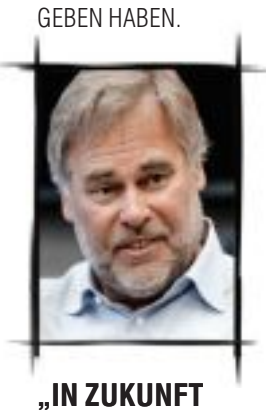
ANGRIFF AUF TSCHECHISCHE REGIERUNG
Nach Angaben des tschechischen Außenministers Lubomir Zaoralek sind Angreifer in Dutzende eMail-Konten des Außenministeriums eingedrungen. Es sei eine umfangreiche Datenmenge gestohlen worden. Auch der Account von Zaoralek sei betroffen gewesen. Hinter dem Angriff in Tschechien wird ein „fremder Staat" vermutet.

20
JAHRE HAFT
DROHEN VIER HOCHRANGIGEN RUSSISCHEN CYBER-SECURITY-EXPERTEN. UNTER IHNEN BEFINDET SICH AUCH DER LEITER DES ZENTRUMS FÜR INFORMATIONSSICHERHEIT DES INLANDSGEHEIMDIENSTES FSB. SIE SOLLEN INFORMATIONEN AN DIE CIA WEITERGEGEBEN HABEN.



„IN ZUKUNFT WERDEN WIR CYBER-ATTACKEN ERLEBEN, BEI DENEN SICH AMERIKANER WIE RUSSEN BENEHMEN UND RUSSEN WIE UKRAINER."

EUGENE KASPERSKY
Der Gründer des gleichnamigen Anti-Virus-Konzerns warnt vor falschen Fährten bei Cyber-Angriffen. Künftig könne es schwieriger werden, die Ursprünge solcher Attacken richtig zuzuordnen.

Krieg ohne Kampf

VON WILHELM THEURETSBACHER

In Österreich wurden der Flughafen Wien, die Nationalbank, ein Telekom-Anbieter, das Parlament sowie Außen- und Verteidigungsministerium Ziel politisch motivierter Cyber-Attacken. Österreich ist nicht das einzige Angriffsziel für Cyber-Kriminelle. Angeblich gab es gravierende Einmischungen in den US-Wahlkampf von außen. Der Instagram-Dienst der deutschen Bundeskanzlerin Andrea Merkel wurde kurz nach dem Start von mutmaßlich russischen Internet-Trollen überschwemmt. Die Ukraine stöhnt ohnehin unter einer Rekordzahl von Hackerangriffen. Montenegro, das gegen den Widerstand Russlands in die NATO will, kann sich neuerdings auch nicht vor Netzattacken unbekannter Herkunft erwehren. Auch Indien und Pakistan lieferten sich kürzlich eine Netz-Auseinandersetzung.

Gefährliche Welt
Die Welt sei gefährlicher geworden. Es gebe mehr offene Konflikte, Terrorismus und hybride Kriegsführung sowie Fehlinformationen in der Öffentlichkeit, befindet EU-Ratspräsident Donald Tusk.

Die NATO hat das Cyberspace als „Kriegsschauplatz" entdeckt. Das Bündnis erklärte das Netz zu einem zusätzlichen militärischen Operationsgebiet neben Boden, See und Luft und versuchte eine Definition der neuen, hybriden Bedrohungen, die sich nicht allein auf Cyber-Aktivitäten beschränken: Terrorismus, Migration, Piraterie, Korruption, ethnische Konflikte. Dabei finde eine Orchestrierung von Diplomatie, politischer Interaktion, humanitärer Hilfe, sozialem Druck, ökonomischen Einflussfaktoren, strategischen Medienkampagnen sowie Einsätzen militärischer Kräfte statt.

Angriffsziel Österreich
Das kleine Österreich mit seinen acht Millionen Einwohnern kann sich dieser neuen Bedrohungen nicht entziehen. So kommt Oberst Anton Dengg, Leiter des Referats „Bedrohungs- und Konfliktbild" vom Institut für Friedenssicherung und Konfliktmanagement (IFK) an der Landesverteidigungsakademie in Wien in einer Studie zu den hybriden Bedrohungen zum Schluss: „Die in der Ukraine-Krise bewaffneten Gruppierungen, die offiziellen Streitkräften nicht mehr zuordenbar waren, und Angriffe auf den Flughafen Wien oder die österreichische Nationalbank gelten als Beispiele für die neuen Machtprojektionsmöglichkeiten."

Methoden
Dengg fasst die neuen Kampfmittel zusammen. Sie umfassen im Wesentlichen:
- Nachrichtendienstliche Methoden
- Cybermittel
- Privatisierte Gewalt und Volksgewalt (Verhetzung, Korruption, Aufstand, Revolution …)
- Aktive oder passive Duldung von Terrorismus
- Diplomatische Noten
- Realwirtschaftliche und wirtschaftliche Ebene
- Umweltauflagen
- Wissenschaftliche und technologische Maßnahmen
- Mediale Vormachtstellung
- Unterschiedliche militärische Formen

Politik und Justiz
Hier gibt es bereits Fälle rückwirkender Enteignungen oder Rücknahmen steuerlicher Begünstigungen. Ein Beispiel: Irland mit Apple.

Auch für Österreich aktuell: Eingriffe in die Sicherheitspolitik eines Staates. Indem die Autorität von staatlichen Sicherheitsakteuren untergraben wird, mindert man das Vertrauen in Sicherheitsinstitutionen, was politische und gesellschaftliche ➔

Der neue Krieg ist scheinbar unmilitärisch. Es gibt keine Panzerdivisionen mehr, die über die Staatsgrenze rollen. Der Feind kommt jetzt aus dem Internet, über die Diplomatie und mit professionellen Saboteuren. Auch Österreich wurde bereits angegriffen.

Österreichs neue Sicherheitsstrategie gegen die

Der Landesverteidigungsplan ist nach dem Ende des Kalten Krieges in Vergessenheit geraten. Aber innerhalb von Vorgaben der EU hat die Regierung eine neue Sicherheitsarchitektur geschaffen.

Österreichs Gesamtstrategie für die Umfassende Sicherheitsvorsorge (USV) zielt auf das systematische Zusammenwirken verschiedener Politikbereiche ab. Ihre Umsetzung erfordert ein umfassendes Lagebild aller Akteure. Aus der USV leiten sich ab die Teilstrategie Innere Sicherheit des BMI und die Teilstrategie Verteidigungspolitik des Verteidigungsministeriums.

Das Bundeskanzleramt koordiniert die Implementierung der USV über wichtige Teilprozesse. Dazu zählen insbesondere das Programm zum Schutz der kritischen Infrastrukturen, die Cyberstrategie und das gesamtstaatliche Auslandseinsatzkonzept.

Innere Sicherheit
Ziel der österreichischen Sicherheitspolitik ist es, Österreich zum sichersten Land mit der höchsten Lebensqualität zu machen. Der soziale Frieden soll gestärkt werden. Daraus ergeben sich folgende Aufgaben:
- Kriminalität wirksam bekämpfen – neben den klassischen Herausforderungen der Massenkriminalität sind vermehrt Phänomene wie Computer- und Netzwerkkriminalität sowie Wirtschaftskriminalität konsequent zu bekämpfen.
- Neue Wege in der Prävention. Sie ist eine gesamtgesellschaftlichen Aufgabe.
- Asyl sichern, illegale Migration bekämpfen und Migration nach den Bedürfnissen Österreich steuern.
- Integration fördern und fordern.
- Daten nützen und schützen.

Aus der Österreichischen Sicherheitsstrategie leitet sich die Teilstrategie INNEN.SICHER ab, in der die Aufgaben und Projekte für die Mitarbeiter des Innenministeriums definiert sind.

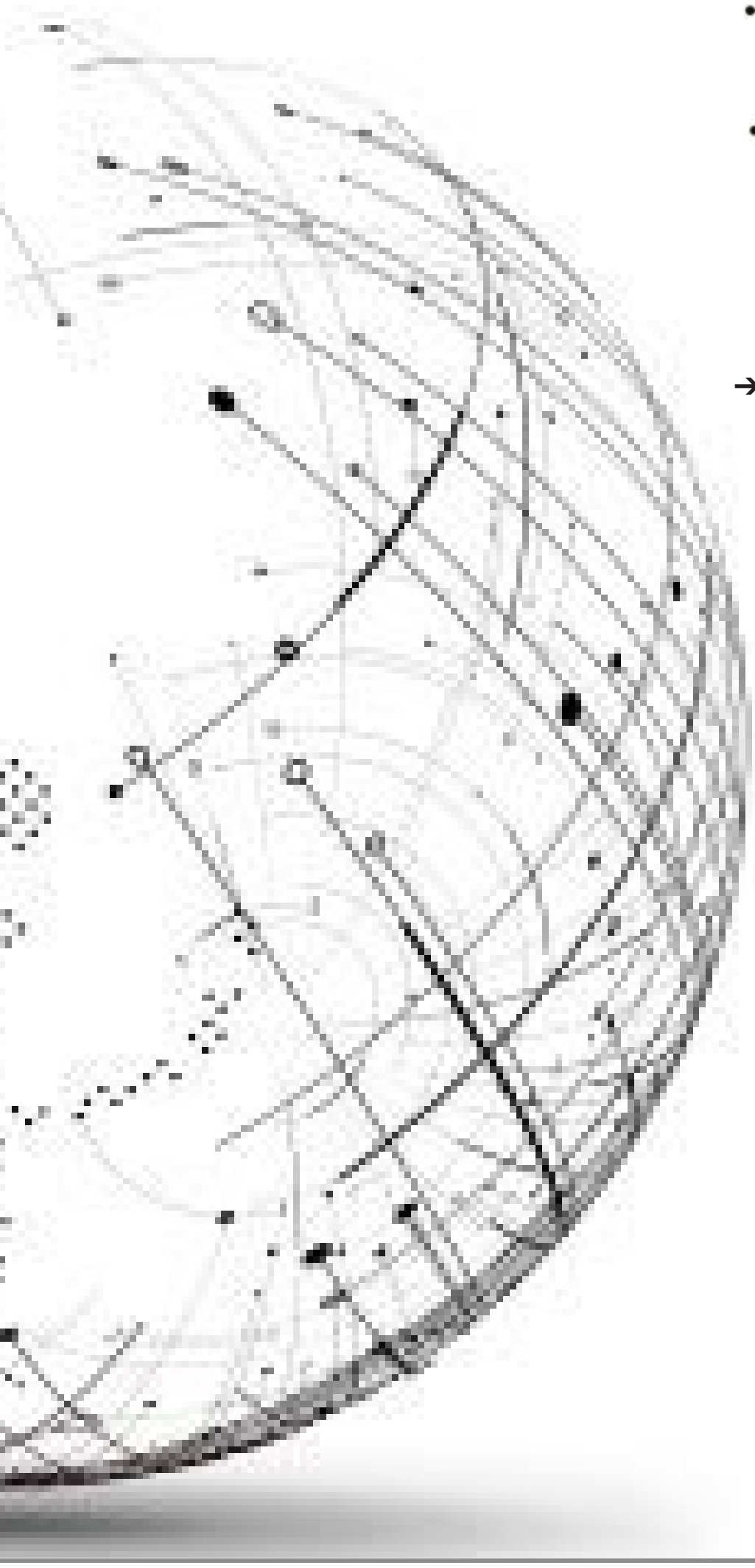
Verteidigungspolitik
Aufgaben des Bundesheeres sind unter anderem Gewährleistung der vollen staatlichen Souveränität und Integrität, Schutz der verfassungsmäßigen Einrichtungen und der kritischen Infrastruktur, Katastrophenhilfe, solidarische Leistung von Krisenmanagementbeiträgen und ein militärischer Solidarbeitrag zum sicherheitspolitischen Handeln der EU. Das Bundesheer wirkt mit der Außenpolitik und der Politik der inneren Sicherheit zusammen.

Diplomatie
Der österreichische diplomatische Dienst nimmt für die innerstaatlichen Stellen eine Vertretungs-, Informations- und Beurteilungsfunktion wahr. Mit seinem Netzwerk von Vertretungsbehörden trägt er dazu bei, dass im Rahmen internationaler Organisationen und Konferenzen österreichische Interessen in die internationale sicherheitspolitische Debatte einfließen.

Österreich wird sich auch künftig als Vermittler in internationalen Konfliktsituationen einbringen und sich um die Ansiedlung weiterer einschlägiger Organisationen und Agenturen bemühen, um damit die bereits bestehende Rolle Wiens als internationaler Amtssitz und als Drehscheibe für die internationale Sicherheitspolitik auszubauen.

Cyber-Strategie
Die „Österreichische Strategie für Cyber Sicherheit" (ÖSCS) bildet die Grundlage für das Zusammenwirken aller Ressorts in diesem Bereich. Ziel ist es, einen regelmäßigen Informationsaustausch zwischen den Cyber-

APA/AFP/ATTILA KISBENEDEK, ISTOCKPHOTO(2), REUTERS, SIMONIS, AP, APA/AFP/JOHN MACDOUGALL



„ DIE BEDROHUNGEN WIRKEN AUCH VOM AUSLAND NACH ÖSTERREICH, EGAL OB ES UM EINEN HACKERANGRIFF ODER ATTACKEN RELIGIÖS MOTIVIERTER EXTREMISTEN GEHT.“

KONRAD KOGLER
Sicherheitschef Österreich

„HYBRIDE KRIEGSFÜHRUNG MIT PROPAGANDA UND ATTACKEN IM INTERNET STELLEN EINE FUNDAMENTALE BEDROHUNG FÜR DIE WESTLICHEN DEMOKRATIEN DAR.“

ALEX YOUNGER
Britischer Geheimdienst MI6

→ Auswirkungen nach sich ziehen kann. Da spielt auch die weltweite Occupy-Protestaktion hinein, die sich von Nordamerika aus verbreitet hat.

Nachrichtendienste

Einflussmöglichkeiten durch Nachrichten- und Geheimdienste umfassen Manipulation von Informationsinhalten zu Propaganda- und Sabotagezwecken jeglicher Art, etwa gehackte eMails der US-Demokraten im Präsidentschaftswahlkampf.

Medienmacht

Zielgerichtete Propaganda und Fehlinformation sind aufgrund neuer Medien leichter zu verbreiten als je zuvor. Dieser Prozess kann als Machtdurchsetzung durch manipulative Information bezeichnet werden.

Dies ist nicht nur auf Medienkonzerne beschränkt, sondern kann auch durch jeden Bürger mit einem Internetanschluss über soziale Medien erfolgen. Jeder ist Teil eines Netzwerkes und kann Ereignisse nicht nur mitgestalten, sondern sogar bestimmend beeinflussen – auch wenn er sich dessen oft gar nicht bewusst ist.

Volksgewalt

Zu dieser Gruppe zählen unter anderem bewaffnete Aufständische, politische oder religiöse Extremisten und „Wutbürger“. Diese Volksmasse kann für die Interessen eines Akteurs instrumentalisiert werden. Die Bürger werden mit professionellen Methoden mittels scheinbar glaubwürdiger Fake-News radikalisiert – ohne, dass sie sich dieser Instrumentalisierung bewusst werden.

Auch eine nicht ausreichend integrierte Diaspora könnte durch das ursprüngliche Heimatland politisch mobilisiert werden. Ein Beispiel in Österreich ist eine türkische Parallelgesellschaft, die sich den politischen Botschaften aus dem Herkunftsland verpflichtet fühlt.

Privatisierte Gewalt

Private Militär- und Sicherheitsfirmen, paramilitärische Freiwilligenverbände, Milizen aber auch Piraten und kriminelle Organisationen verfolgen eigenständige Zielsetzungen. Gehen sie eine strategische Partnerschaft mit einer anderen Interessensgruppe ein, entstehen mitunter für beide Seiten Vorteile.

Mit verschiedensten geheimen Konstellationen von Kooperationen und Unterstützungsmaßnahmen kann im staatlichen Sinne politischer Druck erzeugt werden, wie beispielsweise die Hisbollah-Unterstützung des Iran im Libanon.

„ DIE INFORMATIONSSICHERHEIT DEUTSCHER STELLEN IN REGIERUNG, VERWALTUNG, WIRTSCHAFT, WISSENSCHAFT UND FORSCHUNG IST PERMANENT BEDROHT.“

HANS-GEORG MAAßEN
Verfassungsschutz Deutschland

Militärische Kräfte

Infiltration mit Militärexperten ist keine neue Idee. Schon im Kalten Krieg wurden von der damaligen UdSSR Spezialkräfte (SPEZNAZ) ausgebildet, die den Auftrag hatten, frühzeitig im Angriffsziel bewaffnet wirksam zu werden. Solche Kräfte wurden für Westeuropa ausgebildet. Zum Einsatz kamen sie aber erst bei der sowjetischen Invasion in Afghanistan 1979, wo sie den Auftrag hatten, die dortige Regierung frühzeitig zu liquidieren.

Aktuellstes Beispiel für einen SPEZNAZ-Einsatz ist die Krim, wo uniformierte Soldaten ohne Hoheitsabzeichen die Flugplätze besetzten – sie wurden als „kleine grüne Männchen“ bekannt.

Aber auch britische Elite-Kämpfer, die militärische Ausbildungstätigkeiten für Rebellen in Syrien durchführten, fallen in diese Kategorie. Die Rede ist von früheren SAS-Mitgliedern, die Trainingslager für 300 Rebellen errichteten und betrieben.

hybriden Bedrohungen

Sicherheit-Stakeholdern sicherzustellen, die Situation im Cyber-Raum laufend zu beobachten und ein aktuelles Cyber-Sicherheit-Lagebild zu erstellen.

Die zentralen Aufgaben der operativen Koordinierungsstruktur werden vom Inneren Kreis der operativen Koordinierungsstrukturen (IKDOK) wahrgenommen. Diese Gruppe setzt sich aus Vertretern aus dem Bundeskanzleramt, dem Innen- und dem Verteidigungsministerium zusammen. Der IKDOK bildet im Krisenfall die direkte Schnittstelle zum Cyber Krisenmanagement (CKM).

Krisenmanagement

Zur Bewältigung von Cyberkrisen wurde ein Cyber-Krisenmanagement (CKM) eingerichtet. Im zivilen Krisenmanagement hat das Innenministerium die Federführung. Das CKM ist funktional in das bereits bestehende Staatliche Krisen- und Katastrophenmanagement (SKKM) des Innenministeriums integriert.

Verteidigungsfall

Im Cyber-Verteidigungsfall geht die Zuständigkeit auf das Verteidigungsministerium über. Das Cyber Defence Zentrum (CDZ) des Heeres-Abwehramtes arbeitet in diesem Fall eng mit dem Cyber Sicherheit Center (CSC) des Verfassungsschutzes und dem Cyber Crime Competence Center (C4) des Bundeskriminalamtes zusammen.

Die Umsetzung der Österreichischen Strategie für Cybersicherheit wird von der Steuerungsgruppe (CSS) vorangetrieben. Zur besseren Vernetzung mit der Wirtschaft wurden Vertreter der wichtigen Sektoren Energie, Finanzen, Internet Service Provider, Industrie, Gesundheit, Transport und Kommunikation in die CSS eingebunden.

Die EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) ist der ordnungspolitische Rahmen. Sie ist gemeinsam mit den Ergebnissen der vom Kuratorium Sicheres Österreich (KSÖ) und der ATC - Austrian Technology Corporation GmbH durchgeführten Workshops die Basis für das zukünftige „Bundesgesetz für Cybersicherheit“, das in Vorbereitung ist.

Die österreichische Sicherheitsstrategie und die daraus abgeleiteten Teilstrategien ersetzen den Landesverteidigungsplan und erfassen alle aktuellen Bedrohungen

KOMMENTAR

Wir brauchen ein gesamtstaatliches Lagezentrum

VON WILHELM THEURETSBACHER

Kriege werden heute übers Netz vorbereitet und geführt. Der angegriffene Staat wird mit subversiven Methoden bis an den Rand der Handlungsfähigkeit gebracht. Oppositionsgruppen werden aufgewiegelt, die Legitimität der Führung wird durch eine Welle von Fake-Meldungen in den sozialen Medien untergraben. Das passiert anonym und verdeckt. Bis das Opfer den Angriff als solchen erkennt, ist es oft schon zu spät.

„Hybride Bedrohungen“ und „hybride Kampfführung“ nennt man diese Erscheinungen. Das erfordert völlig neue Sicherheits-Konzepte. Hier ist aber die Republik im internationalen Vergleich bereits recht gut aufgestellt. Abseits aller Koalitionsstreitereien wurde in den vergangenen Jahren eine Sicherheitsstrategie mit den dazugehörigen Teilstrategien geschaffen, die auch mit Leben erfüllt werden. Personal wird aufgenommen, Einsatzstäbe bei Polizei und Bundesheer beginnen zu arbeiten.

Es gibt auch beachtliche Erfolge, wie die Abwehr einer Serie von Cyber-Angriffen und die Enttarnung des mutmaßlichen türkischen Haupttäters durch das Heeresnachrichtenamt zeigt. Es gibt mit dem neu geschaffenen Sicherheitskabinett jetzt auch ein Entscheidungsgremium auf höchster Ebene, das eine scheinbare Führungsunfähigkeit wie während der Flüchtlingskrise 2015 künftig ausschließen soll.

Was noch fehlt, ist ein gesamtstaatliches Lagezentrum als Beratungsorgan für das Sicherheitskabinett. Denn das Sicherheitskabinett braucht exakte Analysen. Nicht nur Unterlassungen, sondern auch Überreaktionen könnten fatal sein. Beispielsweise die Serie von Vorfällen mit türkischem Hintergrund: Randalierer in Wien, ein angebliches Spitzelnetz und der Cyber-Angriff. In diesem Fall den hybriden Verteidigungsfall gegen den türkischen Präsidenten Recep Tayyip Erdoğan auszurufen, wäre vermutlich falsch. Denn nicht alles, was nach einem hybriden Krieg aussieht, ist auch einer. Aber nachdem das Lagezentrum ebenso wie alle anderen, bereits realisierten Einrichtungen im Regierungsprogramm steht, kann man auch hier auf eine Realisierung hoffen.

wilhelm.theuretsbacher@kurier.at