Institute for Peace Support and Conflict Management
National Defence Academy Vienna

November 2019

IFK MONITOR INTERNATIONAL

NEW TECHNOLOGIES - NEW IMPACTS ON INTERNATIONAL MISSIONS OF AUSTRIA?

Markus Gauster

New technologies and "disruptive innovations" are influencing not only international politics and global economy, but also the strategies and operational toolkits of state and non-state actors alike. Above all, they create new threats, but also opportunities for peace operations and humanitarian missions and have complex implications for Austrian and European stability. Technology-driven advances create the need to adapt to challenges and new rules of engagement on land, in the air, at sea and in cyber space. The question then arises: in which way can new technologies improve the ability of Austria and EU to operate in situations of conflict and fragility?

World military and defence technology expenditures continue to rise. At the same time, digital disruptions have a growing impact on arms industries and peace operations. New information and communication technologies (e.g. cloud computing for military networks), innovations in areas such as command and control (e.g. navigation warfare and geo-operations), mobility (e.g. autonomous vehicles, drones) or logistics (e.g. energy storage, 3D-printing) have created new business opportunities for the military-industrial complex. Peace support operations increasingly rely on advanced technological solutions that may differ from those used by Armed Forces for tasks in homeland.

New conflicts, threats & technologies

Armed conflicts have been influenced by the proliferation of technologies coupled with their increasing availability to irregular armed groups. They can now obtain know-how and hi-tech weapons in a relatively uncontrolled manner, either openly or in the Darknet. States have lost their technological supremacy and are struggling with a growing number of hybrid threats (according to Anton Dengg). The race for technologies that allow stakeholders to project power is well under way.

The nature and logic of violent conflicts has changed little. The urge for power, resources and reputation (according to Georg Elwert) remain key drivers of conflict and instability. However, not only technological progress, but also other (partly new) factors such as climate change, environmental disasters (e.g. forest fires) or illegal waste disposal influence the emergence and style of conflicts. Digitalization facilitates the nexus between organized crime and armed groups (e.g. in Mexico or Mali) and leads to a rapid growth of "Civil war economies" (according to Conrad Schetter; e.g. in Afghanistan).

New technologies can increase the probability of conflict spillovers into neighbouring states (e.g. Syria-Lebanon). In addition, social media (e.g. Twitter, Telegram) facilitates the decentralization of terrorist networks and their cross-border recruitment, outreach and propaganda (e.g. in the Sahel). False flag operations and digital dissemination of false narratives may generate unintended effects that

Note: This article represents exclusively the opinion of the author.

can escalate conflicts and endanger missions (e.g. the UNMOGIP mission observing the India-Pakistan conflict).

Peace operations in transition

European states become increasingly reluctant to supply troops to high-risk missions (e.g. MONUSCO in the DRC). New technologies for force protection and protection of civilians in hot spots (e.g. RSM Afghanistan or MINUSMA) are therefore becoming important. E.g., mine-clearing robotic systems in the Western Balkans or Afghanistan are now gaining in relevance, yet they have not been harnessed to their full potential.

UN peace operations require large military infantry numbers and police personnel (e.g. MONUSCO, UNMISS), but also hi-tech equipment to fill capability gaps (e.g. for MINUSMA). EU troop contributions are relatively small, yet some states provide more technologized troops (e.g. Austria‘s logistics unit at UNIFIL in Lebanon) as well as military assistance (e.g. training and advising Malian Forces with EUTM Mali). In addition, drones appear to be a game changer for missions.

The increasing “Digitalisation of peace operations“ (according to Joachim Klerx) creates opportunities for interaction (e.g. with the local population), but also renders peace support activities more vulnerable. Autocratic regimes, militias or the “Digital Caliphate“ (according to Abdel Bari Atwan) are able to attack and disrupt peace operations through the use of hacking, malware, or other methods of information warfare.

Command & Control

Global navigation satellite systems (GNSS) such as Galileo, GPS, GLONASS or BeiDou as well as mobile geo-operations (e.g. tactical mapping and terrain analysis) are both instruments of and subjects to a broader navigation warfare. These systems can support the mission command and enhance situational awareness, but are also subject to attacks since most of the satellite signals are unprotected.

Artificial intelligence (AI) technologies can support Big Data management, media monitoring and intelligence to inform better decision-making in missions. However, adversaries can make use of AI for disinformation campaigns, deepfake-videos or GNSS jamming and spoofing. These actions can be classified as cyber attacks that disrupt or falsify realities on the ground. Missions have to adapt, e.g. by using protected navigation systems.

Drones deployed in missions perform a variety of functions such as monitoring, use or removal of explosive ordnance, transportation, or real-time transmission. However, commercial drones are also widely used by conflict actors in order to undermine peace efforts or humanitarian support (e.g. in Yemen).

Some missions have become increasingly dependent on drones (e.g. the OSCE mission SMM Ukraine). UAVs can be effectively used to collect information and evidence on security-related issues to ensure successful mandate implementation and attract political attention. Therefore, drones are enhancing the legitimacy of the mission.

Information & Communication

The exchange of information during operations is increasingly shifting to virtual storage platforms (clouds), which are, however, quite vulnerable and susceptible to cyber attacks. The “Internet of things” offers new opportunities for military strategy including communication, but it also poses threats regarding cyber security. Information and communication technologies can empower and better equip states as well as non-state actors in hybrid and conventional warfare. In particular, militias have gained strength by using digital recruitment tools to attract fighters in internationalised armed conflicts (e.g. Syria, Afghanistan, Ukraine, Iraq or Libya).

Flatter organisations are, in general, better suited for digital communication, because they allow to control and finance combatants in a decentralized manner, e.g. through blockchain technology. On the other hand, the blockchain can make it easier for missions to follow stakeholder transactions and gather intelligence.

Traditional Armed Forces who struggle to adapt flat structure, risk being less effective on the ground. In order to be suited for dynamic environments and faster decision making, missions must learn how to operate under flatter hierarchies.

Mobility & Logistics

The need for greater mobility comes into conflict with the need for functionality. Hi-tech weapons or transportation systems (e.g. Hägglunds off-road vehicle used by the Austrian Armed Forces) require, in general, maintenance in an even more complex manner and more specialists. Tele- and Reachback-maintenance are therefore growing in importance, as well as 3D-printing to recycle existing materials directly in the area of operation. In addition, autonomous vehicles can replace personnel and help avoid casualties.

However, conflict dynamics are changing. E.g., roadside bombs used by anti-government forces in Afghanistan or Mali may not be as strategically effective for the adversary as ten years ago. Therefore, alternative or new means of combat are being developed and peace operations have to adjust.

Conclusions

The relevance of new technologies is increasing as the needs of missions are shifting: GNSS, Drones, geo-information systems or social media offer multiple benefits to operations and may add to peace support and mandate implementation. Hi-tech missions such as SMM Ukraine are one of the drivers of international crisis management.

Force protection technologies are prioritized: In high-risk environments, self-protection measures are often more important than the implementation of the mission mandate (e.g. the use of robotic systems in Mali or Afghanistan).

More complexity, more business opportunities: Technological progress increases the complexity of operations. Technical contracting and outsourcing have their advantages, but also increase vulnerabilities. In addition, new business models have emerged around missions, as the proliferation of technologies is becoming increasingly lucrative for many actors including private companies and militias.

Threats to missions outpace the benefits of new technologies: The decisive factor is the access to technologies and know-how, which, however, has become easier for adversaries to obtain. Missions are increasingly targeted by cyber attacks. For example, the loss of a drone in a mission means the loss of a crypto-algorithm (as happened in Ukraine, Libya or Yemen).

Added values for humanitarian aid: Digitalization, drones, etc. offer advantages for aid recipients (terrain mapping, search for missing people, aerial photography, medical support), but also pose challenges (e.g. secure data protection management or acting up to the premise of “do no harm“).

Technological “one stop shop“ packages needed: New technologies are often associated with increased costs, e.g. for equipment maintenance or personnel training. They can, however, be decisive for enhancing human security (e.g. easier identifying and reaching victims). Prioritizing the needs and challenges of technology users (troops and mission staff) and improving the quality of human-machine interface design can reduce costs (e.g. easy-to-understand design can lower qualification standards for personnel).

Reality Check: New technologies can be a game changer for future operations. In European Armed Forces, however, there is a general lack of resources to invest strategically in new technologies for peace support. Increased civil-military research cooperation in the field of technology, in combination with pooled funding, can help missions solve this dilemma.

Recommendations

Focus on the overall system (and not only on force protection): A strategic oversight is needed to make full use of technologies in the field of leadership, information, mobility, protection and sustainability. The priority should be given to the most functional and time-proven technological solutions, instead of the "latest" ones.

Analysing and anticipating the potential of new technologies in conflict management and conflict prevention: This must be taken into consideration in planning of military, civilian and humanitarian missions. Cyber warfare and the use of AI and drones also have important implications for International Humanitarian Law. Foreign missions should therefore take note of all legal developments in order to be able to adapt and take action in compliance with the law.

Use both established and innovative technologies for preventive action: In the age of Big Data, new technologies can help to quantify risks and probability of conflict escalation and enhance early warning systems. There is a clear need for a comprehensive situational awareness centre for international crises with inputs from all "Whole-of-nation-approach" stakeholders ("Austrian Stabilisation Team").

Promote interoperability for foreign engagements: In the field of armaments and defence technology, pooling & sharing between troop contributors can reduce costs and make maintenance easier, but it requires political will. In addition, more resources should be allocated to research and development.

Improve civil-military information sharing: Communication and coordination between the various actors in the field should be improved in order to strengthen the effectiveness of missions. In particular, social media dynamics should be assessed from a civilian and military perspective.

Raise awareness about the existing technical capabilities and opportunities: One should not fall for "hype" surrounding new technologies. Healthy scepticism of well-established and new technologies (e.g. strategic communication in missions) is required.

Consider the potential applicability of new technologies and the "human factor": It is crucial to adopt a user-centred approach focusing on user experiences. Ways to reduce cognitive overload have to be explored (e.g. cautious use of touch screens for navigation).

The entire spectrum of capabilities is required: The Austrian Armed Forces have to provide all essential capacities in order to be able to fulfil their role as a strategic reserve for the Republic of Austria. Appropriate resources should be allocated for this purpose.

Impressum:
Copyright, Production, Publisher: Republic of Austria / MoD,Roßauer Lände 1, 1090 Vienna
Edited by: National Defence Academy Vienna/IFK, Stiftgasse 2a, 1070 Vienna
Periodikum der Landesverteidigungsakademie
Printing: ReproZ W 19-XXXX, Stiftgasse 2a, 1070 Wien

www.facebook.com/lvak.ifk