated that Russia's national interests could not be protected without a naval component and also spoke specifically about the Baltic Fleet: "Its existence makes it possible to seriously influence military and political processes taking place on Russia's western frontiers."[552]

The Swedish Government's Position

Despite the comments by Putin and Ivanov, a difficulty for the Swedish government was that it had little freedom of action. Neither Sweden nor the other Baltic states could formally stop pipeline construction but they were involved in consultations which gave them the power to affect how quickly the project moved forward. In effect, they could obstruct and delay the project but not prevent it. According to international legislation, all states are entitled to lay submarine cables and pipelines on the continental shelf.[553] There was therefore no real way to refuse the project, even though the pipeline would pass through the Swedish exclusive economic zone. However, under the Espoo Convention of 1991, the state or enterprise which intended to lay such a pipeline first had to prepare an environmental impact assessment (EIA).[554] A pipeline project could, as a result, be refused upon environmental grounds, until such a time that an acceptable EIA had been prepared. Even so, this meant that it was only strictly environmental considerations associated with the construction or use of the proposed pipeline which might be used to delay the project, and only until such harmful effects upon the environment had been neutralized.

[551] ITAR-TASS, 16.05.2006.

[552] RIA-Novosti, 30.07.2006.

[553] United Nations Convention on the Law of the Sea of 10 December 1982, Article 79.

[554] Convention on Environmental Impact Assessment in a Transboundary Context, signed at Espoo, Finland, on 25 February 1991.

The Swedish government was therefore bound to approve the pipeline project, as long as the consortium submitted a substantive EIA. The closed debate within the Swedish government on what means might be available to stop or at least delay the project until it became unfeasible for economic or practical reasons is evident from the aforementioned internal Swedish government document from August 2006 on the proposed pipeline produced by an inter-ministerial working group from the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment, exposed by Swedish state television. The document concluded that the project was not in Sweden's interest, that Sweden would not benefit from it, and that its many disadvantages would have a considerable negative impact on Sweden. The document listed several areas of negative impact: environmental risks especially with regard to the huge volumes of unexploded munitions (regular munitions, chemical warfare munitions, and mines) known to have been dumped in the Baltic Sea; reasons of national security including the issue of underwater sensors, the potential of Russian signals intelligence collection from the offshore platform, and the risk of an increased Russian military presence in the Swedish exclusive economic zone tasked with protecting the pipeline and offshore installation; the impact on the fishery industry; and the resulting loss of freedom of action within the exclusive economic zone. The document also suggested strategies to contain the threat. The options were quite limited. It might be possible to rely on an exemption within the United Nations Convention on the Law of the Sea by referring to the serious environmental implications of the project. In the event the consortium's EIA discussed other routes with less environmental impact or alternatives which simply were cheaper to build, the government would have cause to refuse the project (Article 5 in the Espoo Convention noted that the EIA might allow for consultation on possible alternatives to the proposed activity, including the no-action alternative and possible measures to mitigate significant adverse transboundary impact). With regard to the potential for Russian intelligence collection, the document concluded that even if the Swedish government accepted the EIA and gave the necessary permits to build the pipeline, the permit would then only cover the commercial activities of the consortium, never any intelligence use of the infrastructure by state actors. Besides, the document duly noted that according to Article 60 in the United Nations Convention on the Law of the Sea, the coastal State shall have the exclusive right to construct and to authorize and regulate the construction, operation, and use of offshore platforms such as the compressor platform planned by the consortium in the exclusive economic zone. The authors of the document consequently noted that if the government refused the construction of the offshore platform, the entire project might become so expensive or possibly even technically unfeasible that the consortium might give up. However, they also concluded that political pressure, from the consortium as well as other states such as Russia or Germany, with the aim of making Sweden issue the required permits for the project would have to be expected.[555]

In other words, the environmental impact was important, but it was the proposed offshore platform which was the key. Not only did it pose a threat to national security, it was also the one component of the project which the Swedish government could legally refuse.

An analysis of the Swedish media shows that it was indeed the military dimension of the pipeline project which came to dominate the public Swedish debate, which can be said to have been opened in July 2006 by retired Ambassador Krister Wahlbäck, an academic who had retained contacts within the Foreign Ministry, in an opinion article in the influential daily *Dagens Nyheter*.[556] Wahlbäck claimed that, earlier in the summer, he had met officials from the German Foreign Ministry who had then said that they expected Sweden to approve the pipeline project. There is little reason to believe that Wahlbäck was unaware of the ongoing internal debate within the Swedish government when he published his article. The first FOI study had been published the previous month. Besides, the key arguments raised in the internal document (dated a week later but surely then already in the making) were also raised by Wahlbäck, including the possibility that the pipeline facilities would be used for Russian intelligence collection. In addition, the same evening following its publication, Wahlbäck appeared on

[555] Sveriges Television (SVT), Nyheter, 07.12.2006, which exposed and published the aforementioned Policy Memorandum from the Ministry of the Environment, dated 8 August 2006.

[556] Wahlbäck, Krister: Stoppa ryska gasledningen som hotar Östersjöns hälsa ("Stop the Russian gas pipeline which threatens the health of the Baltic Sea"). Dagens Nyheter (Sweden), 31.07.2006.

national television together with Minister of Education and Culture Leif Pagrotsky, who commented on the pipeline project in a semi-private capacity.[557]

Wahlbäck began his article by arguing for environmental concerns, yet he focused on economic and national security issues. This became the pattern of the public debate. While many newspaper articles on the projected pipeline predictably mentioned the environmental concerns raised by the project, they often did so only in passing, without giving any substantial information. This was in contrast to newspaper articles on the economic and security aspects of the project. The press treated the environmental effects as self-evident or merely used the environment as a dramatic enhancer. A study on how the Swedish press reported the pipeline issue determined that the information category most frequently covered by the press was the economy, which appeared in 71 per cent of the articles in which the pipeline appeared in the influential daily *Dagens Nyheter* from March 2002 to May 2008. The second most important information category was national security, which appeared in 62 per cent of the articles. In comparison, environmental aspects of the project were mentioned in only 39 per cent of the articles. When passing mentions were excluded, the pattern became yet clearer: 68 per cent of the articles included substantial information on the project's economic aspects, 59 per cent provided the same on national security aspects, and only 25 per cent did the same with regard to the project's environmental aspects. And of the articles which dealt with the environmental implications, 11 per cent in fact downplayed environmental concerns.[558]

Even so, this focus on economics versus national security was not acknowledged by the press itself. In fact, in November 2006, the national daily *Svenska Dagbladet* noted in the aforementioned major article on the

[557] Roos, Lars André: Politiska nätverk och Nord Stream. En möjlighet att vara med och påverka. Report, Karlstads universitet 2007, p. 8.

[558] Fransson, Anna-Lisa Sayuli/Elander, Ingemar and Lidskog, Rolf: Framing Issues and Forming Opinions: The Baltic Sea Pipeline in the Swedish Media. In: European Spatial Research and Policy 18: 2 (2011), p. 102, 103 and 104.

national security implications of the pipeline project that “so far, the Swedish debate has been on the environmental risks”—but went on to describe the entire pipeline project as a potential national security problem.[559] On the very same morning, the leading daily *Dagens Nyheter* published a substantial opinion article on the national security aspects of the project by the opposition Social Democratic party’s national security spokesperson, Ulrica Messing. This article too began by concluding that “the perhaps most obvious threat – the environmental threat – has received considerable and deserved attention, whereas another at least equally important factor so far has been ignored”—which was the national security implication.[560] Yet, an examination of the contents of the newspaper articles devoted to the project shows that as of this particular date, only 6 out of 28 articles in *Dagens Nyheter* had dealt with environmental issues.[561] Sweden’s official core interests focused on the environment but they took little space in either the public or internal government debate.

The two leading Swedish dailies raised the national security aspects of the pipeline project on the very same day that the Nord Stream consortium submitted its formal notification of intent. On the same day, Sweden’s Defence Minister Mikael Odenberg made common cause with his opposition counterpart, Messing, explaining in a national public radio interview that “[t]his kind of pipeline can be used as a platform for intelligence collection. This naturally causes concerns. It brings security and defence repercussions for us.”[562] On the following day, a printed interview with Defence Minister Odenberg was even more outspoken, as Odenberg was cited as explaining that “[w]e get a gas pipeline which motivates a Russian naval presence in

[559] Svenska Dagbladet (Sweden), 14.11.2006.

[560] Dagens Nyheter (Sweden), 14.11.2006. Messing subsequently published, alone or with party colleagues, a number of identical or almost identical articles in various Swedish provincial newspapers. See, e.g. Blekinge Läns Tidning, 17.11.2006; Gotlands Allehanda, 17.11.2006; Barometern Oskarshamns-Tidningen, 20.11.2006; Ljusdals-Posten, 24.11.2006.

[561] Fransson, Elander, and Lidskog, ”Framing Issues and Forming Opinions,” p. 105.

[562] Sveriges Radio (Sweden), 14.11.2006.

our economic zone and which the Russians, if they wish, can exploit for intelligence collection. This is obviously a problem."[563]

Sweden, by the way, was not the only country which by then had noted the national security aspects of major energy sector projects. For several years, the German intelligence service, the Bundesnachrichtendienst (BND), had organized public seminars on important issues. On 12 October 2006, the BND held its "BND Symposium 2006" in Berlin. The topic was "Energie - Quelle von Konflikt und Kooperation/Energy - Source of Conflict and Cooperation" which in light of the pipeline debate was highly topical. During the Symposium, Germany's chief of the Chancellor's office and federal minister of special affairs as well as Federal Government Commissioner for the Intelligence Services (*Kanzleramtsminister*) under Chancellor Merkel, Thomas de Maizière, noted that Germany's and Europe's energy supply by no means was secure. Cooperation with Russia was necessary, or the Russian natural gas risked being diverted to China, de Maizière warned, in the same way that other energy streams risked being diverted to the United States. The intelligence service would have to pay particular attention to the strategic developments within the energy sector, and would have to contribute to the nation's energy supply, he concluded.[564] There was little doubt during the Symposium that the German side considered the pipeline project across the Baltic a key priority, although the Germans too were

[563] Dagens Nyheter (Sweden), 15.11.2006.

[564] de Maizière, Thomas: Unsere Energieversorgung ist keineswegs gesichert. Speech at the BND Symposium 2006: Energie - Quelle von Konflikt und Kooperation/Energy - Source of Conflict and Cooperation, Berlin 12.10.2006, subsequently published in the German Federal Government web site, www.bundesregierung.de. His exact words were: "Unsere Energieversorgung ist keineswegs gesichert. [...]Auch die Energieversorgung Europas kann keineswegs als gesichert angesehen werden. [...] Selbst das Gas aus Nordwestsibirien, das seit langem mehr als ein Drittel unserer Erdgasimporte sichert und damit unverzichtbar ist, könnte zu einem Teil nach China abfließen. Entsprechende Äußerungen russischer Verantwortlicher haben in den letzten Monaten in Europa beträchtliche Unruhe verursacht. [...] Diese Entwicklungen zu beobachten und zu analysieren ist eine wichtige Aufgabe auch und vor allem für Nachrichtendienste. [...] Eine verlässliche und wirtschaftliche Versorgung mit Energie ist keine Selbstverständlichkeit. Sie ist eine zentrale Aufgabe, dazu können auch die Nachrichtendienste beitragen."

suspicious of Russia's ultimate intentions. Germany's diplomatic lobbying in favour of the project would continue. When Günter Gloser, German Minister of State for Europe, visited Sweden in April 2008, he concluded that Nord Stream was "essential" to meet European demand for gas.[565] And when in June 2009 the U.S. Ambassador in Moscow asked whether the Nord Stream project had the full support of the German government, the managing director of Nord Stream, Matthias Warnig, reportedly

> "said yes, noting that he has regular, direct access to Chancellor Merkel's office and that Nord Stream Chairman Gerhard Schroeder also meets frequently with Merkel. However, Warnig lamented that Russian diplomacy is sometimes heavy-handed and counterproductive."[566]

Whether Russia's intelligence services took active part in support of the Nord Stream project remains unknown to outside observers, even though rumours to this effect were in sway.[567] Indeed, the Russian media noted that in Germany accusations were directed against Gerhard Schröder who

[565] Gloser, Günter, Minister of State for Europe: The European Partnership with Russia, speech at the Swedish Institute of International Affairs, Stockholm 01.04.2008, transcript.

[566] According to one of the U.S. State Department cables exposed by Wikileaks. Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

[567] According to one of the U.S. State Department cables exposed by Wikileaks, an American diplomat on 03.11.2009 met with Estonian Member of Parliament Marko Mihkelson, Chair of Parliament's European Affairs Committee. Mihkelson reportedly claimed that "Russian foreign intelligence officers (SVR) have been active in Estonia investigating opposition to the pipeline. This he saw as clear evidence Nord Stream is a political, not economic project." Mihkelson also reportedly noted that militarily, Russia had used the defense of Nord Stream as an element of its September 2009 Ladoga and Zapad military exercises, during which Russia and Belarus had practiced fending off an attack from the direction of the Baltic States. Reference ID #09TALLINN325, dated 06.11.2009. <http://wikileaks.org>. While the exposed cable was cited widely, it in no way proves that the SVR operated in support of the Nord Stream project. At most, the cable suggests that there was a belief among some policy makers that the SVR was so engaged.

some claimed had already fallen into the hands of Russian intelligence during his term as Chancellor.[568]

The Seabed Surveys

It was not only the initiative to build the pipeline which came from the Russian state. So did the decision to launch the first seabed surveys in anticipation of constructing the pipeline. In addition, they were carried out in part by Russian naval personnel.

The first seabed survey was commissioned in 1998 by the company North Transgas as part of the first feasibility study.[569] The consortium later claimed to have asked the Swedish firm Marin Mätteknik AB (MMT) and Geoconsult in July-September 1998 to carry out the work.[570] Yet the study was carried out by AO PeterGaz, a Gazprom subsidiary. PeterGaz subsequently claimed that permits had been issued by the national authorities of the countries involved; presumably the firm considered the aforementioned protocol signed on 3 December 1997 by Russian First Deputy Prime Minister Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Sundström equal to a permit.[571]

PeterGaz also carried out the first surveys for NEGP. The first was initiated in 2004, conducted in October 2005 and consisted of a geophysical survey of the seabed in a corridor two kilometres wide along the proposed route. Two potential routes were chosen. In 2006, yet another survey took place. This was more detailed, along a corridor 180 meters wide.[572] The

[568] Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 141.

[569] Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>.

[570] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 41.

[571] Nord Stream: Nord Streams kartläggningsaktiviteter i överensstämmelse med internationella och nationella rättsliga krav. Press release. 30.08.2007. On PeterGaz, see company web site, <www.petergaz.com>.

[572] Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>; Nord Stream: Sammanfattning av projektet.

Swedish government in fact issued a permit in 2005 which was renewed and applied also for 2007.[573] At a minimum, the 2005 and 2006 surveys involved Russian naval personnel onboard the research ships, R/V *Professor Shtokman* and R/V *Akademik Golitsyn*, for instance when the latter carried out survey work "on behalf of Gazprom" in the Gulf of Finland and around the Danish island of Bornholm. Nord Stream AG later claimed that Russian naval personnel only participated when in Russian waters, but this was clearly incorrect with regard to the survey work around Bornholm.[574] Whether Russian naval personnel in fact participated along the entire route remains unknown to outside observers. At any rate, their participation was hardly surprising since President Putin had suggested that the Russian Baltic Fleet would be involved in the construction work and Dmitry Shilyayev, head of the PeterGaz research department, later reportedly acknowledged that the Baltic Fleet would use modern deepwater unmanned devices for the control both of the route and the quality of laying the pipeline.[575] The two research vessels, R/V *Professor Shtokman* and R/V *Akademik Golitsyn*, had formerly been registered as state-owned, belonging to the Soviet Academy of Sciences, but had since been re-registered as belonging to Gazflot, a Gazprom-affiliated company. They were advanced research vessels of the types which were repeatedly suspected of involvement in intelligence collection during the last years of the Cold War, owing to their advanced communications and survey equipment and often unusual sailing pat-

Stockholm 30.09.2009, p. 4; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15 and 41.

[573] Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006; Dagens Nyheter (Sweden), 02.02.2007.

[574] Krasnaya zvezda (Russia), 25.07.2007; citing Fleet Admiral Vladimir Masorin, commander of the Russian Navy; Nord Stream: Nord Streams kartläggningsaktiviteter i överensstämmelse med internationella och nationella rättsliga krav. Press release. 30.08.2007.

[575] Putin in Pryamaya liniya s Prezidentom Rossii Vladimirom Putinym, 25.10.2006, TV transcript <www.liniya2006.ru>; Russian Petroleum Investor 16: 10 (November/December 2007), p. 30. Shilyayev presumably referred to a remotely operated vehicle (ROV).

terns.[576] As research vessels, they were eminently suitable for survey missions. In September-December 2006, for instance, the *Akademik Golitsyn* surveyed the entire sea route of the proposed gas pipeline utilizing video camera equipped underwater apparatus, with experts from PeterGaz alongside the naval personnel.[577] Other research vessels which participated included the *Akademik Mstislav Keldysh* and *AtlantNIRO*, operated by the Russian Academy of Sciences and AtlantNIRO, a research institute subordinated to the Russian Federal Agency for Fisheries, respectively. The vessels and institutes involved in the surveys thus show a clear pattern of Russian state control. However, from 2007, when the NEGPC had become Nord Stream AG, non-Russian survey ships were chartered as well. The consortium, for instance, employed a Swedish company, Marin Mätteknik AB (MMT), which specialized in sea measurements and geology, for the continued environmental studies and seabed survey. MMT began with a survey of construction routes in the area of Bornholm Island in May 2007.[578] The firm used a multipurpose offshore support vessel named *Pollux*.[579]

By then, Nord Stream AG was in the process of contracting with a large number of international companies and institutions. Quite a few were Swedish, including some which were state-owned. In addition to MMT, the consortium hired, among others, SSPA (formerly *Statens Skeppsprovningsanstalt*, Sweden); Geological Survey of Sweden (*Sveriges geologiska undersökning*, SGU, Sweden); Stockholm University; IVL *Svenska Miljöinstitutet* (Sweden); Environmental Resources Management (ERM);[580] DOF Subsea (Norway)

[576] See, e.g, Agrell, Wilhelm: Bakom ubåtskrisen: Militär verksamhet, krigsplanläggning och diplomati i Östersjöområdet. Stockholm 1986, p. 176f.

[577] Russian Petroleum Investor 16: 10 (November/December 2007), p. 30; citing Dmitry Shilyayev, head of the Petergaz research department.

[578] Russian Petroleum Investor 16: 10 (November/December 2007), p. 30; citing MMT founder and managing director Ola Oskarsson and others. On the AtlantNIRO, see the institute web site, <www.atlantniro.ru>. On MMT, see company web site, <www.mmt.se>.

[579] Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>. MMT among other systems employed a remotely operated vehicle (ROV).

[580] Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 28 and 93.

and continued to rely on PeterGaz (Russia) for the seabed survey and technical engineering for the Russian section. In addition, Nord Stream AG hired the Danish consultancy company Rambøll[581] to prepare the EIA; Institut für Angewandte Ökologie (Institute for Applied Ecology, Germany) to conduct additional Baltic Sea environmental studies; and the company Det Norske Veritas (DNV, Norway) for controlling and certification. Saipem Energy Services (formerly Snamprogetti, Italy) would have the lead for the technical engineering process, while Saipem (Italy) would be responsible for pipe laying. EUPEC (France) would be responsible for logistics (concrete coating, pipe storage, transport), while EUROPIPE (Germany) would manufacture the majority (75 per cent) of the pipes needed for the first line, and OMK (Russia) the remaining 25 per cent of pipes. PetrolValves (Italy) would supply the necessary valves.[582]

NEGP Becomes Nord Stream, and the EIA Approval Process Begins

On 4 October 2006, coincidentally a week before the BND Symposium, the North European Gas Pipeline Company (NEGPC) changed its name to Nord Stream AG and opened its head office in Zug, Switzerland.[583] On the following day, 5 October 2006, the Dutch gas firm N.V. Nederlandse Gasunie became the fourth member to join the pipeline consortium. Gasunie CEO Marcel Kramer and Gazprom CEO Alexei Miller signed a Memorandum of Understanding in Moscow, with Dutch Minister of Economic Affairs Joannes Gerardus (Joop) Wijn attending the meeting.

[581] On this company, see Rambøll web site, <www.ramboll.com>. Rambøll had carried out the first feasibility studies for the pipeline project already at the time of North Transgas Oy. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 26.

[582] Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG. See also Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 95.

[583] Russian Petroleum Investor 16: 1 (January 2007), p. 31; Nord Stream: The New Gas Supply Route to Europe. Press release. 22.11.2006.

Gasunie would eventually acquire 9 per cent of Nord Stream equity out of the German-held shares.[584]

As noted, the Swedish counterstrategy relied on the legal requirement that the pipeline construction project would have to undergo an EIA in line with the Espoo Convention and national legislation of the concerned countries. The EIA authorities in Germany, Denmark, Sweden, Finland, and Russia had already agreed, in a meeting on 19 April 2006, that the pipeline project would be handled under the Espoo Convention. The Espoo Convention called for submitting a notification of intent about the project to responsible authorities in those countries (Russia, Finland, Sweden, Denmark, and Germany), the exclusive economic zones of which would be crossed by the pipeline, as well as in neighbouring states such as Poland, Latvia, Lithuania, and Estonia. The consortium submitted the notification documentation to the littoral states of the Baltic Sea on 14 November 2006.[585] In the 80-page Project Information Document, the venture was described as an offshore natural gas transmission system consisting of two separate pipelines crossing the Baltic Sea between Russia and Germany. The second line would be built after the first one. Consultations with competent bodies and the public at large were also planned, along with the preparation of a program and EIA report. The EIA report was then expected to be finalized in the fall of 2007, and Nord Stream hoped to have the EIA approved in early 2008.[586] In fact, Nord Stream optimistically planned that the materials acquisition would already begin in April 2007 and that the first line would be laid by December 2009.[587]

[584] Russian Petroleum Investor 16: 1 (January 2007), p. 31.

[585] Nord Stream: Project Information Document – Swedish Version (November 2006), dated 24.10.2006. This was the document submitted with the notification to the littoral states of the Baltic Sea on 14.11.2006. On the 19.04.2006 meeting, see p. 32.

[586] Sveriges Radio (Sweden), 14.11.2006; Nord Stream: Nord Stream. The New Gas Supply Route to Europe. Press release. 2211.2006; Russian Petroleum Investor 16: 1 (January 2007), p. 34f.

[587] Followed by the second line from November 2011 to October 2013. Nord Stream, Nordeuropeiska gasledningen (NEGP) (Sjödel): Bilaga till anmälan till utsatta parter enligt artikel 3 i Esbokonventionen. Zug 2006, p. 3. The document, which

Nord Stream submitted different EIA reports to each country, since each was responsible for its exclusive economic zone.[588] In Sweden, the Environmental Protection Agency administered the EIA approval process. After Nord Stream AG had submitted its notification of intent, Sweden followed protocol, publishing the notification with a request that all relevant agencies and authorities would comment by 26 January 2007.[589] A number of comments came in, and on 16 February 2007, the compiled comments were sent to Nord Stream AG.[590] In Sweden, two permits were needed. The part of the pipeline located in the Swedish exclusive economic zone would require a permit under the Act of the Continental Shelf. The

accompanied the notification to the littoral states of the Baltic Sea on 14.11.2006, was marked as a preliminary version, yet was the one submitted.

[588] See, e.g. Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 121. In Denmark, the approval process was administered by the Forest and Nature Agency, Ministry of the Environment; in Estonia, by the Ministry of Environment; in Finland, by the Ministry of the Environment; in Germany, by the Federal Maritime and Hydrographic Agency (Bundesamt für Seeschifffahrt und Hydrographie); in Latvia, by the Ministry of Environmental Protection and Regional Development of Latvia; in Lithuania, by the Ministry of Environment; in Poland, by the Ministry of Environment; and in Russia, by the Department of International Cooperation in the Field of Environmental Protection and Nature Use of the Ministry of Natural Resources of the Russian Federation. Swedish Environmental Protection Agency (Naturvårdsverket), Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference Dnr 121-7846-06 Rv, dated 14.11.2006, p.4; Federal Maritime and Hydrographic Agency, Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, n.d. (November 2006).

[589] Naturvårdsverket, Synpunkter på underlag för miljökonsekvensbeskrivning för Nord Stream Gas Pipeline, reference Dnr 121-7846-06, dated 17.11.2006.

[590] Naturvårdsverket, Synpunkter på Nord Stream AG:s planerade gasledning genom Östersjön öster om Gotland (Naturvårdsverket, press release, 17.11.2006); Naturvårdsverket, Synpunkter inför utarbetandet av miljökonsekvensbeskrivning (MKB) för den planerade nordeuropeiska gasledningen Nord Stream och prövningarna enligt kontinentalsockellagen och lagen om Sveriges ekonomiska zon: Yttrande, reference Dnr 382-216-07, dated 15.02.2007; Larsson, Nord Stream, Sweden and Baltic Sea Security, 25.

permitting authority was the Government (Ministry of Industry (Enterprise), Employment and Communications). As for the offshore service platform, it would require a permit under the Act of the Swedish Economic Zone. The permitting authority was again the Government (Ministry of Sustainable Development, that is, the Environment).[591]

Meanwhile the Nord Stream consortium continued to promote the project. Problems soon appeared. In early 2007, the government of Finland recommended Nord Stream AG move the projected route in the Gulf of Finland further south, into the exclusive economic zone of Estonia. On 31 May 2007, Nord Stream AG turned to Estonia with a request to survey the possibilities for a change of route. However, by then relations between Estonia and Russia had grown increasingly tense, in particular because of the controversy of the Bronze Soldier, a Soviet Second World War memorial which had recently been moved out of the city centre of the Estonian capital. In September 2007 the Estonian parliament refused Nord Stream's request.[592]

Poland too attempted to thwart the project, among other concerns arguing that the pipeline would hinder future dredging of the seabed to accommodate a route for tankers to reach Poland.[593] This objection was eventually overcome as well.[594]

So far, no EIA had yet been submitted. However, by the end of 2007, Nord Stream AG noted that Denmark and Germany were in agreement

[591] Swedish Environmental Protection Agency (Naturvårdsverket), Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference Dnr 121-7846-06 Rv, dated 14.11.2006, p. 2.

[592] See, e.g. BBC News, 28.04.2007; Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 116ff; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 72.

[593] Letter from Minister of the Environment Jan Szyszko to the Swedish Environmental Protection Agency, reference DOOS-082/ /2007/AK, sent as part of the notification process.

[594] But not until February 2010 when a route change was approved in German waters. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 72 and 75.

with the Russian position, while negotiations with Sweden were still ongoing. Nord Stream hoped for a constructive position by Sweden, claiming that the Swedish authorities had already agreed to a route within Sweden's economic zone. Presumably Nord Stream meant the aforementioned protocol signed on 3 December 1997 by Russian First Deputy Prime Minister Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Sundström and the undisputed, by Sweden, TEN-E status of the project.[595]

On 21 December 2007, Nord Stream AG submitted the EIA to the Swedish government and applied to lay a pipeline in the Swedish exclusive economic zone.[596]

The Nord Stream project was by no means an issue only between Sweden and the consortium. The pipeline had been debated in the European Parliament as well, and the Directorate-General for Internal Policies had scrutinized the project.[597] On 29 January 2008, a public hearing on the Nord Stream project was organized by the Committee of Petitions, in association with the Committee on Foreign Affairs and the Committee on Industry, Research and Energy of the European Parliament. A number of critical voices were raised, particularly by members of parliament from Britain,

[595] Russian Petroleum Investor 16: 10 (November/December 2007), p. 30. On 06.09.2006, the European Commission confirmed the project's status within the Trans-European Network (TEN-E). Decision No 1364/2006/EC of the European Parliament and of the Council of 06.09.2006 laying down guidelines for trans-European energy networks. The project was mentioned in an appendix among many others. Although the decision on TEN-E status was formalized only in 2006, the actual deliberation on TEN-E projects took place already on 17.06.2005, before the September 2005 Schröder-Putin summit which alerted the neighbouring countries to the immediate realization of the pipeline project. It is highly unlikely that either EU or national political decision-makers took notice of the implications of each and every project listed in the appendix when the list was compiled.

[596] Ministry of the Environment, press release, 21.12.2007.

[597] See, e.g. European Parliament, Directorate-General for Internal Policies: The Nord Stream Gas Pipeline Project and its Strategic Implications: Note. Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Petitions, PE 393.274, 2007.

Poland, Lithuania, and Estonia, as well as by a representative of Sweden's FOI.[598]

On 12 February 2008, the Swedish government rejected the application as incomplete, claiming the need for a more complete EIA.[599] Nord Stream had to begin work on a second EIA. A period of intensive Nord Stream lobbying then began (see below), to secure the approval of the second application, when it finally would be ready. However, various Swedish interest groups continued to express negative views on the project. So did the German media. On the day following Sweden's rejection of the application, the German weekly *Stern* argued that serious questions remained with regard to the sensors issue, and also the fibre optic communications cable which would accompany the pipeline. *Stern* had noted that the sensor monitoring data would end up in Moscow in addition to Zug. Besides, *Stern* observed, in a previous pipeline project built through Poland (the Yamal pipeline), Gazprom had installed its own telecommunications system without first informing the Polish authorities. As it turned out, the main source for the *Stern* article was the Swedish FOI.[600] The German media apparently found the FOI conclusions more persuasive, or at least better copy, than those of the German government, which remained in favour of the project,

[598] Nord Stream: Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008. Nord Stream AG produced the document immediately following the 29.01.2008 hearing. Among the participants were Robert Larsson of the Swedish FOI and Andrew Riley of City University, London.

[599] Miljödepartementet and Näringsdepartementet: Begäran om komplettering av ansökan om tillstånd till utläggande av rörledningssystem enligt lagen (1966:314) om kontinentalsockeln och ansökan om tillstånd till uppförande och användning av en serviceplattform enligt lagen (1992: 1140) om Sveriges ekonomiska zon.. 12.022008. Reference M2007/5568/F/M, N2008/147/FIN; Andreas Carlgren: Miljödepartementet, Regeringens prövning av gasledning i Östersjön. Press meeting. 12.02.2008.

[600] Larsson, Robert L.: Security Implications of the Nord Stream Project (FOI Memo, 12.02.2008, reference FOI-R-2336-SE), p. 15; Stern (Germany), 13.02.2008.

as was evident from the aforementioned remarks by Günter Gloser, Minister of State for Europe, in April 2008.[601]

The Modified EIA

On 1 October 2008, the Nord Stream consortium updated and modified its application, that is, in effect submitted a second one. The application to build an offshore service platform, the one feature of the project which the Swedish government could legally refuse, was thereby formally withdrawn.[602]

Would the Swedes accept the updated EIA? On 12 November 2008, Putin himself joined the fray. In a meeting in Moscow with Finland's Prime Minister Matti Vanhanen. Putin suddenly declared that if Europe was unwilling to accept the pipeline, then Russia would instead build LNG plants and ship the LNG in a fleet of tankers.[603] The option of using LNG tankers was again raised in September 2009.[604] The threat of using tankers rather than a pipeline was bound to make an environmental impact.[605] Moving the gas as

[601] Gloser, Günter, Minister of State for Europe: The European Partnership with Russia, speech at the Swedish Institute of International Affairs, Stockholm 01.04.2008, transcript.

[602] Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6; Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009. Nord Stream had already in early 2008 admitted that no offshore platform was necessary. Nord Stream: Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea", European Parliament, Brussels. 29.01.2008, p. 11. Nord Stream AG produced the document immediately following the 29.01.2008 hearing. Realizing that Sweden would not grant a permit for the offshore platform, Nord Stream abandoned this part of the project. Nord Stream claimed to have withdrawn the application to build an offshore platform on 08.04.2008. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 69.

[603] Reuters, 12.11.2008; Dagens Nyheter (Sweden), 13.11.2008.

[604] Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 101.

[605] The environmental implication of LNG tankers in the Baltic had been raised by the FOI already in early 2007. FOI, Yttrande till Försvarsdepartementet rörande Nord

LNG in tankers would be more expensive, and Putin no doubt knew that the environmental impact of increased shipping in the Baltic would worry Sweden and other Baltic powers more than that of the pipeline. According to some calculations, transporting the same annual amount of natural gas through the Baltic Sea by ship would demand from five hundred to six hundred LNG tankers, and tanker collision would be a real danger.[606] In early 2008, Nord Stream AG had indeed argued that more than six hundred tankers per year would be needed in the Baltic.[607]

Other European countries proved more amenable to the Nord Stream project than Sweden. In June 2009, Russia's Ministry of Natural Resources and Ecology (MNRE) noted that Russia, Denmark, and Germany, following the latest round of consultations in Germany, had concluded that the project did not entail material environmental risks.[608] On 30 June 2009, Russia's Regional Water Administration issued a water permit for construction in Russian waters.[609] Soon after, in July 2009, positive news came from Finland as well. The Finnish environmental regulator concluded that construction of Nord Stream did not represent a serious environmental threat for Helsinki. While the Russian side took this as an approval, the conclusion did not represent a final assessment so more would be needed. However,

Stream och gasledningen genom Östersjön, 06-1964:3, dated 07.02.2007. Written response to Ministry of Defense request for information FÖ2006/2715/MIL, dated 17.11.2006. By 2009 (if not before), it was also known that the Swedish Coast Guard opposed the idea to bring more tankers into the Baltic Sea. Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 22.

[606] European Parliament, Directorate-General for Internal Policies: The Nord Stream Gas Pipeline Project and its Strategic Implications: Note. Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Petitions, PE 393.274, 2007, p. 2. The document carries no exact date but was produced after 14.11.2007.

[607] Nord Stream, Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008, p. 5. Nord Stream AG produced the document immediately following the 29.01.2008 hearing.

[608] Russian Petroleum Investor 18: 8 (September 2009), p. 22.

[609] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73.

the project could move to the next approval stage, according to the Finnish environmental preservation agencies. This was the Uusimaa Regional Environment Centre which, although it considered Nord Stream AG's environmental impact assessment to be sufficient in its fundamental aspects, required further investigations, including that of the spread of nutrients and harmful substances during the project; ensuring maritime safety during construction; restricted zones for fishing and trawling; continuous monitoring of environmental impacts; and the effects of eventual pipeline decommissioning. More research was also needed on the impact on fishing, and the plan for the follow-up monitoring of the project's environmental impact was poorly laid out, the Finns concluded.[610] In a separate development, on 2 October 2009, a munitions clearance permit was granted by the Finnish authorities.[611]

The Swedish position by then remained unchanged. Formally Sweden stuck to a legalistic approach, had not yet taken an official position, and awaited additional environmental impact studies.[612] In January and February 2009, the Nord Stream consortium responded to the comments received with regard to the second application.[613] Between 9 March and 21 August 2009,

[610] Russian Petroleum Investor 18: 8 (September 2009), p. 26.

[611] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 47 and 73. In November-December 2009 and April-June 2010, the munitions in Finnish waters were cleared by BACTEC International Ltd., which in March-April 2010 also cleared the munitions found in Swedish waters.

[612] This was also the position usually adopted in discussions with representatives of other countries. According to one of the U.S. State Department cables exposed by Wikileaks, a Swedish diplomat reportedly said that "the Swedish government was not opposed to the project, as long as it passed strict Swedish environmental review. 'The environment is important to Swedes; there will [be] no special deals and no political intervention.'" Reference ID #07MOSCOW5585, dated 29.11.2007. <http://wikileaks.org>. According to another cable, a Swedish official reportedly said that "all public signs from Sweden's political leadership support Nordstream, for 'greater diversity leads to decreased dependency.' However, he added, 'remember that the bridge to Denmark took 8-10 years to approve' because of challenges and appeals based on environmental concerns. Approvals for the Nordstream pipeline to cross Sweden's EEZ would take at least as long," the official reportedly concluded "with a grin." Reference ID #08STOCKHOLM792, dated 28.11.2008. <http://wikileaks.org>.

[613] Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6.

another period of consultation took place during which all relevant agencies and authorities were requested to comment on the Nord Stream project, and Nord Stream AG took the opportunity to present its view to those who commented. On 5 June and again on 30 September 2009, Nord Stream AG supplied additional data on the alternative routes which had been suggested.[614] Still Sweden made no commitments. Furthermore, Sweden would assume EU presidency during the second half of 2009. This period would prove crucial for the project, and the trade press glumly argued that the Swedish presidency might cause difficulties for Russian projects.[615]

On 16 July 2009, as soon as Sweden had assumed the EU presidency, Russian President Dmitry Medvedev held a press conference with German Chancellor Angela Merkel during an official visit to Germany. Medvedev first thanked Finland for its positive decision on the EIA (although in fact no final decision had been made), then expressed his hope that this example would inspire the other states involved in the process. Medvedev noted:

> "With regard to the position of Sweden, we know what their position is and we have to treat it with respect. At the same time, we believe that there are additional explanations that can make a difference, and given the fact that Sweden currently holds the presidency of the EU, it has a great opportunity to contribute to the energy security of Europe."

Speaking in support of the Russian view, Merkel added,

> "I am one of those who don't spend a lot of time worrying about the controversy surrounding pipelines. [...] And if you look at the demand for gas in Europe over the next decade, there are many opportunities for trade between Russia and Europe, Russia and Germany."

[614] Letter from Matthias Warnig, Nord Stream, to the Ministry of Industry (Enterprise), Energy and Communications (Näringsdepartementet), dated 29.09.2009; Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6; Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009.

[615] Russian Petroleum Investor 18: 8 (September 2009), p. 26f.

There was thus little doubt that Germany still lobbied for the pipeline project.[616]

On 2 October 2009, the French firm GDF SUEZ announced that its intention to acquire 9 per cent of the shares in Nord Stream AG would be negotiated shortly.[617] This meant that France too wished to see the pipeline built.[618] A number of West European countries by then supported the pipeline project, as can be seen by a brief survey of the annual contracts for gas delivery up to 2035 which had already been signed. Wingas (Germany) had contracted up to 9 bcm of natural gas, followed by E.ON Ruhrgas (Germany), with up to 4 bcm. Gazprom Marketing & Trading (Britain) had contracted up to 4 bcm. Britain had visibly supported the project during the early years (although interest later faded because of political changes in its relationship with Russia which went beyond the purpose of this study[619]).

[616] Ibid., p. 27.

[617] Russian Petroleum Investor 18: 10 (November/December 2009), p. 9. In June 2008, Gaz de France and Suez had merged and named itself GDF SUEZ.

[618] Russian Petroleum Investor 19: 3 (March 2010), p. 14. Indeed, a memorandum to this intent was eventually signed on 01.03.2010, during an official visit to France by President Dmitry Medvedev, with GDF SUEZ SA on 20.06.2010 acquiring 9 per cent of the equity from the German shares. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 23.

[619] The reason was chiefly connected to energy policy and state control. Gazprom had in 1999 established a subsidiary in Britain named Gazprom UK Trading, which in 2004 was replaced by Gazprom Marketing & Trading Ltd. Its purpose was to sell natural gas to the U.S. market, among others, but also eventually to gain a 10 per cent share of the British market. In 2006, Gazprom negotiated to purchase a 20 per cent share of Britain’s largest energy utility firm, Centrica, a bid ultimately not found acceptable by the British authorities, likely upon political grounds. See, e.g., RIA-Novosti (Russia), 17.11.2004; BBC News, 02.02.2006, 03.02.2006. In summer 2006, Vitaly Vasiliev, head of Gazprom Marketing & Trading, still worked to receive 3-7 bcm through Interconnector and BBL to gain 10-15 per cent of the British market. Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 121. However, other political tensions were building up as well, with Britain hosting a cluster of high-profile Russian exiles unanimously opposed to President Putin including the Chechen leader Akhmed Zakayev, wanted for charges of terrorism, the controversial Russian businessman Boris Berezovsky, wanted for charges of, among others, corruption, and former Russian agent Alexander Litvinenko, who died on 23.11.2006 in London and who in a posthumously public letter accused Putin of his death. In 2007, Zakayev and oth-

GDF SUEZ (France) contracted up to 2.5 bcm, while Dong Energy (Denmark) had contracted up to 1 bcm.[620] The Netherlands too had an interest in the project, as was clear from Gasunie joining the consortium in 2006.[621]

On 20 October 2009, Denmark granted a construction permit for Nord Stream through Danish waters.[622]

Finally, on 5 November 2009, Sweden and, a few hours later, Finland approved Nord Stream construction through their exclusive economic zones. Sweden added a number of conditions for its approval so as to ensure some degree of control over the pipeline project.[623] Sweden's approval came two weeks before an EU-Russia summit in Sweden's capital Stockholm scheduled to take place on 18 November.[624] Holding the EU chairmanship, there had apparently been no way for Sweden to postpone the decision further. Even so, the process had taken almost three years since notification and 23 months since Sweden received the original EIA application.

Yet the Swedish government stuck to its official legalistic line and noted that the environmental provisions had been satisfied. "No serious Swedish government would so blatantly break international law that it would say no to the pipeline," clarified the Minister of the Environment, Andreas Carlg-

ers repeated Litvinenko's accusations. The tensions grew, and in early 2008 the British Council offices in Yekaterinburg and St. Petersburg were ordered closed. See, e.g. Reuters, 18.01.2008.

[620] Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG. Dong expected to sell on some 0.6 bcm of its share to Gazprom Marketing & Trading Ltd for sale in Britain. Western Europe Oil and Gas Insight 4 (Business Monitor International, August 2006), p. 8.

[621] An historian cannot fail to note that Sweden had not faced such an alliance since the days of the Great Northern War (1700-1721).

[622] Russian Petroleum Investor 18: 10 (November/December 2009), p. 9 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73.

[623] Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009; Russian Petroleum Investor 18: 10 (November/December 2009), p. 9f.

[624] Russian Petroleum Investor 18: 10 (November/December 2009), p. 10.

ren, in an interview.[625] On a personal level or in a semi-private capacity, comments were often less neutral. Indeed, the personal views of Swedish government members remained mostly identical regardless of political party affiliation.[626] With regard to Russian natural gas, the opinion of a majority of Swedish politicians could seemingly be summarized in the words of the Minister of Education, Jan Björklund, a few months prior to the decision: "There are only two problems with Russian gas. First, it is gas. Second, it is Russian."[627] The view of the Swedish government was that any increased use of hydrocarbons was detrimental to its ambition to reduce the global emission of greenhouse gases. No matter that other European countries needed the natural gas; this was a matter of faith for Swedish governments regardless of political colour, as Björklund's comments showed.

When the Swedish approval came, few bothered about the fact that Russia and Germany had not yet approved the project. The Russian and German approvals were by then rightly assumed to be a formality.[628] Russia granted the permit to construct the offshore section on 18 December 2009, and Germany followed on 21 and 28 December.[629] Finland had granted an exclusive economic zone usage license on 5 November 2009, in accordance with the Act on the Finnish Exclusive Economic Zone, but had not yet

[625] Dagens Nyheter (Sweden), 05.11.2009.

[626] Göran Persson, Prime Minister of the Social Democratic government until 06.10.2006, was a noted opponent of both Russian natural gas and the pipeline project, and this was well known in Russia. On 13.06.2006, he in Parliament noted that he had never hidden the fact that he did not wish to introduce Russian natural gas in the Swedish energy supply system (in Swedish: "Jag har heller aldrig dolt att jag inte vill introducera rysk gas i det svenska energisystemet"). EU-nämndens stenografiska uppteckningar 2005/06:42 13.06.2006. A month later, Prime Minister Persson in an interview with a leading Swedish financial news weekly said that Sweden was ready to stop the pipeline project. Veckans affärer (Sweden), 09.08.2006 (print issue dated 17.08.2006). On 18.08.2006, he in Visby described the pipeline project as an environmental threat since it could stir up munitions and chemical substances from the Second World War. Vedomosti (Russia), 21.08.2006.

[627] Jan Björklund. Speech in Marstrand, 20.08.2009. In Swedish: "Det finns bara två fel på rysk gas. Det ena är det är gas. Det andra är att den är rysk."

[628] Russian Petroleum Investor 18: 10 (November/December 2009), p. 9.

[629] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73 and 75.

granted a construction permit. The latter would be provided by the Western Finland Environmental Permit Authority which decides whether to approve a construction permit under Finland's Water Act. Finland provided its second and final approval on 12 February 2010.[630]

Nord Stream AG was finally cleared to begin construction. On 6 April 2010, the first seabed pipe was laid. Three days later, a ceremony to celebrate the event was held, attended by Russian President Dmitry Medvedev, Dutch Prime Minister Jan Peter Balkenende, ex-Chancellor of Germany and chairman of the Nord Stream board Gerhard Schröder, Gazprom CEO Alexei Miller, Nord Stream AG managing director Matthias Warnig, and the new Commissioner for Energy in the European Commission, Günther Oettinger.[631]

Nord Stream Lobbying

"Nord Stream was possibly the most unpopular infrastructure project in Europe," Nord Stream later admitted.[632] During the entire EIA process, Nord Stream AG therefore spent considerable efforts on lobbying and the recruitment of lobbyists. Already from the outset, when ex-Chancellor Schröder was appointed chairman of the consortium, the venture had been keen to recruit influential lobbyists. Yet more were to follow, on national as well as local levels in the countries in which the EIA process and pipeline construction would take place. In August 2008, for instance, Finland's former Prime Minister Paavo Lipponen was employed as a consultant for Nord Stream AG, with the task of assisting in the application to Finland.[633]

[630] Ministry of the Environment (Finland): Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference YM5/5521/2006. 14.11.2006; Russian Petroleum Investor 19: 3 (March 2010), p. 14.

[631] Russian Petroleum Investor 19: 5 (May 2010), p. 41.

[632] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 75.

[633] Helsingin Sanomat (Finland), 15.08.2008.

But most lobbying activities took place in Sweden. When the commercial Swedish television station TV 4 investigated the lobbying activities of Nord Stream AG in its investigative television show *Kalla fakta* ("Cold facts"), it noted that many of these activities took place on the local level of government, in towns and local academic institutions. For instance, the television reporters alleged that a professor at Gotland University College who had criticized the pipeline project had changed his assessment after having been offered, and receiving, a research grant of SEK 5 million from Nord Stream AG in June 2007. The reporters also alleged that politicians on Gotland who had criticized the pipeline had ceased their criticisms when it was decided that Nord Stream AG would renovate the local port town of Slite.[634] In August 2007, months before the consortium even approached the Swedish government with its EIA, the Gotland port town of Slite had accepted that the Nord Stream consortium would use its facilities for logistics during the pipeline project construction, in exchange for the consortium providing approximately SEK 70 million to renovate the harbour.[635] A new quay was eventually constructed, since the old quay was too small, with work starting in December 2008, before the consultation period relating to the amended EIA was over.[636] In total, Gotland benefited from SEK 100 million which was spent on Slite port and various cultural research projects.[637] Slite henceforth became an important logistics site and storage depot for the Nord Stream project, together with the port town of Karlskrona—which in addition to becoming one of the Nord Stream project's two Swedish warehouse terminals also hosted one of Sweden's most important naval bases. But Sweden was not the only country in which local politics, the project's need for logistics, and lobbying activities took place. In Finland, the consortium employed the port of Hanko (which after the Second World War had been the site of a Soviet naval base) as a warehouse terminal and the port of Kotka as a pipe coating yard. In Germany, the

[634] Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009.

[635] Ibid. See also Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 129.

[636] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 121.

[637] Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 121.

port of Sassnitz/Mukran was used both as a warehouse terminal and for pipe coating.[638]

On the national level in Sweden, following Sweden's rejection of the first EIA application in spring 2008, Nord Stream AG, hired Dan Svanell, who had been press secretary to seven Social Democratic ministers, including Leif Pagrotsky who had met Gazprom CEO Miller for discussions on the pipeline project in 2003 and been one of those who initiated the public debate in 2006 (the Social Democratic party had since lost an election), and knew the Swedish government structure well.[639] Then Nord Stream hired Tora Leifland Holmström, a close advisor of Minister of Agriculture Eskil Erlandsson, as communications project manager.[640] Finally, Nord Stream hired former State Secretary Ulrica Schenström, who had been described as the right hand of Prime Minister Fredrik Reinfeldt and reportedly had enjoyed access to classified information about Swedish strategies with regard to the Nord Stream project.[641] With these recruitments, Nord Stream AG successfully hired key people from both the government and the leading opposition party who were well versed in how the Swedish government functioned and, at least in some cases, no doubt had insider knowledge of the government's views on the Nord Stream project.

In addition, Nord Stream AG spent considerable efforts and funds on public hearings in Stockholm and other Swedish cities and the distribution of information on the pipeline project. Between 2006 and 2008 the Nord Stream consortium claimed to have arranged or participated in more than a hundred public meetings and conferences in the countries around the Baltic Sea.[642] As lobbying intensified, this number rose to more than two

[638] Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG.

[639] Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009.

[640] Ibid.; Morén, Kristoffer. In Baltic Worlds 4, 2010, p. 15.

[641] Resumé, 09.07.2008; Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009; Nyhetskanalen (Sweden), 15.02.2009; Dagens Nyheter (Sweden), 15.02.2009.

[642] Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 5.

hundred by late 2009.[643] Of these, a large share took place in Sweden. Nord Stream AG even sponsored a number of academic research projects, including marine archaeology research carried out off Gotland in 2007 and a book in Swedish on sixteenth-century naval warfare written by a Russian journalist.[644] The book described the Northern Seven Years' War (1563-1570), which was chiefly fought between Sweden and Denmark. It was presumably a coincidence that the book described a war between Sweden, the government of which was against the Nord Stream project, and Denmark, which was in favour of it.

Nord Stream AG also employed the renowned British public relations agency Hill and Knowlton to polish the image of the project. Hill and Knowlton described the firm's participation in the following terms: "H+K Strategies' corporate communications and public affairs activities have helped enable Nord Stream maintain open dialogue with regulatory decision-makers and enhance information flow at an international level."[645] In other words, Hill and Knowlton assisted Nord Stream AG with the EIA application process (while Ramsbøll produced the actual EIA). The Hill and Knowlton agency was quite successful, and indeed won several awards in 2009 for its public relations activities on behalf of Nord Stream AG.[646]

5.3.3 Outcome

The first line of the pipeline was eventually constructed according to plan, as adjusted for the delays in the EIA process, with work beginning in 2010 and coming on line on 8 November 2011, at a ceremony attended by French Prime Minister François Fillon, German Chancellor Angela Merkel (who six years earlier had declined to attend the welding of the first joint of

[643] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 71.

[644] Smirnov, Alexej: Det första stora kriget. Stockholm 2009.

[645] Hill and Knowlton web site, <www.hillandknowlton.co.uk>. The web site mentions the firm's successful work for Nord Stream but does not offer access to details with regard to the project.

[646] AMEC Communication Effectiveness Awards. Web site, <http://amecorg.com/wp-content/uploads/2011/08/amec_awards_2010_winners.pdf>.

the pipeline), Dutch Prime Minister Mark Rutte, Russian President Dmitry Medvedev, EU Energy Commissioner Günther Oettinger, and Erwin Sellering, Minister President of Mecklenburg-Western Pomerania. The second line came on line on 8 October 2012, with less pageantry and official representation.[647] Transport capacity would be 55 bcm per year.[648] Yet, no offshore platform was ever built, nor were any military sensors installed, as far as is known.

There is the distinct possibility that the Swedes were right in suspecting the Russian Navy or intelligence services of plans to use the offshore platform for military intelligence collection. As noted, the offshore platform was the only part of the project which Sweden actually could veto, according to the United Nations Convention on the Law of the Sea. Yet on 13 February 2007, before Sweden had even responded to the submitted notification of intent, the Russian Ambassador to Sweden, Alexander Kadakin stated, in a controversial interview on national public radio, that "it is even imaginable that the platform will not be built. It is technically possible to have a pipeline without such a platform, as a worst-case scenario."[649] This was not, at the time, the official position of the Nord Stream consortium, which had made elaborate plans for the offshore platform and claimed that it was really necessary for the viability of the entire project.[650] As late as on 14

[647] Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 76, 133, 141 and 240. By late May 2012, Nord Stream announced plans for a third and fourth line. Ibid., p. 75.

[648] Ibid., p. 284.

[649] Sveriges Radio (Sweden), 13.02.2007. In the same interview, Kadakin concluded that he could not understand "what kind of an idiot" had been able to argue to his superiors that the offshore platform could be used for intelligence collection aimed at Sweden (in Swedish: "Jag fattar inte vad det är för en slags idiot som har kunnat hävda detta i sina rapporter till sina svenska överordnade.") However, even as the Ambassador referred to the project's individual detractors as idiots, he stressed that relations with the Swedish government remained friendly and concluded that there had been no official Swedish criticism aimed at the Nord Stream project, thus maintaining the illusion of smooth and disinterested government-to-government relations.

[650] Dirk von Ameln, Deputy Technical Director, Nord Stream AG: Hearing in Swedish Parliament. Stockholm 12.12.2006, Hearing in Visby 22.01.2007. Noted in Carl B.

September 2007, Nord Stream explained in Stockholm that the platform was an integral part of the pipeline system.[651] Even so, the possibility of building the pipeline without an offshore platform had already been raised by an anonymous source reportedly "close to" the pipeline project in an interview with the Russian newspaper *Vremya Novostey* in August 2006.[652] And in early 2008, Nord Stream AG confirmed that it could build the pipeline without the offshore platform.[653] In other words, Ambassador Kadakin and *Vremya Novostey*'s anonymous source seemed to have access to more information, and at an earlier stage, than the authorized representatives of Nord Stream AG. This indeed fuels suspicions that the offshore platform's primary purpose indeed may have been intelligence collection, but that Russia scrapped these plans when confronted with the Swedish resolve to stop the entire project, if possible, by refusing permission to build the platform. Because for Russia, the export pipeline was the greater good, due to the need to bring in revenues from the export of natural gas to Western Europe. Intelligence collection would no doubt have been an added benefit but was not the primary driver behind the project. The other possible explanation is that the platform all along was regarded as a negotiable concession, which would be a benefit if permitted but was not really necessary for the project.

Further support for the suspicion that there had indeed been Russian plans to use the offshore platform, and likely the entire pipeline, for military intelligence collection came in 2008, after the Nord Stream consortium had already confirmed that no offshore platform would be built. A Russian paper was then published in a scientific journal about the sensor systems to

Hamilton: Naturgasledning på Östersjöns botten: Lägesrapport 23 februari 2007 (Folkpartiet, 23 February 2007), p. 19f.

[651] Nord Stream, The Service Platform: An Intergral *(sic)* Part of a Safe System. Nord Stream Forum. Stockholm, 14.09.2007.

[652] Vremya Novostey 149, 21.08.2006.

[653] Nord Stream, Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008, p. 11. Nord Stream AG produced the document immediately following the 29 January 2008 hearing.

be used to protect the Nord Stream pipeline from terrorism. The article was written jointly by two lieutenant colonels and two scientists and concluded that the pipeline might be under threat not only from terrorists but also from saboteurs from companies and countries opposed to its construction. In response to this threat, the pipeline would be protected by a composite sensor system consisting of surface and underwater components, including sensors mounted on the pipeline itself. Based on the information received from the sensor systems, suitable measures, including the firing of missiles against hostile surface vessels or aircraft, could be initiated in real time to destroy the threat, the authors argued. The paper quaintly referred to the pipeline under its old name NEGP and the accompanying map still included the offshore platform, although the text mainly referred to non-stationary surveillance means such as satellites, unmanned aerial vehicles (UAV), and autonomous underwater vehicles (AUV). It thus gave the distinct impression of being an old paper dusted off and updated for publication despite, to some extent, being out of date. But the affiliation of the writers left little room for doubt. The two scientists were affiliated with the State Research Navigation-Hydrographic Institute (GNINGI), a state institute under the Russian Ministry of Defence, whereas the two military officers were listed as serving officers of military unit number 54023, which elsewhere has been identified as a formation within the Russian military intelligence service Main Intelligence Directorate (GRU) believed to be involved in satellite imagery intelligence collection. The authors ended the paper by suggesting that the several countries with an interest in the pipeline could work together to protect it, by integrating some of their respective surveillance systems.[654]

[654] Katenin, V. A./ Surzhikov, I. M. and Makarov, A. M: Vozmozhnyy oblik sistemy osveshcheniya nadvodnoy i podvodnoy obstanovki v interesakh obespecheniya deystviy antiterroristicheskikh sil i sredstv zashchity podvodnykh truboprovodnykh sistem (Possible Look of a Surveillance and Warning System Aimed for Provision [of] Effective Actions of Anti-terror Forces and Security Protection of Underwater Pipeline Systems). In: Morskaya radioelektronika 24, No. 2, June 2008, p. 12ff. On GNINGI, see its web site, <http://gningi.ru/>. For the identification of military unit number 54023 as the 162nd Military-Technical Center, based on Volokolamskoye Shosse 56/2 in Moscow, a formation within the GRU which engaged in satellite reconnaissance, see commonly available web sites, e.g. http://wikimapia.org

As far as is known, no military sensors were installed in conjunction with the pipeline. Simply by advertising its concern widely and vociferously, Sweden ensured that it would be difficult for the Russian side to use the pipeline for military intelligence purposes. The Policy Memorandum exposed by Swedish national television made it abundantly clear that even if the Swedish government eventually accepted the EIA and gave the necessary permits to build the pipeline, then this permit would only cover the commercial activities of the consortium, never any intelligence use of the infrastructure by state actors.[655] The condition that would adhere to the eventual permit was duly noted by the Nord Stream consortium, and when Nord Stream AG arranged a public hearing in Stockholm on 29 November 2006, about four months after the document was written (but about a week before it was leaked to the press, posing questions on whether the Russian side had already learnt of the Swedish assessment), its materials included an addendum which acknowledged that the permit would only apply to natural gas deliveries, and that any "incorrect usage" might result in a halt in the pipeline's operation.[656] The addendum was duly noted by the Swedish side.[657] It is for this reason that Russia, faced with Swedish opposition and known determination to treat any installation of military sensors as grounds for refusing the project, would be unlikely to take the risk of installing any such sensors later. If military sensors were eventually discovered in conjunction with the pipeline, Sweden could retroactively recall its permit. One could of course argue that if the Russians really wanted to install military sensors, they might be able to install the appropriate sensors anyway, by clandestine means after the pipeline was put in operation. However, since the primary purpose of the project was always to guarantee the export of natural gas, the risk of installing such sensors for the secondary purpose of military intelligence collection would no doubt be assessed as too great.

; <http://agenturaforum.com>; <www.evasiljeva.ru/2014/04/blog-post_30.html>. This identification is supported by official tenders for satellite equipment, as published in the Russian government web site, <www.zakupki.gov.ru>.

[655] Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), 08.08.2006.

[656] Nord Stream: Säker gasförsörjning för Europa. Presentation, 29-30.11.2006.

[657] Larsson, Robert: Nord Stream presentation . FOI Memo 1905, 30.11.2006.

Besides, in a real crisis, such sensors would be of little use – since the pipeline had a known, fixed location and despite the assurances of the two GRU officers would be easy to breach, if this was ever deemed necessary, thus at the same time destroying the integrity of the sensor chain. Needless to say, this would also halt any natural gas exports, which would affect Russia more than its Western customers who were not fully dependent on Russian supplies.

The Russian side thus attained its primary objective of building natural gas export infrastructure which bypassed the transit countries. However, when the necessary permits to build the Nord Stream pipeline were finally granted, in November 2009, the world was suffering from a global financial crisis.

The 2003 energy strategy had been afflicted with several problems. In addition to alarming consumer and transit countries, it also consisted of detailed objectives that, in some cases, soon no longer corresponded to market realities. In late 2006, Russia accordingly commenced work on an updated energy strategy.[658] The new Russian energy strategy was approved in late 2009, eight days after Sweden's approval of the Nord Stream project.[659] The new strategy was in many ways a response to the then ongoing financial crisis. Gone were the phrases that suggested military strategy. Instead the new strategy repeatedly emphasized the need to create a favourable economic environment.[660] Of the statements in the 2003 strategy that the energy factor would be a fundamental element within Russian diplomacy, nothing remained but the hardly unusual, in international commerce, conclusion that the strategic objective of the foreign energy policy was the Russian energy sector's full-scale integration into the world energy market,

[658] Ministry of Industry and Energy: On a refinement of the Energy Strategy of Russia for the period up to 2020 and its prolongation up to 2030. Decree of the Ministry of Industry and Energy No. 413, 21.12.2006.

[659] Government of the Russian Federation: Energeticheskaya strategiya Rossii na period do 2030 goda ("Energy Strategy of Russia to the Year 2030"), Government of the Russian Federation Decree No. 1715-r, 13.11.2009.

[660] See, e.g. Government of the Russian Federation: Energeticheskaya strategiya Rossii na period do 2030 goda ("Energy Strategy of Russia to the Year 2030"), Government of the Russian Federation Decree No. 1715-r, 13.11.2009, p. 16, 18 and 19.

the enhancement of its positions thereon, and gaining the highest possible profit for the national economy.[661] The leading Russian energy companies would receive diplomatic support abroad.[662] Russia had national interests in the operation of the global energy market, but in the roadmap of state policy measures attached to the strategy there were no alarming statements beyond that of promoting Russian energy companies abroad and offering them "information, political, and economic support."[663] In fact, the energy strategy candidly admitted problems in Russia's foreign energy policy, including the financial crisis but also the continuing export dependence on transit countries and the politicization in the energy relationships between Russia and foreign countries.[664] And politicization was indeed what had characterized the struggle to build the Nord Stream pipeline.

5.3.4 Concluding Remarks

The Nord Stream pipeline was successfully completed as a commercial project, but Sweden made certain that no offshore platform was built and worked to ensure that no military sensors were installed. The Swedish opposition and strong resolution with regard to the minutiae of the EIA may also have pushed the consortium into taking the environmental aspects very seriously, something for which Nord Stream AG eventually received considerable and deserved recognition. In effect, both sides achieved some of their goals. Russia succeeded in building a natural gas export pipeline with direct access to Germany, thus bypassing those transit states with which Russia had frequently encountered political problems. Sweden, as far as is known, prevented Russia from laying an underwater sensor chain across the Baltic Sea and obstructed the project by legalistic means to the extent that Russia would find it difficult to justify an increased naval presence in the Swedish exclusive economic zone based on the existence of the pipeline alone (although there was, as before, nothing to prevent a naval presence as such). Sweden did not succeed in its lofty but futile attempt

[661] Ibid., p. 34.
[662] Ibid., p. 35, app. 5, p. 23f.
[663] Ibid., p. 89, app. 5, p. 18ff.
[664] Ibid., p. 35.

to save the EU from importing more Russian natural gas, nor save the Baltic Sea from the environmental impact of the pipeline, if there was one (an issue to which everybody had paid lip service but which was quickly forgotten by the media and the public after construction began).

The Nord Stream consortium claimed that Sweden's obstruction cost more than EUR 100 million in expenses related to the EIA process and associated lobbying activities, not counting almost two years of added time spent on the EIA process.[665] These costs would initially have to be borne by the corporations which owned Nord Stream AG but in the end were likely to be recouped from the European consumers. Sweden devoted considerable resources to monitoring and delaying the pipeline project, but these costs were taken from the regular operational funds of the government ministries and agencies involved, which ultimately came from the Swedish taxpayers. In return, the taxpayers and European consumers could enjoy the media show of the Nord Stream controversy, which ran for several years and provided entertainment to all and lucrative careers to some.

There was certainly a Swedish *long-term strategy*, on political and environmental grounds, to oppose further imports of Russian natural gas. When faced with the perceived threat of the pipeline as a sensor platform for Russian military intelligence, the long-term strategy hardened into an *intention* to oppose the pipeline project. Did this also lead to a Swedish *master plan* on how to thwart the project? If so, it was the one formulated by the inter-ministerial working group set up in 2006. The actual details – the *operations plan* – were then worked out in the winter of 2006/2007, coordinated by the Ministry of Defence. However, because of the decentralized administrative system there was probably never any formal operations plan, only a general agreement on what could be done to oppose the pipeline project by the respective actors which then *executed* the informal plan independently.

[665] Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6. In fact, this was the total cost of the environmental studies, route surveys, and technical planning and many of these would in any case have been necessary for the project. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 43, 58 and 72.

The Russian *long-term strategy* was the one formulated by President Putin over a series of years, and this resulted in an *intention* to bypass the transit countries so as to avoid further political difficulties with Russia's energy exports. This led to the *master plan* which can be said to the one presented in the 2003 energy strategy, in conjunction with the presumably secret plans of the Navy and GRU to use the pipeline as a sensor platform. The Russian side seems not to have anticipated the Swedish counterstrategy against the pipeline plan. The Russian side only developed a counter-counterstrategy, an *operations plan*, in early 2007, having then realized the scale of Swedish opposition. The *execution* phase of the operations plan began with full force only from 2008, after the Swedish government had rejected the original EIA.

The conclusions presented here would likely be disputed by both the Swedish and Russian governments. The Swedish government never officially voiced its concerns over the military intelligence collection opportunities for Russia perceived to exist in the pipeline project, nor did the Russian government ever mention an intention to use the pipeline in this way. Instead the struggle was relegated to low-level civil servants, military officers, retired officials, newspaper editors, lobbyists, and businessmen, whose activities, if necessary, could be disregarded as not representative of the formal stance of their respective governments. As in the work of the intelligence services, deniability was the key. Neither government was prepared to shatter the illusion that official relations remained smooth and without mutual suspicions with regard to intentions. Minister of the Environment Carlgren approved the project by referring to international law and concluded that the environmental provisions had been satisfied. The outspoken Ambassador Kadakin referred to the project's opponents as idiots but stressed that relations with the Swedish government remained friendly and concluded that there had been no official Swedish criticism aimed at the Nord Stream project. Such comments were unsurprising. Nor would the two governments acknowledge that their respective intelligence services might be in the process of collecting information on each other. For a state, a hybrid power projection must in its essentials remain covert. There may be overt aspects, such as through the use of diplomatic power and commercial entities, but its targeted, multi-dimensional, and coordinated features may not be acknowledged, or the hybrid power projection becomes an open act of aggression, which might escalate existing rivalry into open confrontation.

5.4 The Hybrid Threat Capability of the Afghan Taliban Movement, 2001-2014

Michael Fredholm

When the Afghan Taliban leaders withdrew into Pakistan in late 2001, they had no intention of surrendering the struggle against the U.S.-led international coalition which had forced them out of Afghanistan. Yet, with a substantial international military presence firmly entrenched in Afghanistan, there was no way that the Taliban could regain power by conventional military means. Even with Pakistani military support, the Afghan Taliban movement could not have repeated the 1994 invasion of Afghanistan in the face of such military opposition.

For this reason, soon after its forced withdrawal into Pakistan, the Afghan Taliban began to employ the means and methods of hybrid warfare and hybrid threats, in this work defined as *"a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests."*[666] This was a result of strategy debates within the Taliban top leadership, likely with the support of political agents and military advisors from the Pakistani Inter-services Intelligence agency (ISI). Pakistan had long considered influence in Afghanistan a vital component of national security policy and was reluctant to surrender its influence. The policy is generally regarded as having originated from two perceived strategic needs: (1) to allow Pakistan the use of Afghanistan's territory for strategic depth in a conventional war against India; and (2) to ensure friendly Pashtun hegemony in Afghanistan so that ethnic Pashtuns on either side of the Pakistan-Afghanistan border would drop any

[666] As defined by the National Defence Academy (Landesverteidungsakademie), Vienna: "Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen."

plans to unite in a single Pashtun nation, and thereby compromise Pakistani territorial integrity.[667] Pakistani specialists were certainly dispatched into Afghanistan when the Taliban movement aimed to establish a new front, or when combat conditions were particularly difficult. It is likely but not conclusively proven that Pakistan modelled its support to the Taliban on that provided to favoured Afghan insurgent leaders within the mujahidin front in the 1979-1989 Soviet war in Afghanistan.[668] Even so, there is little doubt that it was the Afghan Taliban leaders, not their Pakistani advisors, who formulated policy, including hybrid warfare and hybrid threats.

The hybrid threat capability developed by the Afghan Taliban (here defined as the Afghan Taliban movement with affiliates, excluding allied but independent international terrorist groups such as Al-Qaida and foreign terrorist groups such as the Pakistani Taliban) included various tactics and strategies to be employed at home and abroad. From 2002 onwards, the Afghan Taliban movement developed a considerable capability for hybrid threat projection. Being at war, in Afghanistan the Taliban movement, unsurprisingly, engaged in hybrid warfare. Abroad, the movement utilized its capacity for hybrid threats. For this reason, the domestic threat in Afghanistan deriving from the Taliban and the international threat of the movement were quite different in character.

While the Afghan Taliban movement had no expressed policy on the concept of hybrid warfare or hybrid threats as such, the movement was obviously aware of the means and potential of the concept. So were, for instance, the entire first two sections of the Taliban *Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan* primarily focused on the effect that the means of intimidation would have to compel the population into joining the Taliban, and how ordinary people and collaborators should then be

[667] See, e.g. Fredholm, Michael: Afghanistan and Central Asian Security. Asian Cultures and Modernity Research Report 1, Stockholm University March 2002, p. 16.

[668] Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 242ff, on p. 246, 256 and 259.

treated.[669] In addition, the *Code of Conduct* emphasized that all who worked for the Taliban Islamic Emirate must strive to force those who supported the infidels to acknowledge and surrender to the Taliban.[670] It was clear from the *Code* that this encompassed threats and propaganda as well as fighting. The *Code* stressed the need to win the hearts and minds of the population. Article 78 translates as "The mujahidin are duty-bound to show good character and Islamic behaviour to the nation. They should win the hearts of Muslims at large."[671] The Taliban *Code* mirrored the counterinsurgency strategies adopted by Western countries in these respects, in their emphasis on winning the hearts and minds of the contested population.[672] In this regard, there was no great difference between Western and Taliban views on warfare. Nor was there such a difference in the view on new tactics and technologies. The Taliban movement, in similarity to other military organizations, displayed a learning curve, in which new methods, tactics, and technologies were adopted to stay abreast of developments.[673]

In fact, the hybrid threat capability of the Afghan Taliban movement soon grew to encompass several distinct types of powers, in both domestic and international dimensions. Many of these powers were exercised from Af-

[669] Sections 1 and 2, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010 (Taliban Voice of Jihad Online in Pashto, 09.08.2010). The second edition included 14 sections and 85 articles. The first edition, which used very similar language, was published in the first half of 2009 and included 13 sections and 67 articles. The first edition in turn replaced the *Book of Rules for the Mujahidin*, first published in the holy month of Ramadan 2006.

[670] Article 77, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010.

[671] Article 78, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010. This article was also in the 2009 edition. However, it was not in the original 2006 Book of Rules.

[672] See, e.g. the emphasis on statements such as "The decisive terrain is the human terrain" and "The people are the center of gravity". In: Petraeus, David H.: Counterinsurgency Guidance. 01.08.2010, COMISAF/CDR USFOR-A.

[673] Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 242ff, passim. The learning curve was also evident in the aforementioned updated and improved editions of the *Book of Rules* and *Code of Conduct*.

ghanistan, but particularly those with an international dimension more often geographically originated in Pakistan, where the Taliban leadership enjoyed safe havens. The full hybrid warfare and hybrid threat capability of the Taliban is summarized in Table 8.

Domestic Threat						
Type of Threat	Target	Means and Method	Purpose	Geographic Origin	Effect	Defensive Actors
Military Power	ISAF/ ANSF	Guerrilla attacks, IEDs	Defeat or intimidate enemy	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Terror Power	ISAF/ ANSF	E.g. suicide bombers	Intimidate enemy	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Terror Power	Population	E.g. killings, mutilations	Intimidate population	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Media Power	Population	E.g. night letters, proclamations, videos	Propaganda	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Organized Crime Power	ISAF/ ANSF	Support to bandit gangs	Cause disruption	Afghanistan/ Pakistan	Medium	Armed forces, police, intelligence

International Threat						
Type of Threat	Target	Means and Method	Purpose	Geographic Origin	Effect	Defensive Actors
Diplomatic Power	ISAF member states	Negotiations	Negotiate withdrawal	Pakistan	Medium	Foreign Ministry, International organizations
Diplomatic Power	Worldwide Muslim community	Negotiations	Appear as responsible party	Pakistan	Medium	Foreign Ministry, International organizations
Media Power	ISAF member states, worldwide Muslim community	*Afghanistan In Fight*, Internet, Twitter	Propaganda	Pakistan	Low/ medium	Media houses, government institutions, think tanks, NGOs
Terror Power	ISAF soldiers' family members	Threats by telephone or SMS	Intimidate individual to resign	Afghanistan, ISAF member state	Low/ medium	Security service, Intelligence service, police
Terror Power	Attacks	Not used	Intimidate enemy to withdraw	Pakistan	None	Security service, Intelligence service, police

Table 8: Afghan Taliban Movement Hybrid Threat
Michael Fredholm

5.4.1 Background

The Taliban Movement in the 1990s

To assess the Afghan Taliban movement's capability for hybrid warfare and hybrid threats, it helps to first explain the origins of the movement. The Afghan Taliban movement emerged as a military force in 1994, when it was created, in all essentials, by and for Pakistani interests even though few, if any, Taliban leaders subsequently were much concerned about following Pakistani orders.[674] The movement's leaders at the time regarded themselves as the world's perhaps only true Islamic government, on the lines of the righteous caliphate of the early years of Islam.[675] The Taliban government accordingly styled itself the Islamic Emirate of Afghanistan.[676]

The Taliban were reinforced by large numbers of Pakistanis, religious volunteers as well as regular Pakistani military units. Indeed, the very first Taliban incursion into Afghanistan in 1994 was reportedly supported by Pakistani army artillery fire and motor transportation from the Pakistani side of the border.[677] The volunteers, who were first reported by the Pakistani press in mid-June 1997,[678] were initially mostly Pashtuns of Afghan or Pakistani origin but from 1999, Pakistani Punjabis arrived in increasing numbers and eventually formed the majority of the Pakistani volunteers.[679]

[674] Rashid, Ahmed: Taliban. Islam, Oil and the New Great Game in Central Asia. London 2000, p. 26ff and 125; Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 71 and 82.

[675] Gohari, M. J.: The Taliban. Ascent to Power. Oxford 1999, p. 118.

[676] Taliban web sites: <www.taleban.com>; <www.afghan-ie.com> (both now defunct).

[677] Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 45f and 49f.

[678] Ibid., 12 and 25.

[679] Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan. 30.08.2000; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 22ff, in particular on 100; Davis, Anthony: Struggle for Recognition. In: Jane's Defence Weekly, 04.10.2000, p. 21; Davis, Anthony: Foreign Fighters Step Up Activity in Afghan Civil War. In: Jane's Intelligence Review 13: 8 (August 2001), p. 14ff.

The Pakistani military played a considerable role in the military success of the Taliban. Senior Pakistani intelligence and army officers were involved in strategic planning. Regular Pakistani soldiers served as units in combat roles, or were detached from their units for the provision of special skills such as those of tank drivers and aircraft pilots, in technical and rear support, maintenance, and administrative functions. Pakistani aircraft assisted with troop rotations for Taliban forces during combat operations in late 2000. Pakistani military officers from the ISI as well as commandos from Pakistan's Special Services Group (SSG, a special forces regiment based near Peshawar) also appeared to take considerable responsibility for the planning and execution of major operations. This was shown by the impressive use of mobility, speed, logistics support, as well as efficient contemporary command, control, communications, and intelligence procedures displayed by the Taliban, on a level hitherto never seen among Afghan troops and certainly not to be expected from such a comparatively new military formation, even considering the fact that the Taliban also recruited numerous officers and men of the pre-1992 Afghan army, many from the hard-line, Pashtun nationalist Khalq ("Masses" or "People") wing of the Communist Party.[680] Pakistan-based Western diplomats knew that the ISI was instrumental in forming and supporting the Afghan Taliban movement.[681] However, following the 11 September 2001 terrorist attacks, this was seldom mentioned so as not to embarrass Pakistan and cause further tensions in an already dangerous domestic political environment.

[680] Davis, Anthony: How the Taliban Became a Military Force. In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, in particular on 68ff; Saikal, Amin: The Rabbani Government. 1992-1996; In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 29ff, on 39; Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000; Davis, Anthony: Struggle for Recognition. In: Jane's Defence Weekly, 04.10.2000, p. 21; Davis, Anthony: Foreign Fighters Step Up Activity in Afghan Civil War. In: Jane's Intelligence Review 13: 8 (August 2001), p. 14ff; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 49; Rashid, Ahmed: Jihad: The Rise of Militant Islam in Central Asia. New Haven 2002, p. 174; Human Rights Watch (HRW): Fueling Afghanistan's War. HRW Press Backgrounder, 2001.

[681] Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 45f, 49 and 91.

Weapons being abundant in Afghanistan, the Taliban did not really have a supply problem with regard to personal weapons. Fuel, heavy weapons, and ammunition were another matter. The Taliban depended on Pakistan for delivery of ammunition, particularly for tanks and artillery, some small arms, pick-up trucks, and petroleum (both motor and aviation fuel), oil, and lubricants. They also received financial payments. A significant share of the Taliban procurement of arms, munitions, and spare parts was handled by Pakistani private companies, often run by retired military officers. They bought considerable quantities from Chinese manufacturers through dealers in Hong Kong and Dubai (United Arab Emirates). The supplies were usually shipped in sealed containers to the Pakistani port of Karachi, whence they were trucked to Afghanistan without normal customs inspection, since this was not required by the two countries' trade agreement, the Afghan Transit Trade Agreement (ATTA).[682] Some were probably paid for through financial assistance to the Taliban from private or state supporters in the Arabian Peninsula through the use of Islamic charities such as the Al-Rashid Trust, which has since been accused of smuggling weapons and supplies, disguised as humanitarian aid, to the Taliban.[683] The Taliban were funded partly from contributions from supporters abroad, typically on the Arabian Peninsula, partly from taxes, in particular deriving from narcotics production in Afghanistan.[684] It was not unknown for Taliban leaders to

[682] Support from Pakistan: Human Rights Watch (HRW): Fueling Afghanistan's War. HRW Press Backgrounder, 2001; Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 28.05.1999; 30.08.2000; 17.10.2000; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 44f, 72 and 183f; Rashid, Ahmed: Heart of Darkness. In: Far Eastern Economic Review, 05.08.1999, p.8ff; Magnus, Ralph H./Naby, Eden: Afghanistan: Mullah, Marx, and Mujahid. Boulder, Colorado 1998, p. 190; Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 69.

[683] The New York Times (USA), 25.09.2001.

[684] Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 35, 120 and 123f; Rashid, Ahmed: Heart of Darkness. In: Far Eastern Economic Review, 05.08.1999, p. 8ff. The Taliban in mid-2000 banned the cultivation of opium poppy. Some Western drug law enforcement officials claimed that this was merely a public-relations exercise, and that drugs were instead stockpiled in order to push up the price. Because of the 2001 downfall of the Taliban, we may never know their ultimate intentions. The Taliban certainly made substantial profits from the

maintain foreign bank accounts. For instance, Taliban supreme leader Mullah Muhammad Omar had accounts in the Laskari Bank in Islamabad and the National Westminster Bank in Britain. Both were allegedly opened for him by the ISI.[685] Many Pakistanis too profited from business connections with the Taliban. Taliban leaders soon developed relations with a number of Pakistani businessmen close to Asif Ali Zardari, the husband of Benazir Bhutto, Pakistan's prime minister 1993-1996, who in turn were given highly lucrative permits for fuel deliveries from Pakistan to the Taliban. Pakistan also assisted in the development of necessary infrastructure in Taliban-controlled Afghanistan. Pakistan Telecom, for example, set up a microwave telephone network in Kandahar. This became part of the Pakistani telephone grid. Kandahar received the same prefix (081) as that for Quetta, so Kandahar could be called from Pakistan as a local call.[686]

In the early years of the movement, the Taliban received considerable material and financial support also from Saudi Arabia. By then, every major Taliban offensive seemed to be preceded by a visit from Prince Turki ibn Faisal al-Saud, head of the Saudi General Intelligence Agency (*al-Istakhbarah al-Amah;* or simply *Istakhbarat*), and his staff. Earlier, Prince Turki also

narcotics trade *before* they outlawed it. See, for instance, Far Eastern Economic Review (Hongkong), 28.12.2001. They also reportedly sold large quantities of the stockpiled drugs after the 11.09.2001 terrorist attacks on the United States in order to finance the expected war. Jacquard, Roland: Les archives secrètes d'Al-Qaida. Révélations sur les héritiers de Ben Laden. Paris 2002, p. 62 n.4. According to Vladimir Fenopetov, Chief, Europe and West/Central Asia, UN Office on Drugs and Crime, the Taliban ban of opium production, which came into force in 2001, was merely a ruse to (1) make full use of an existing overproduction, and (2) increase the price of opium. Trafficking out of Afghanistan, according to United Nations statistics, in fact remained constant. Vladimir Fenopetov, "Eurasia's Narcotics Situation", conference on 'New' Security Threats in Eurasia: Implications for the Euro-Atlantic Space. Central Asia-Caucasus Institute/Silk Road Studies Program, Stockholm, 20.05.2005.

[685] Jacquard, Roland: Les archives secrètes d'Al-Qaida. Révélations sur les héritiers de Ben Laden. Paris 2002, p. 24.

[686] Rashid, Ahmed: Pakistan and the Taliban. In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 72ff, on 84f.

played a major role in organizing the mujahidin front against the Soviets during the 1979-1989 war.[687]

The Taliban military chain of command was vague and ill-defined at the time. The top decision-making body was the Rahbari Shura (Leadership Council, often referred to as the Supreme Shura) in Kandahar, headed by Mullah Omar. There were also other, lower shuras that reported to the Kandahar Leadership Council, such as the Kabul Shura and the Military Shura or Military Commission. The Kabul Shura was fundamentally a cabinet of acting ministers in Kabul. They primarily dealt with day-to-day problems and local military and political activities, since all important decisions were taken in Kandahar. The Military Commission, another loose body of senior Taliban officials, was technically in authority of military affairs. However, Mullah Omar remained head of the Taliban armed forces, and the Military Commission accordingly seemed to limit itself to planning strategy and in some cases the implementation of tactical decisions. It had no strategic decision-making powers, and all decisions on military strategy, appointments of key commanders, and the allocation of funds were taken by Mullah Omar. Under Mullah Omar, there was a chief of the general staff and chiefs of staff for the army and air force, supposedly in command of ground operations and air operations, respectively.[688] Military operations were supposed to be directed by the minister of defence or the military chief of staff. However, it seems that ground operations remained in the hands of various local task force commanders, several of whom were also

[687] On 19.09.1998, the uncompromising Taliban leader Mullah Omar insulted Prince Turki and the Saudi royal family. Saudi Arabia then ceased its support for the Taliban, although the diplomatic recognition pushed through by Pakistan in May 1997 was not withdrawn. Perhaps significantly, from October 1998 the Taliban, who previously had generally been able to seize the initiative in any military offensive, began to lose ground to a Northern Alliance offensive that managed to maintain its momentum until the summer of 1999. Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 48, 72, 131, 138f, 201f, 227ff and 264 n.16.

[688] Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 95ff and 220f.

members of the Taliban government.[689] The Taliban ran an intelligence service, the *Istakhbarat* (named after, and no doubt at first assisted by, Saudi intelligence).[690]

Due to its foreign support, the early Taliban movement operated more as a conventional although semi-irregular military force than as an actor in hybrid warfare. For all its harsh policies, the Taliban movement never engaged in terrorist activities against neighbouring states.[691] However, at times during its offensives, the movement did indulge in what can only be called terrorist activities aimed at its Afghan enemies. Examples include the torture, castration, and killing of former President Sayyid Muhammad Najibullah in 1996, followed by the public display of his corpse, and the massacres of an estimated six to eight thousand civilians in Mazar-e Sharif, Maimana, and Shiberghan in 1998. These acts of terrorism were ordered by the Taliban leadership, and can be interpreted as an active strategy of intimidation directed against the Afghan population.[692]

The Taliban forces varied widely in training and experience. Some had considerable military experience, and many men had received military training in Pakistan, around Kabul, or in other quiet areas of Afghanistan. Others, however, especially some of the recent recruits from Pakistan, had received virtually no training and were frequently trucked straight to the front to take part in combat operations.[693] Most Taliban soldiers received regular salaries. Among those who did were the professional soldiers from the former communist armed forces, serving in the capacity of gunners, tank drivers, mechanics, and aircraft pilots. Although the majority of the

[689] Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000.

[690] Burke, Jason: Lies, Payoffs, Traps Are Allies' Weapons. Observer (UK), as included in Japan Times, 10.11.2001.

[691] Afghanistan was not on the United States list of states sponsoring terrorism, since the United States did not recognize the Taliban government.

[692] Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 49f and 73f.

[693] Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000.

professionals were Pashtuns, they were seldom as religiously motivated as other Taliban soldiers, particularly the volunteers from Pakistan.[694]

This description of the first years of the Afghan Taliban movement shows that far from being a tribal army, the early Taliban leaders and in particular their Pakistani supporters were often reasonably sophisticated fighting men, aware of the practicalities of both conventional and irregular warfare. While their military capabilities in the 1990s should not be exaggerated, the Taliban understanding of tactics and strategy was not much inferior to that of their neighbours, something which is easily forgotten in light of the speed in which their state collapsed in the face of the Afghan Northern Alliance campaign on the ground supported by American-led air support in late 2001.[695]

The Post-2001 Taliban Movement

With the invasion of U.S.-led forces in October 2001, the Taliban movement retreated into Pakistan. Following the withdrawal, it took some time before the Taliban movement fully reorganized and reconstituted itself as a military force. Due to the large and resilient support system the Taliban had acquired during its rule prior to 2001, the Taliban remained the largest threat to stability in Afghanistan.[696] This was facilitated by the fact that until 2005, the Taliban were not under serious military pressure.[697] In Pakistan, the Taliban movement continued to receive substantial support from Pakistani sources.[698]

[694] Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 100.

[695] Hammer, Carl: Tide of Terror. America, Islamic Extremism, and the War on Terror. Boulder, Colorado 2003, p. 223ff.

[696] National Counterterrorism Center (NCTC): Afghan Taliban. NCTC web site, <www.nctc.gov>, 2013.

[697] Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 244.

[698] See, e.g. Fredholm, Michael: The Need for New Policies in Afghanistan: A European's Perspective. Himalayan and Central Asian Studies 15: 1-2 (2011), p. 54ff, on 67. In

From the viewpoint of the international coalition, the conflict in Afghanistan can be summarized as having consisted of four phases. In 2001-2005, the international forces followed the Light Footprint approach, which resulted in modest and insufficient foreign military and financial aid to the government of Afghanistan. The U.S.-led coalition was from 2003 onwards also distracted by the Iraq War. In the years 2005-2009, a Taliban resurgence took place, largely as a result of the Light Footprint of previous years and the existence of Taliban sanctuaries in Pakistan. By then, foreign aid was increasingly used as a tool for short-term stabilization in response to Taliban activity, instead of for much-needed long-term developments. The years 2009-2011 saw a U.S. military and civilian surge, accompanied by a substantial increase in aid. Unfortunately, the surge did not succeed in uprooting the Taliban insurgency. The years 2011-2014, finally, were characterized by the concept of transition intended to accomplish Afghan assumption of full sovereignty. Paradoxically, transition and full sovereignty were accompanied by almost complete foreign aid dependency, since insufficient long-term developments had taken place to ensure Afghanistan's economic future.

It follows from this that the Taliban movement was granted several quiet years in which to grow in strength, without being under serious military pressure anywhere. Yet the movement was an exile organization, without the benefits of being in control anywhere outside its Pakistani sanctuaries. Consequently, the Taliban movement came to fragment into several semi-autonomous organizations, nominally united under Mullah Omar and what became known as his Quetta Shura, so named since it was for many years based in the Pakistani city of Quetta.

time, the Taliban also began to receive some support from Iran. In 2010, at least three meetings between Iranian Islamic Revolutionary Guards Corps (IRGC, *Pasdaran-e Enghelab-e Islami*) officers and Taliban leaders took place. The Iranians reportedly had considerable success in offering patronage to individual Taliban commander Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 247, 257.

The Taliban was never a homogeneous movement, not even in the 1990s, and the divisions remained and to some extent deepened in exile. Mullah Omar and the Quetta Shura had one agenda, which the affiliated and allied groups only shared in part, since they had agendas of their own. In addition, even the Quetta Shura was a decentralized organization and in most cases consisted of loose units independent of each other, even though they all claimed allegiance to Mullah Omar. In fact, the Quetta Shura itself fragmented. In 2012, a power struggle emerged within the Shura, and internal rivalries sharpened in 2013.[699] By mid-2013, Mullah Omar remained the nominal head of the movement, although its members sometimes believed that he was held captive in Pakistan, or even that he was dead (he was not, as it turned out).[700] The Taliban movement was then widely regarded by its own members as having become divided into several largely autonomous alliances. These were the original Leadership Council in Quetta,[701] Abdul Qayyum Zakir's alliance within the Quetta Shura,[702] Akhtar Mansur's alliance within the Quetta Shura,[703] the Peshawar Shura,[704] and the Miram

[699] Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013; Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 6.

[700] Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013; Ron Moreau: Taliban Forces Desperate to Hear from Their Absent Leader, Mullah Omar. Daily Beast, 01.05.2013. < http://www.thedailybeast.com/articles/2013/05/01/taliban-forces-desperate-to-hear-from-their-absent-leader-mullah-omar.html>.

[701] The Leadership Council (Rahbari Shura) in Quetta was the main decision-making body of the Taliban and accordingly included several old Taliban leaders. Although of diminishing importance because of a decline in revenue and power, as a collective force the Rahbari Shura still enjoyed a certain amount of prestige within the movement.

[702] Abdul Qayyum Zakir's alliance within the Quetta Shura was based on Zakir's personal network but also included those of several other Taliban leaders. Zakir, a former Guantanamo detainee transferred to Afghan custody who following his 2007 release by Hamid Karzai's government returned to the insurgency and in 2009 was appointed head of the Quetta Military Commission, was supported by both the Pakistani government and the Peshawar Shura, thus enjoying his own sources of revenue. See, e.g. Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 17.

[703] Akhtar Mansur's alliance within the Quetta Shura was based on Mansur's personal network, funded from sources inside Afghanistan and among the Afghan Diaspora,

Shah Shura, also known as the Haqqani Network.[705] However, by April 2014 some of the tensions and divisions were resolved with the removal of Abdul Qayyum Zakir from the Military Commission, ostensibly owing to illness.[706]

Nominally, the organization known among Western analysts as the Haqqani Network but in Afghanistan more often referred to as the Miram Shah Shura formed a part of the Peshawar Shura. However, being the most formidable of the various alliances within the Taliban movement, this was a fundamentally autonomous wing of the Afghan Taliban movement based in Miram Shah in Pakistan and named after its leader, Jalaluddin Haqqani.[707] The Haqqani Network was a distinct military and political organization created by Jalaluddin Haqqani during the 1980s which, after the war against the Soviet Union, remained a source of power in the borderlands shared by Afghanistan and Pakistan. The Haqqani leaders were experienced; having survived three decades of warfare, educated in theology,

and also included the powerful Baradar and Dadullah networks (the latter revived in 2010-2011 after a period of disorder due to the death of its founder; Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013, p. 3) in common opposition to Abdul Qayyum Zakir. As head of the Quetta Political Commission, Mansur had considerable political influence.

[704] The Peshawar Shura, which itself consisted of several smaller networks, some of which were of Pakistani jihadist origin, was reportedly more state- and university-educated than clerical as well as directly supported, and thus under a certain level of control, by the Pakistani government. See, e.g. Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013, p. 2; Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 17.

[705] Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

[706] Voice of Jihad: Statement dated 25.04.2014.

[707] Gopal, Anand/Mahsud, Mansur Khan and Fishman, Brian: The Battle for Pakistan. Militancy and Conflict in North Waziristan. Washington, DC 2010; Peters, Gretchen: Crime and Insurgency in the Tribal Areas of Afghanistan and Pakistan. Harmony Program, Combating Terrorism Center, West Point 2010; Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

and with a sophisticated understanding of international trade and politics. Their patriarch, Jalaluddin Haqqani, had earned the name Haqqani as an honorific title as a result of his studies at the prestigious Dar ul-Ulum Haqqaniyyah *madrasah*. He spoke excellent Arabic, as did his son Sirajuddin, and both had first-rate connections in the Arab world. The Haqqanis could discuss the intricacies of Islamic theology in the language of the Prophet, and kept a low profile by avoiding Western journalists, thereby also avoiding the taint of international terrorism for decades, despite close links to Al-Qaida.[708]

Affiliated to the Taliban movement but even older than the Haqqani Network was the Hezb-e Islami of Gulbuddin Hekmatyar (HIG), popularly named for its leader Gulbuddin Hekmatyar, a former Afghan warlord and prime minister and one time ally of the United States. Originally a political party in the 1980s involved in the war against the Soviet Union, the HIG had political allies in the Afghan parliament, may have supported its own candidate in the 2014 presidential election (possibly Qutbuddin Hilal who once served under Hekmatyar[709]), and was perhaps the most politically sophisticated and well-established Afghan insurgent group. Most Hezb-e Islami members were then detribalized Pashtuns from the state-educated state intelligentsia. The leaders were primarily intellectual Islamists from an urban background, so the party lacked a firm tribal base. This was in fact an advantage, as the party tended to recruit where tribal structures had broken down, which made it highly popular in Pakistani refugee camps. The party, radical Islamist in world view, was regarded as the best organized and most disciplined party within the anti-Soviet resistance. However, Hekmatyar's organisation collapsed as Pakistani funds from 1994 were diverted from it to the newly created Taliban movement. Reportedly with thousands of sympathisers and fighters, HIG had strong relations with Al-Qaida and was closely linked with the Afghan Taliban. Hekmatyar and his followers were

[708] Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

[709] Institute for War and Peace Reporting, 27.03.2014.

believed to have remained operating chiefly in Kunar Province, Afghanistan.[710]

Then there were several similarly autonomous groups of foreign fighters, including the remnants of the Al-Qaida core as well as groups such as the Uzbek-led Islamic Movement of Uzbekistan (IMU) and the Pakistani, ethnically Pashtun terrorist group, the Tehrik-e-Taliban Pakistan (TTP, "Movement of Pakistani Taliban"). All these groups enjoyed bases and sanctuaries in Pakistan.

It was never known how many insurgents operated in Afghanistan. Besides, many were, at any given moment, based on the Pakistani side of the border. A common estimate was up to 25.000 Quetta Shura Taliban fighters, in addition to about 3.000 Haqqani fighters and 1.000 HIG fighters. As for Al-Qaida and other foreign fighters, their total number in Afghanistan was unlikely to have exceeded a thousand and was likely far fewer, probably only numbering a few hundred.[711] Since the foreign fighters played a strictly supporting role in Afghanistan, their means and motivations will not be further covered here.[712]

The post-2001 Taliban movement was, as a military force, less conventional in outlook than the old 1990s Taliban, but no less sophisticated and not lacking connections in a large number of countries. Moreover, the existence of sanctuaries in Pakistan enabled the movement to develop strategies based on hybrid warfare and hybrid threats.

Hybrid Warfare and Hybrid Threats

As noted, the hybrid warfare and hybrid threat capability developed by the Afghan Taliban included different tactics and strategies to be employed at

[710] GlobalSecurity: Hizb-i-Islami. 15.08.2012.

[711] Katzman, Kenneth: Afghanistan. Post-Taliban Governance, Security, and U.S. Policy, Washington, DC 2012, p. 48.

[712] On that topic, see, e.g. Fredholm, Michael: Afghanistan Beyond 2014. Stockholm 2013.

home and abroad. From both an analytical and practical perspective, these two theatres of war are best described as distinct from one another.

Being at war, the Taliban movement engaged in hybrid warfare in Afghanistan. Abroad, the movement instead utilized its capacity for hybrid threats. The domestic threat in Afghanistan deriving from the Taliban and the international threat of the movement were, consequently, quite different in character.

5.4.2 The Domestic Theatre: Hybrid Warfare

Military Power Projection against the ISAF and ANSF

In Afghanistan, the Taliban soon began to carry out a hybrid warfare campaign against the international coalition (Operation Enduring Freedom and the International Security Assistance Force, ISAF) and the fledgling Afghan National Security Forces (ANSF). The purpose of the campaign was to defeat or at least intimidate the coalition. Some Taliban leaders conceived that inflicting casualties on the foreign military forces would demoralize public opinion in their country of origin, causing panic among politicians, and thereby force a withdrawal.[713]

The hybrid warfare campaign consisted of two mutually supporting activities. First, the Taliban employed military power, early on by what in effect were guerrilla-style attacks but soon thereafter they increasingly made use of Improvised Explosive Devices (IEDs) placed at convenient locations, in particular along roads, in vehicles, or used in suicide attacks. The IED campaigns had the dual objective of limiting the freedom of movement of the international military forces and at the same time intimidating the foreign soldiers, if they could not be defeated outright.[714]

[713] See, e.g. Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 255.

[714] For an example of the Taliban IED campaigns, see Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 29.

Pakistani military support, whether official or non-official, was particularly conspicuous in the IED campaign. As late as 2011, IED specialists in southern Afghanistan were still often of Punjabi origin. Locals believed that they were Pakistani Army specialists. When killed, the IED specialist would have to be replaced, so a replacement IED specialist was sent from the Taliban leadership. As a result, there was a degree of central control over the IED effort, which again suggests Pakistani involvement.[715] The Taliban had an IED development centre in Pakistan. The Taliban confirmed that Iraqi insurgents assisted them with IEDs, but ISAF assessed that both Iranian and Pakistani support played a major role.[716]

Since the Taliban knew that ISAF's rules of engagements did not permit the killing of minors, the Taliban developed a strategy of employing children as emplacers of IEDs.[717] In effect, this was yet another form of hybrid warfare tactics, since any killings of children by ISAF could be used for propaganda purposes.

Terror Power Projection against the ISAF and ANSF

At the same time, the Taliban employed what can best be termed terror power, through the use of suicide bombers against international and Afghan military targets. Sometimes they were particularly effective, such as when on 15 January 2006 the director of the Canadian Provincial Reconstruction Team (PRT), senior diplomat Glynn Berry, was killed in Kandahar City.[718] Tactics developed in which one or more suicide bombers were used to spearhead an assault which then was followed up with guerilla-style forces (a tactic incidentally first development in Chechnya[719]). Re-

[715] Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 250ff.

[716] Ibid., p. 252.

[717] Ibid., p. 251.

[718] Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 25.

[719] Fredholm, Michael: The New Face of Chechen Terrorism. Central Asia - Caucasus Analyst, September 2003, Johns Hopkins University, Georgetown.

sults could be spectacular, such as when the Taliban attacked Sarpoza Prison on the outskirts of Kandahar City on 13 June 2008 with a vehicle borne IED (VBIED), a suicide bomber, and a rapid full scale attack by Taliban fighters on motorcycles. Some 400 imprisoned Taliban fighters were released, then removed in buses which the Taliban had waiting outside.[720]

The purpose of the terror campaign was to intimidate the ISAF coalition into withdrawing its forces. A further objective was to create success stories which could be used for propaganda purposes (see below).

Terror Power Projection against the Afghan Population

The Taliban also engaged in terror campaigns directed specifically against the Afghan population. This can be seen as a continuation of the policies used by the Taliban in the 1990s (see above). Terror power was used to intimidate the population into defecting from the government supported by international forces and the ANSF. Shadow government structures (often far better organized than the governing structures used when the Taliban in fact ruled major parts of Afghanistan pre-2001) were set up to exert control over the population. Examples of the use of terror power include the killings of collaborators (government workers and ordinary Afghans who reported the location of Taliban units or IEDs to the international military forces) and what the Taliban in religious terms labelled apostates, that is, Muslims who did not subscribe to the extreme version of Islam adopted by the Taliban. The Taliban would then execute, often by beheading, a number of locals for cooperating with foreign troops, displaying the corpses in public as a warning to others.[721] These methods had a major impact on the Afghan rural population. Cases were noted when Afghan National Police (ANP) units failed to engage the Taliban, since they knew that they or their families would then face the prospect of Taliban reprisals.[722]

[720] For this and other examples, see, e.g. Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 40 and 46.

[721] Ibid., p. 25 and 42.

[722] Ibid., p. 30.

In a similar manner, the Taliban regularly attempted to dissuade people from voting in the national elections. A common method to influence voters not to participate was to cut off the index finger of those who went to the polls, who were easily recognizable since dipping the finger in black ink was part of the election process.[723] The campaign served a dual purpose. First, it terrorized the population into adopting the extreme version of Islam which served as the Taliban movement's ideology, since the Taliban considered democratic elections an affront to Islam. Second, the mutilations eroded trust in the Afghan government.

Another example of how the Taliban imposed their will by terrorist power was the strategy to force telecom operators to close cellular telephone networks at night. The Taliban believed that the international military forces used cellular phone signals to track and launch attacks against them. This was probably a correct assessment since cell phones periodically send signals to the network even when they are not in use making calls and such signals can be monitored by signals intelligence, satellites, and other means. But the Taliban also feared that ordinary Afghans on the side of the government might observe them and wished to prevent such collaborators from privately calling in to report Taliban movements. ISAF set up a call centre for this very purpose in 2007. Since most Taliban movements took place at night for reasons of security, this was the time to shut down the telephone networks. For this reason, the Taliban began to blow up telecommunications towers following threats to telephone operators warning them to shut down the towers at night or face attack. When telephone service providers responded by following the Taliban movement's orders, the Taliban not only ensured their own security, they also made a huge impact on the Afghan population, eroding their will to resist Taliban control by showing them by example that it was the Taliban movement, not the government forces, which set the agenda.[724] This successful intimidation

[723] See, e.g. BBC News, 15.06.2014.

[724] See, e.g. the Textually.org web site <www.textually.org/textually/archives/2008/03/019260.htm>; citing AP, 01.03.2008; Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 33.

campaign enabled the Taliban to impose a strategic, delegitimising blow to the authority of the government.

A similar delegitimizing effect was achieved by the widespread assassinations of government leaders, high-ranking members of the clergy on the side of the government, and women in public service and girls' schools. While government leaders and women in public service were primarily targeted for political reasons and to intimidate the population, the assassination of pro-government clergy had the added effect of reducing their influence with the population. Those who were not killed had to remain in Afghan National Army (ANA) compounds from which they primarily preached by radio, not in person, which severely limited their impact and cleared the field for Taliban clergy to win the battle for souls.[725]

Media Power Projection against the Afghan Population

In the battle for souls, the Taliban also exercised its media power. This showed itself as proclamations and videos distributed online and by other means. The Taliban also used night letters, which were leaflets distributed at night, thus serving as a tangible reminder that the Taliban had a presence seemingly everywhere.[726] Due to the widespread illiteracy in Afghanistan, the night letters were often read out aloud by a mullah or an elder, which in itself increased the impact of the message. Media power fundamentally consisted of the dissemination of threats to collaborators and propaganda, which not only resulted in the winning of hearts and minds but also in the intimidation of the general public, who realized then, if not before, that when the foreigners eventually withdrew, the Taliban would remain.

Examples of intimidating propaganda included the video recording of public execution by stoning in August 2010 of a couple in Kunduz who in

[725] See, e.g. Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 44ff.

[726] Johnson, Thomas H.: The Taliban Insurgency and an Analysis of Shabnamah (Night Letters). In: Small Wars and Insurgencies 18: 3 (September 2007), p. 317ff.

the eyes of the Taliban had committed adultery, the recording of which was subsequently distributed through the Internet.[727]

Power Projection through Organized Crime

The Taliban also enlisted, in a manner, the help of organized crime.[728] The Taliban often encouraged the activities of local bandit gangs in areas where the Taliban movement had not yet established, but was working to gain, a presence. Not only did this facilitate Taliban activities by causing confusion and presenting additional targets to the international military forces and ANSF, the activities of bandit gangs also legitimized the subsequent imposition of Taliban justice and its harsh methods. In effect, the Taliban first encouraged the growth of crime, then stepped in to suppress it. Many bandit gangs would indeed find the arguments to join the Taliban movement persuasive at this time, especially if they had already used the Taliban name to discourage police and local communities from resisting.[729]

5.4.3 The International Theatre: Hybrid Threats

Diplomatic Power Projection against the ISAF Member States

Internationally, the Taliban primarily focused on diplomatic power projection. A major aim was to negotiate the withdrawal of the international coalition, with threats if necessary, so that the Taliban could return to power. For this task, the Taliban relied on diplomatic power, with negotiations

[727] Reuters, 16.08.2010; The Telegraph (UK), 27.01.2011 (<www.telegraph.co.uk>, with video).

[728] Here we will disregard the question of the extent to which the Taliban movement funded its activities through Afghanistan's abundant opium production. The opium trade was fundamentally a means for funding, thus providing the means to fight, and not intended as a means for hybrid threat projection as such, even though one could argue that in the long term, drugs from Afghanistan would play its role in destabilizing some of the states which provided troops to ISAF.

[729] Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 245.

conducted through friendly Muslim countries such as Pakistan, Saudi Arabia, the United Arab Emirates, and Qatar. These countries were not chosen at random; only Pakistan, Saudi Arabia, and the United Arab Emirates, in this order, had recognized the Taliban Emirate of Afghanistan in May 1997.[730]

The diplomatic process against ISAF member states can be said to have begun in September 2009 in Dubai, United Arab Emirates. At the request of the Taliban, German intelligence then held a first meeting with a Taliban delegation. A further eight meetings had to take place before the Germans brought in American representatives so that real negotiations could get underway. This first U.S.-Taliban meeting took place outside Munich in Germany on 28 November 2010, with the participation of a Qatari representative whom the Taliban representatives trusted. A second meeting consequently took place in Qatar's capital Doha on 15 February 2011. The third meeting took place in Munich on 7-8 May 2011. Through this series of meetings, the Taliban aimed to persuade the United States to lift sanctions, release high-level Taliban prisoners, and to allow the opening of a Taliban representative office in a Muslim country.[731]

These meetings all took place in secret, and at the time there was little chance for the Taliban to gain a negotiated American withdrawal. However, the Taliban diplomatic campaign eventually paid off in the form of a more public, international diplomatic presence, aimed more at the worldwide Muslim community than at the West.

[730] AFP, 25.05.1997 (Pakistan, on 25.05.1997); The News International, 27.05.1997 (Saudi Arabia, on 26.05.1997); AFP, 28.05.1997 (UAE, last of the three). Incidentally, the Taliban government in turn recognized the separatist government in the Russian republic of Chechnya in January 2000, an act which caused the lasting enmity of Russia. Jane's Sentinel: Afghanistan, 01.06.2000.

[731] Rashid, Ahmed: The Truth behind America's Taliban Talks. In: Financial Times, 29.06.2011.

Towards the worldwide Muslim community, it was important for the Taliban leadership to appear as a responsible and religiously legitimate party. The Taliban did not mind meeting with the Kabul government, as long as they met as equals. This was accomplished when Saudi King Abdullah hosted talks with the Taliban in the holy city of Mecca from 24 to 27 September 2008.[732]

However, it took some time before suitable conditions for further meetings could be agreed, not least because of difficulties for outside observers to ascertain whether the alleged Taliban representatives who turned up from time to time really represented Mullah Omar. In June 2013, formal peace talks between the Afghan government and the Taliban were finally announced, to take place in Doha. However, the Qatari leaders were somewhat too hospitable to their Taliban guests, allowing them to open a formal representative office, and the talks were cancelled in a row over the Taliban displaying their flag and presenting themselves as the legitimate rulers of the Islamic Emirate, that is, the state of Afghanistan. The Doha office was closed within 24 hours of its opening, amid speculations that negotiations would reopen in Turkey or Saudi Arabia.[733]

Nonetheless, the Taliban had achieved their aim of appearing as a responsible and legitimate party. Besides, U.S. President Barack Obama had by then announced the planned drawdown of American military forces in Afghanistan, so for the Taliban leadership, it was only a question of time before they could make a move for real power. When in early 2014, Taliban leaders met representatives of the Afghan government in Dubai, United Arab Emirates, and in Riyadh, Saudi Arabia, they refused to negotiate a peace agreement.[734] This led to discussions on whether the Taliban representatives had been genuine emissaries of Mullah Omar or frauds; however, there was at this time no reason for the Taliban movement to negotia-

[732] CNN, 05.10.2008.

[733] Reuters, 14.08.2013.

[734] The New York Times (USA), 04.02.2014.

te further, since they had already achieved their key diplomatic aim of being seen as a legitimate party.

Media Power Projection against the ISAF Member States and the Worldwide Muslim Community

In conjunction with the application of diplomatic power, the Taliban movement also made good use of media power projection. The media campaign was aimed simultaneously at the ISAF member states and the worldwide Muslim community. Its purpose was to show the might of the Taliban, the hopelessness of continued war against them, and their legitimacy vis-à-vis the worldwide Muslim community.

Already in the 1990s, the Taliban had operated a series of web sites, and this practice continued from the sanctuaries in Pakistan. Taliban web sites primarily published statements of the Leadership Council of the Islamic Emirate of Afghanistan, that is, the Taliban government, but they also published articles, weekly analyses, interviews, and reports, as well as a continuing list of news from the front. For an example of the latter, see Table 9. The emphasis was on enemies killed, in particular foreigners, ANA troops, and Arbakis (self-defence militias on the side of the government), and installations attacked.

11/05 : Enemy vehicle blown up in Kunduz

11/05 : Enemy base struck with missile strikes in Logar

11/05 : Arbakis come under attack in Kunduz

11/05 : Base in Logar comes under artillery rounds

11/05 : 46 killed, many injured in Ghazni operation

11/05 : 6 killed in gunfight in Nangarhar

11/05 : 6 Arbakis killed in Wardak

11/05 : Commander along with 2 police captured in Kabul

10/05 : 5 enemy soldiers killed, 4 injured in Ghazni

10/05 : Enemy security post destroyed in Laghman

10/05 : Army installations attacked in Kabul

10/05 : Enemy check point attacked

10/05 : Mortar shells hit post; Arbaki killed

10/05 : Clash occurs as enemy attacked in Paktika

10/05 : Arbaki commander, 2 gunmen killed in Paktika

10/05 : Arbaki militias suffer deadly losses in Kunduz

10/05 : 6 killed, two armored tanks destroyed in Kunduz

10/05 : 14 killed, 22 vehicles destroyed as convoy ambushed

10/05 : Double martyrdom attack causes U.S.-nato invaders heavy losses

10/05 : 5 puppets[735] killed and wounded, vehicle and equipment seized

10/05 : Check post attacked, 3 police killed in Marjah

10/05 : 3 police and ANA trooper killed in clash

10/05 : 5 ANA and 3 Arbakis killed in Gerishk, equipment seized

10/05 : Roadside bomb rips through police truck, kills and wounds 4

10/05 : Chora firefight leaves 2 puppets wounded

Table 9: Sample text from Taliban web site*<http://shahamat-english.com/>, 11.05.2014.*

[735] Afghans who supported the international forces.

The Taliban movement also published a glossy, professionally produced electronic news magazine in English, with news from the front, lists of destroyed enemy aircraft, statistics of attacks, articles, interviews, and the like. This was *Islamic Emirate Afghanistan In Fight*, a publication with many colour photographs, including photos of killed and wounded enemy soldiers and destroyed enemy vehicles. The magazine was most likely published and distributed from Pakistan.

The Taliban also discovered, and made good use of, Twitter. As a tool for the dissemination of brief propaganda nuggets in English, Twitter eventually began to rival the Taliban web sites. The Taliban tweets focused on news from the front, with the customary emphasis on enemies killed and installations attacked. For a few examples of Taliban tweets, see Table 10.

Abdulqahar Balkhi @ABalkhi

A martyrdom seeker detonated car bomb on dismounted foreign troops in front of Maiwand district HQ building (#Kandahar) 3:30pm today...

Abdulqahar Balkhi @ABalkhi

cont: as other troops gathered to evacuate the casualties around destroyed tank, another martyrdom seeker approached & detonated motorbike.

Abdulqahar Balkhi @ABalkhi

cont: blasts killed more than 15 invaders & wounded many on final day of #KbWaleed operations, area cordoned off from public #Afghanistan

Abdulqahar Balkhi @ABalkhi

A US terrorist along with Arbaki lapdog were killed, 3 US invaders wounded in missile strike on Shilgar district HQ (#Ghazni) 10am Wed.

Table 10: Sample Taliban tweets <*https://twitter.com/ABalkhi*>, *07.05.2014*

While the Taliban media campaign did have the objective of influencing the population in the ISAF member states, the Taliban no doubt realized that few ordinary Westerners would read their magazines, announcements, or tweets. Something more tangible was therefore needed to influence public opinion in the ISAF member states. For this purpose, apparent Taliban agents issued threats by telephone or Short Message Service (SMS) text messages to the family members of ISAF soldiers serving in Afghanistan on a number of occasions. Some were threats that family members would be murdered if the soldier did not leave Afghanistan, while others assured family members that it was the ISAF soldier who would be killed, if his or her family did not get their offspring back home. There was little doubt that the threats were meant to intimidate the individual into resigning from service in Afghanistan. Some calls emanated from the area of operations in Afghanistan, while others originated within the ISAF member state, likely within the Afghan refugee Diaspora. This showed the apparent worldwide reach of the Taliban movement. Less obvious but possibly equally serious, was that the telephone and SMS threats were directed to the private telephones of family members, which could only have been identified by somebody taking note of the private calls from ISAF garrisons to the place of origin of the troops. This showed that the Taliban had been able to infiltrate at least some of the Afghan telecom companies providing roaming services.[736]

Among the various types of international hybrid threat projection employed by the Taliban, this was the only one which was not exclusively directed and executed from Pakistan. Threatening telephone calls and text messages also emanated from within the ISAF member states, proving that the Taliban had supporters within the Afghan Diaspora and among other groups overseas.

[736] Radio Sweden news program *Ekot*, 01.07.2010; Försvarsmakten (Armed Forces), Årsrapport Säkerhetstjänst 2011: Militära underrättelse- och säkerhetstjänsten, MUST (Försvarsmakten 2012), p. 18.

As far as is known, none of the telephone threats resulted in an actual attack. Indeed, a conspicuous characteristic of the terror power projection abroad of the Afghan Taliban movement was that the Taliban neither planned, nor carried out through opportunistic means, terrorist attacks *outside* Afghanistan. This did not happen during the 1990s, nor after the Taliban withdrawal into Pakistan. International terrorism would seem to have been a certain means to intimidate a foreign population into forcing a withdrawal of its military forces from Afghanistan. Yet no such attacks were carried out by the Afghan Taliban movement (although they certainly were carried out by the Taliban movement's allies among the Al-Qaida and other international terrorist groups for reasons of their own).

The reason for this curious absence of international terror power projection can presumably be seen in two characteristics of the Afghan war. First, the Afghan Taliban movement had no history of engaging in terrorism abroad and many of its leaders had little interest in events elsewhere. Second, from 18 June 2004, when the first known American drone attacks was carried out,[737] a balance of terror emerged between the United States and the Taliban movement. As long as the Afghan Taliban movement did not sponsor international terrorism, the United States did not direct any drone attacks against the senior Afghan Taliban leaders in Pakistan. Whether this was a deliberate agreement with the Americans, if so it was no doubt negotiated with the help of Pakistani mediators, or merely an assumption on the part of the Taliban leadership remains unknown. Implicit in the understanding must have been the American realization that one eventually would need to have somebody to negotiate with in the Taliban leadership. Whether this conclusion is correct remains unknown to outside observers. Yet the fact remains that the Taliban leadership did not sponsor international terrorism, and no American drone attacks were aimed against the senior Taliban leaders in their well-known and easily recognizable compounds in a suburb of the Pakistani city of Quetta.

[737] The New York Times (USA), 19.06.2004.

5.4.4 Concluding Remarks

The Taliban leadership had a *long-term strategy* to gain political power and impose a strict form of Islam in Afghanistan. When faced with the inability to defeat the coalition by regular military means, the long-term strategy hardened into an *intention* to fight with whatever tactics and strategies that were available. Although not conclusively proven, it seems likely that a *master plan* on how to oppose the coalition and the government of Afghanistan through a combination of military power and terror power was worked out with the assistance of former or serving ISI officers. The actual details – the *operations plan* – grew out of developments in Afghanistan and elsewhere, such as the limited number of foreign troops that were sent to Afghanistan. The Light Footprint policy, that is, the lack of boots on the ground, enabled the Taliban movement to reassert power in parts of the country. The *execution* phase of the operations plan began with full force only from 2005, since, despite incursions into Afghanistan, the Taliban were, as noted, earlier not under serious military pressure there or elsewhere.

This operations plan certainly included aspects of hybrid warfare and hybrid threats. Whether the Taliban actually used such terms is a moot point; events show that they knew about and understood the concepts of hybrid warfare and threats very well. The Afghan Taliban leaders consequently developed a hybrid threat capability, which they subsequently used as part of the tactics and strategies of the movement.

There is no denying that the Afghan Taliban movement enjoyed a certain level of success in its hybrid warfare campaigns. Most successes derived from the movement's capability to create and sustain a domestic hybrid capability. While the Taliban hybrid warfare capability was not in itself sufficient to defeat the international coalition, it certainly helped to create a sense of defeatism which ultimately led to President Obama's 22 June 2011 decision to end the American-led military presence in Afghanistan by 2014.[738] But this defeatism was not the result of the Taliban movement's

[738] The New York Times (USA), 22.06.2011.

attempts to intimidate the foreign militaries or their constituencies abroad. Instead, it derived directly from the Taliban ability to intimidate the Afghan population into turning away from the foreign military presence and the government of Afghanistan, an effect much facilitated by the general ineptitude and widespread corruption of the latter during these crucial years.

Then why did the Afghan Taliban movement neither plan, nor carry out through opportunistic means, terrorist attacks outside Afghanistan? International terrorism would seem to have been a certain means to intimidate an enemy population into forcing a withdrawal of its military forces from Afghanistan, yet no such attacks were carried out by the Afghan Taliban movement—and the behaviour of the Taliban toward the Afghan population shows that it was not a reluctance to engage in violence that decided the issue. The reasons for this lack of foreign terrorism were no doubt twofold. First, the Afghan Taliban had no history of engaging in terrorism abroad. Second, a balance of terror emerged between the Taliban and the U.S.-led coalition. As long as the Afghan Taliban movement did not sponsor international terrorism, no drone attacks targeted senior Afghan Taliban leaders in Pakistan.

This balance of terror also illustrates the phenomenon that successful insurgencies tend to share two common features: access to sanctuaries in a neighbouring country and access to material support and financing from outside the conflict zone, either in the neighbouring country or from a Diaspora population abroad. In 1964, the experienced French counterinsurgency and counterterrorism practitioner Roger Trinquier concluded that the best strategy to confront such an insurgency was a secret war against the neighbouring country, through the creation of a clandestine guerrilla force on its territory to strike the insurgent sanctuaries and serve as leverage until the material support ceases.[739] The armed drone program, which

[739] Trinquier, Roger: Modern Warfare: A French View of Counterinsurgency. Westport, Connecticut 2006 (first published in 1964), p. 83. Trinquier describes the enemy in both counterinsurgency and counterterrorism as an armed clandestine organization, engaged in clandestine warfare. The clandestine organization operates in one or both of two modes, that of partisan/guerrilla and terrorist, respectively. These two categories function in different ways since they operate in different types of terrain. In the

was led by the civilian Central Intelligence Agency (CIA) and utilized a combination of military and terror power, was in effect a high-tech version of such a clandestine force, which in the context of the present paper easily qualifies as a hybrid threat response to a hybrid threat.

There could be no purely military solution to the problem of Taliban and foreign fighters as long as they retained sanctuaries in Pakistan.[740] History is rife with cases in which guerrilla groups could not be defeated as long as they were granted sanctuaries in neighbouring countries. A military solution could certainly have been found—if the coalition had been prepared to follow the enemy into their sanctuaries in Pakistan. However, the countries that constituted ISAF were unwilling to do so without Pakistani cooperation, and such was never likely to be forthcoming since Pakistan was sensitive about its territorial inviolability and integrity. The problem of the inviolability of the Pakistani sanctuaries of the Taliban became evident when U.S. conventional troops launched the only major ground offensive in the 2001-2002 war against the Taliban. This was Operation Anaconda, commanded by Major General Franklin Hagenbeck and commenced on 1 March 2002 against what was reported to be a concentration of several hundred Taliban and Al-Qaida troops south of Gardez in Paktia province.[741] This was the first time U.S. and coalition conventional forces were at the forefront of ground combat. Operation Anaconda was declared over on 18 March 2002. As before, the Taliban and Al-Qaida fighters simply

partisan/guerrilla mode, an armed clandestine group will choose targets to establish a presence and gain territorial control through a display of power. The post-2001 Taliban movement operated in this mode in Afghanistan, and the same went on among jihadist insurgents in Pakistan, Yemen, Somalia, Mali, Syria, and fundamentally in any other place where armed clandestine groups operated. Having established a degree of territorial control (cf. Al-Qaida in Afghanistan prior to 2001), the group was, simultaneously with conducting local operations, free to engage, or not, in international terrorism as well. Ibid., p. 16. Yet the importance of a local base is often forgotten in terrorism studies. Trinquier's experiences could have been particularly useful in post-2001 Afghanistan but were largely forgotten when operations were initiated.

[740] Fredholm, Michael: The Need for New Policies in Afghanistan: A European's Perspective. Himalayan and Central Asian Studies 15: 1-2 (2011).

[741] John Pike: Operation Anaconda. 05.07.2011. <http://www.globalsecurity.org/military/ops/oef-anaconda.htm>.

dispersed and withdrew, many of them into Pakistan, when the battle turned against them. After the operation, Major General Hagenbeck indicated the need to engage in hot pursuits into Pakistan, but on 25 March he was overruled by then Secretary of Defence Donald H. Rumsfeld.[742] As a direct result of Rumsfeld's decision, the Taliban and allied non-Afghan terrorist groups established bases in Pakistan, the Taliban set up in and around Quetta and the Al-Qaida and other foreign fighters went, primarily, to Waziristan.

How could the coalition reach and neutralize these bases? By military means, it could not, since no coalition soldiers were permitted to engage in hot pursuit into Pakistani territory. Drone warfare became the solution, and the CIA's clandestine Predator and Reaper armed drone program inflicted significant losses on terrorists and insurgents in Waziristan.[743]

The drone campaign had a strategic effect that went far beyond the killing of insurgent leaders and the disruption of insurgent networks and activities. First, data-driven as opposed to anecdotal research shows that drone strikes were associated with decreases in the incidence and lethality of terrorist attacks. They were also associated with decreases in particularly lethal terrorist tactics, including suicide and IED attacks.[744] A primary reason for this was the disruption mechanism of drone strikes. Strikes disrupted and reduced the ability of terrorists in the safe havens to operate in a cohesive and effective manner. The havens were simply not safe anymore, and the terrorists found it increasingly difficult to exercise sovereign control over their sanctuaries. In addition, the drone strikes resulted in the deaths of many terrorist leaders. This too reduced the ability of the terrorists to engage in violence elsewhere, since the decapitation of the terrorist leadership reduced its ability to plan and carry out acts of terrorism. In effect, drone

[742] Hammer, Carl: Tide of Terror: America, Islamic Extremism, and the War on Terror. Boulder, Colorado 2003, p. 281.

[743] Roggio, Bill/Mayer, Alexander: Charting the Data for US Airstrikes in Pakistan, 2004-2014. <www.longwarjournal.org>.

[744] Johnston, Patrick B./Sarbahi, Anoop K.: The Impact of U.S. Drone Strikes on Terrorism in Pakistan and Afghanistan. Paper, RAND Corporation and Stanford University 11 February 2014.

attacks terrorized the terrorists, forcing them to change their activities so as not expose themselves needlessly to strikes. Moreover, data indicate that drone strikes seemed to reduce terrorist activity not only in their safe havens but in their immediate neighbourhoods as well.[745] It was thus hardly surprising that Pakistan's military leadership tacitly agreed to the drone campaign in Waziristan early on, a territory which by then was beyond the control of the Pakistani military, even though it resulted in political frictions.[746]

There is thus little doubt that drone strikes aimed at the Taliban Leadership Shura in Quetta would have made an impact on the Taliban movement, had such strikes taken place. However, this particular method of hybrid warfare was not used by the United States against the Taliban leaders, nor did the latter respond with terrorist attacks overseas. A hybrid threat, drone warfare, was accordingly successfully used to counter another hybrid threat, that of international terrorism

[745] Ibid., p. 25.

[746] See, e.g. Reuters, 20.05.2011, based on a U.S. diplomatic cable from 11.02.2008 exposed by WikiLeaks detailing discussions between Pakistan's chief of army staff General Ashfaq Kayani and Admiral William J. Fallon, then commander of U.S. Central Command.

6 Index

6.1 Index of Abbreviations

ACT	Allied Command Transformation
AG	public limited company
AIVD	(Dutch) General Intelligence and Security Service
ANA	Afghan National Army
ANP	Afghan National Police
ANSF	Afghan National Security Forces
AP	Associated Press
APCIP	Austrian Program for Critical Infrastructure Protection
ATTA	Afghan Transit Trade Agreement
AUV	autonomous underwater vehicle
BBK	Federal Office of Civil Protection and Disaster Assistance
BiH	Bosnia-Herzegovina
BMLVS	(Austrian) Ministry of National Defence and Sport
BND	(German) Federal Intelligence Service
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CPNI	(Dutch) Centre for Protection of National Infrastructure
CSCE	(American) Commission on Security and Cooperation in Europe
CSEC	(Swedish) Certification Body for IT Security

CSIRT	(Dutch) Computer Security Incident Response Team
CSP	comprehensive security provision
DDoS	distributed denial-of-service
DefCERT	(Dutch) Defence Computer Emergency Response Team
DG TREN	(European) Directorate-General for Transport and Energy
DNV	Det Norske Veritas
DO(o)D	(U.S.-American) Department of Defense
EBRD	European Bank for Reconstruction and Development
EC	electronic cash
EIA	environmental impact assessment
EMC	electromagnetic compatibility
ENISA	European Union Agency for Network and Information Security
EPCIP	European Program for Critical Infrastructure Protection
ERM	environmental resources management
ESB	(Swedish) Electrical Safety Board, responsible for EMC
ESDP	European security and defence policy
ESS	European security strategy
EU	European Union
EUFOR	European Union Force
EUMM	European Union Monitoring Mission
EUR	euro (currency)
FBI	(U.S.-American) Federal Bureau of Investigation
FHS	Swedish National Defence College
FIOD	(Dutch) Fiscal Information and Investigati-

	on Service
FMV	(Swedish) Defence Materiel Administration
FOCP	(Swiss) Federal Office for Civil Protection
FOI	(Swedish) Defence Research Agency
FRA	(Swedish) National Defence Radio Establishment
GAO	(U.S.-American) Government Accountability Office
GCHQ	(U.K.) Government Communications Headquarters
GIUK	Greenland-Iceland-United Kingdom
GNINGI	(Russian) State Research Navigation-Hydrographic Institute
GOVCERT	(Austrian) Government Computer Emergency Response Team
GPS	Global Positioning System
GRU	(Russian) Main Intelligence Directorate
HIG	Hezb-e-Islami of Gulbuddin Hekmatyar
HIIK	Heidelberg Institute for International Conflict Research
HRW	Human Rights Watch
ICCM	international conflict and crisis management
ICJ	International Court of Justice
ICT	information & communication technology
ICTY	International Criminal Tribunal for the former Yugoslavia
IEA	International Energy Agency
IED	improvised explosive device
IFK / IPSCM	Institute for Peace Support and Conflict Management
IMF	International Monetary Fund
IMU	Islamic Movement of Uzbekistan

IR	international relations
IRB	(Dutch) IT Response Board
IS	Islamic State
ISAF	International Security Assistance Force
ISI	Pakistani Inter-services Intelligence agency
ISIS	Islamic State of Iraq and (greater) Syria
ISS	International Security Strategy
IT	information technology
IVL	(Swedish) Environmental Research Institute
IWWN	International Watch and Warning Network
KBM	(Swedish) Emergency Management Agency
KBV	(Swedish) Coast Guard
KGB	(Russian) Committee for State Security
LNG	liquefied natural gas
LVAk	(Austrian) National Defence Academy
MIVD	(Dutch) Military Intelligence and Security Service
MMT	Marin Mätteknik AB
MNRE	(Russian) Ministry of Natural Resources and Ecology
MSB	(Swedish) Civil Contingencies Agency
MSD	(Swedish) Military Strategic Doctrine
MUST	(Swedish) Military Intelligence and Security Service
NATO	North Atlantic Treaty Organization
NBV	(Dutch) National Communications Security Agency
NCSC	(Dutch) National Cyber Security Centre
NCT	(Swedish) National Centre for Terrorist Threat Assessment
NCTB	(Dutch) National Coordinator for Counter-terrorism

NDS	(U.S.-American) National Defense Strategy
NEGP	North European Gas Pipeline
NEGPC	North European Gas Pipeline Company
NEL	Northern European natural gas pipeline
NG(R)O	non-government organisation
NORDEFCO	Nordic Defense Cooperation
NSA	(U.S.-American) National Security Agency
NSIT	(Swedish) National Cooperation Council against Serious IT Threats
NTSG	(Swedish) National Telecommunications Coordination Group
OECD	Organisation for Economic Co-operation and Development
OC	organised crime
OPAL	Baltic Sea connection pipeline
OPTA	(Dutch) Independent Post and Telecommunications Authority
OSC(Z)E	Organization for Security and Cooperation in Europe
OSSR	Armed Forces of the Slovak Republic
PR	public relations
PRT	(Canadian) Provincial Reconstruction Team
PTS	(Swedish) Post and Telecom Authority
RAF	Red Army Faction
RKP	(Swedish) Criminal Investigation Service
SAMFI	(Swedish) Cooperation Group for Information Security
Säpo	Swedish Security Service
SAS	Special Air Service
SASIB	Slovak Association for Information Security
SCADA	Supervisory Control and Data Acquisition
SEK	Swedish krona (currency)

SGU	Geological Survey of Sweden
SIOD	(Dutch) Social Information and Investigation Service
CIP	critical infrastructure protection
SMS	Short Message Service
SOFÄ	(Swedish) Cooperation Project against Hazardous Substances
SOSUS	Sound Surveillance System
SR	Slovakian Republic
SRV	(Swedish) Rescue Services Agency
SSG	(Pakistani) Special Services Group
SST	state-sponsored terrorism
TEN	Trans-European Network
TTP	Tehrik-e-Taliban Pakistan, “Movement of Pakistani Taliban”
UAV	unmanned aerial vehicle
USSR	Union of Soviet Socialist Republics
UK	United Kingdom of Great Britain and Northern Ireland
ULV	comprehensive national defence
UN(O)	United Nations (Organization)
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNTSO	United Nations Truce Supervision Organization
USA / U.S.	United States of America
USD	(U.S.-American) dollar (currency)
VBIED	vehicle-borne improvised explosive device
VUCA	volatile, uncertain, complex and ambiguous
WGA	whole-of-government approach
WHO	World Health Organization
WMD	weapons of mass destruction

WTO	World Trade Organization
ÖBH	Austrian Armed Forces
ÖSS	Austrian security strategy

6.2 Index of Illustrations

6.3 Index of Tables

6.4 Author Biographies

In alphabetical order:

Mag. Dr. Rastislav BÁCHORA, eMA, born 1978. Doctorate in political science at the University of Vienna, postgraduate studies at the Faculty of Political Sciences at the University of Belgrade, since 2010 teaching at the Institute of European Studies and International Relations at Bratislava University.

Mag. Dr. Gerald BRETTNER-MESSLER, born 1969, studied history and a combination of topics (contemporary history, history of law, eastern European history, political science) at the university of Vienna, since 2003 principal teaching officer and researcher at the National Defence Academy.

Mag.iur. Christoph R. CEDE, born 1992, studied law at the University of Graz. Currently continuing with Intelligence and Strategic Studies at the University of Aberystwyth. In the summers of 2014 and 2015 he worked as an invited researcher at the IFK.

ObstdhmfD Mag. Anton DENGG has been at the IFK since 2004. He studied political science at the University of Vienna. Various lecturing activities on the topics of terrorism and counter-terrorism as well as threat and conflict scenarios. Member of the Combating Terrorism Working Group (CTWG) of the PfP Consortium. From 2011-2013 engaged as adviser on anti-terrorism issues at the Action Against Terrorism Unit (ATU) in the Transnational Threat Department (TNTD) of the Organization for Security and Cooperation in Europe (OSCE). Since March 2013 head of the department of conflict and perceived threats at the IFK.

Prof. Dr. Michael FREDHOLM is a historian and defence analyst who has written extensively on the history, defence strategies, security policies, and energy sector developments of Eurasia. He is currently affiliated to the Stockholm International Program for Central Asian Studies (SIPCAS), which originated at Stockholm University and, since 2012, has been based at the Swedish Research Institute in Istanbul. At SIPCAS, he has made a special study of Central Asian geopolitics, Afghanistan, Islamic extremism, and the causes of and defence strategies against terrorism. He has worked as an independent academic advisor to governmental, inter-governmental, and non-governmental bodies for more than two decades, including on Foreign Ministry official reports on Eastern Europe, Russia, Central Asia, and failing states. Educated at Uppsala, Stockholm, and Lund Universities, Michael Fredholm taught at Stockholm University (South and Central Asia Programme), Uppsala University (Orientalist Programme), the Swedish Royal Military Academy and Defence Academy (various courses), and a special educational and advisory programme on East Asia for the Commander-in-Chief. He also lectured, during conferences or as visiting professor, at numerous institutions and universities in cities around the world including Ankara, Bishkek, Istanbul, Kolkata, Krynica, Madrid, New Delhi, Oslo, Shanghai, Srinagar, Stockholm, Tashkent, Tsukuba, and Vilnius.

Miliz MjrdhmtD Dipl.-Ing. Alfred GULDER, MBA, born 1967, works as deputy head of air traffic control at the national authority / Supreme Civil Aviation Authority at the Federal Ministry for Transport, Innovation and Technology (bmvit). He studied telecommunications at Vienna University of Technology, completed a Master of Business Administration and has worked in both civil and military industries as well as Austrian air traffic control.

Mag. Ramy YOUSSEF has been a member of technical staff since April 2013, working at the Bielefeld Graduate School in History and Sociology (BGHS) under the auspices of the German-Federal-government-supported initiative for excellence, and a member of the Institute for World Society Studies at Bielefeld University. Before that he studied political science at the University of Vienna, was a trainee in 2011 at the Institute for Peace Support and Conflict Management (IFK) of the National Defence Academy Vienna, and subsequently went on foreign deployment for KFOR. His fields of research include the sociology of political force and world politics, sociology theory with a focus on system-theoretical societal analysis. Currently doing a doctorate on the function, differentiation and communication of diplomacy from a system-theoretical perspective.

Mag.iur. Reinmar NINDLER has been a university assistant at the Intute of International Law and International Relations at the University of Graz as well as at the European Training and Research Centre for Human Rights and Democracy at the University of Graz, and is a Fulbright scholar at Columbia Law School, New York.

Dr. Thomas PANKRATZ, born 1967 in Linz. Political scientist. Researcher and principal teaching officer for strategy at the Institute for Strategy and Security Policy at the National Defence Academy (Vienna).

Herbert SAURUGG, MSc, Major, born 1974, for 15 years a regular officer in the area of command support, ICT and military security, and has been on sabbatical since 2012. Following on-the-job training as an academical security expert for ICT, he completed a Master's at Budapest Business School. He is a founding member of Cyber Security Austria, an association for promoting the security of Austria's strategic infrastructure, and creator of the civil society initiative "Plötzlich Blackout!", involving preparation for a pan-European electricity black-out. He works on systemic approaches to topics surrounding "systemic risks, critical infrastructure and crisis management".

Mag.iur. Mag.phil. Paul SCHLIEFSTEINER, born 1986, studied law and history at the University of Graz. Employed at the Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS). Currently participating in the Master's course in "International Security Studies" at the Universität der Bundeswehr, Munich.

Mag.iur. Michael N. SCHURIAN, BSc, born 1986, worked from 2013 till 2014 as an administrative trainee and technical assistant at the IFK. Studied law and international business administration at the University of Vienna and Singapore Management University. Currently doing a doctorate in law. Various courses at the Peace Operations Training Institute. Areas of research: theory of just war, military ethics, polemology, post-conflict rehabilitation.

Mag. Martin STAUDINGER, born 1968, head of the foreign department of 'profil' news magazine, for which he has reported from war and crisis zones such as Afghanistan, Congo (Kinshasa), Mexico, Libya, Syria, Chad and the Ukraine.

Band 17 / 2016

The technical achievements make our networked society ever more complex, thus increasing the factors that influence the security of social systems.

Whereas in this connection security experts speak about hybrid warfare, the authors of this book go one step further and examine the options of power projection that go far beyond combat operations. They see hybrid threat as the security challenge of the future. Examples support the book's theoretical part and possible options for action complete this publication.

ISBN: 978-3-903121-01-0

VIRIBUS UNITIS

www.bundesheer.at

SCHUTZ und HILFE