RÓBERT ONDREJCSÁK
TYLER. H. LIPPERT (EDS.)

PANORAMA
SPECIAL EDITION OF PANORAMA OF THE GLOBAL SECURITY ENVIRONMENT 2019

NATO at 70:

OUTLINE OF THE ALLIANCE TODAY AND TOMORROW

HYBRID WARFARE – ORCHESTRATING THE TECHNOLOGY REVOLUTION

JOHANN SCHMID, RALPH THIELE

The Challenge of Hybrid warfare

Twenty-first century security and prosperity are challenged by complex, trans-regional, all-domain and multifunctional hybrid security threats particularly posed by a combination of state, non-state and pseudostate actors. In the Nordic and Baltic region and particularly regarding Ukraine, Russia continues to use disinformation, cyber-attacks and military posturing to challenge security. Additionally, an increasingly assertive China is looking to secure access to strategic geographic locations and economic sectors through financial stakes in ports, airlines, hotels, and utility providers, while providing a source of capital for struggling European economies. Russia and China have increased their transactional collaboration to increase their power and influence. Particularly in its neighbourhood, Russia is conducting a campaign of hybrid warfare below the level of openly declared war using various tools of national power in order to advance its strategic interest.

At the same time, Europe's borders, particularly in the south, are wide open. As dividing lines within European societies are growing and deepening, this exposes numerous vulnerabilities that can be exploited by all kinds of hybrid actors from various directions, not only or primarily from Russia. However, military strength provides additional opportunities to exploit hybrid methods, even without the active use of force. Military escalation potential or dominance by its mere existence would support any kind of subversive hybrid activities.

The Ukraine case illustrates an important relationship. The more closely connected and interwoven a country's relations with its adversary, and the more pronounced their mutual dependencies, the more potential starting points there are for hybrid methods of warfare. Consequently, globalization, close international interaction and intercon-

nected societies – as positive and desirable as these developments may be – have the potential to open up additional starting points for hybrid methods of warfare. This could make hybrid warfare a particularly favoured means among former friends such as Ukraine and Russia had been within the framework of intrastate conflicts, and especially in civil wars.

Hybrid warfare of a type e.g. demonstrated on the Ukrainian battlefield, if carried out against European countries, would pose a particular challenge for Europe and the crisis management of both NATO and the EU. Although it may seem unlikely from today's perspective, in an extreme case, NATO's military defence could be bypassed by subversive means in a 'downward escalation mode'. This may include possible military threats from within, for example as a result of long-term subversion, infiltration, propaganda or destabilization. With their security and defence policy primarily oriented towards external threats, neither NATO nor the EU would be prepared, able or ostensibly entitled to protect their member states, as well as themselves as organizations, against such challenges at the blurred interfaces of internal and external security.

Technological trends suggest that the portfolio of hybrid hazards will rapidly expand. While the EU and NATO have stated the high relevance of hybrid threats to include the meaning, possibilities and challenges of emerging, disruptive technologies, knowledge of their true capacities and capabilities is a privilege of the few. It is evident that political, civilian and military decision makers need to become more knowledgeable of the disruptive potential of new technological trends, which may offer new options of violence, as well as of the use of force in a hybrid warfare/conflict context. They also need to become sovereign actors, applying all necessary instruments of power to effectively counter hybrid threats (Schmid 2019a).

Clearly, it is of importance to come to a shared understanding of what is at stake. Yet, if it is time to act, for Europe, for NATO, for our nations – who is to act? If the given technological revolution must be orchestrated – by whom should it be orchestrated? Responsibilities need to

be defined. Orchestration in authoritarian states like Russia or China is not a problem - neither legally, not politically, nor ethically speaking. But in democratic nations this is a different matter. In countering hybrid warfare, there is more at stake than "prepare – deter – defend", as NATO is traditionally called upon to do.

Conceptual Considerations

All war is hybrid, but there is also a specific hybrid way of conducting war. In contrast to military-centric warfare, its centre of gravity is not primarily located in the military domain. While far from novel in its essence, the empirical manifestation of hybrid warfare can be surprisingly new and differ from case to case (Schmid 2017a). This hybrid warfare in the narrower sense is of a strategic nature and can be identified by three key characteristics and their hybrid orchestration:

1. Focussing the decision of war/conflict primarily on a broad spectrum of non-military centres of gravity (CoG).
2. Operating in the shadow of various interfaces, such as between war and peace, friend and foe, internal and external security, civil and military domains, state and non-state actors.
3. Utilizing a creative combination, hybrid orchestration and the parallel use of different civil and military, regular and irregular, open as well as covert means, methods, tactics, strategies and concepts of warfare, thereby creating 'ever-new' mixed hybrid forms.

While hybrid warfare actors generally resort to creative and indirect strategies of limited warfare and a limited use of military force, it must be emphasized that hybrid warfare potentially includes all levels of escalation. Friction and uncertainty are always part of the game and the perceived manageable use of force may get out of control. Due to its focus on a broad spectrum of non-military CoGs, a military decision as such is not necessarily required for hybrid warfare actors to achieve their political goals. As happened in Donbas or during the Second In-

dochina War (Schmid 2017b, 373-390), militarily it may be sufficient for the hybrid warfare actor to prevent his opponent from deciding the war on the military battlefield, while seeking a decision on a non-military centre of gravity. Morale and legitimacy can become strong weapons in this context.

Hybrid warfare generally favours the offensive as it offers a huge potential for surprise and offensive action, even against militarily superior opponents. This builds on the ability to create ambiguity by silently operating in the grey areas of interfaces, while concealing or plausibly denying an actor's intent and role as a party to the conflict, combined with a limited use of force only as a last step. By following a long-term, indirect or masked 'salami tactics' approach or, conversely, by conducting rapid, unexpected offensive operations thus achieving a fait accompli, hybrid actors can create new sets of circumstances that are almost impossible to be changed afterwards without undue effort. Hence, the offensive power of hybrid warfare presents the defender with a particular challenge: being taken by surprise without even recognising that one is under hybrid attack until it is too late.

In the face of these developments, hybrid warfare becomes not only the war of choice for the small and poor, such as terrorists, North Korea or Iran. It may also become particularly attractive for larger powers, as they can pursue their political interests with little risk. Against this backdrop, the crux of meeting this challenge will be to identify and understand in due time its ever-changing, multiple and often disguised appearances, as well as the pattern and strategic rationale behind it. It will likely be impossible to respond appropriately unless the strategies and methods of a certain hybrid warfare actor are identified and understood comprehensively and early enough.

Consequently, awareness is the first precondition for addressing hybrid warfare challenges. A multi-domain situational awareness needs to cover the full spectrum of opponents' hybrid activities. Decision makers need to understand the entire set of domains, thus broadening considerably the spectrum of situational awareness requirements. The shifting focus opens up a need for new tools and technologies

to fully understand the operating environment, and thus to take valid decisions. Real-time analytics and anomaly detection will serve as elements to uncover hybrid operations. With sensors (Internet of Things), people (social media), systems (Logs), mobiles (locations), etc. generating continuous and/or event driven data, the capability of processing online data streams will be pivotal to a situational awareness, which alerts to certain actions, flags complex events or points out new developments.

While military means and the use of force play an important role in hybrid warfare, and in its respective campaigns – in contrast to military centric/conventional warfare – the strategic CoG of hybrid warfare is not primarily located in the military domain. This has consequences for political, civilian and military elites in democratic societies. The ability to constantly perform in-depth analyses of specific hybrid challenges, related actors and strategies will become a key capability in countering and responding to hybrid methods of warfare. A comprehensive understanding of hybrid warfare and a related education of judgment, not least to prevent overinterpretation and overreaction, are decisive.

Digital Challenges

Today the nation's power—militarily as economically—rests on data. Via data and communication networks, computers and automation come together in a new way with remotely connected robotics. In a world of constant connectivity, data is the new oil. And networks are the new oil rigs. Just as crude oil needs to be refined to create usable products like gasoline, data needs to be refined to deliver actionable information.

The backbone of the Information or Digital Age is the Internet, a global infrastructure for information transfer, a complex and hard to comprehend system of systems. Digital transformation has deeply affected all areas of society, including industry and economy, as well as governmental domains, such as defence and security.
Against this backdrop, armed forces have structured a new business

model on modern, interoperable, scalable and service-oriented information and communications technology (ICT). Rapidly increasing complex data volumes, and the capability to make their information actionable have become of decisive importance to military operations. Data may arrive on specialised secure military channels, or it may be so-called open intelligence gathered over the internet or media reports. The sheer diversity of platforms– airborne, satellite, submarine, surface ship, soldier-borne – generating and acquiring data is immense. Connectivity boosts the efficiency of the power instruments non-linearly. Appropriately employed ICT is nowadays decisive for the outcome of war and war-like operations. The cyber world offers a set of hardware and software systems, including data and information processing, globally available broadband data transmission at the speed of light, mass data storage, algorithms and artificial intelligence (AI), precision timing, databases with geo-data, and geolocation services.

The technologies of the digital age have moved us rapidly into the cyber space. Cyber is an abstract realm with its high-speed communication lines, data mountains and processing capabilities not easy to grasp and comprehend. We call it the virtual world as we cannot sense the occurrences in the web and the connected number crunching machines. To most of us the net evades our perceptiveness. We sense results of virtual world processes when they hit the real world often to our surprise or embarrassment.

The tremendous computing power and ubiquitous connectivity have become an everyday feature of our life. Powerful processing and storage devices and global infrastructures providing timing, geolocation and communication changed our political, societal and economic systems. It equally changed warfare. Information and communications technology (ICT) emerged as a key enabler for all human controlled processes. It has opened new ways to collect, store, manipulate, use and distribute data and information and to create knowledge. It even empowers non-military operations to achieve war like effects as demonstrated by the destruction of the centrifuges of the nuclear enrichment facility in Natanz/Iran by malign software in the first decade of this century. It provides access to information and enables influencing in-

dividuals, interest groups, and states on a global scale. ICT has become the underpinning of hybrid warfare.

Hybrid warfare happens in the real and in the virtual world. The real-world segment is in principal well observed and understood, while the virtual segment operates stealthy in the invisible world of computers and networks until showing effects in the real world, often to the surprise of an unprepared target.

Conventional warfare employs Industrial Age technologies, in which mechanical systems embody and deliver the military force. The Industrial Age has been shaped in particular by three revolutions in military affairs (RMAs), i.e. the emergence of disruptive technologies that overtake existing military concepts and capabilities and necessitate a rethinking of how, with what, and by whom war is waged (Wilson 2019, 3).

- RMA I is the method of war fought with combat vehicles and industrial production and it emerged out of the second half of World War I.
- RMA II is the method of war of the insurgent that emerged out of the Sino-Japanese war during the 1930s and led to the successful seizure of power by the Chinese Communist Party (CPP) in 1949.
- RMA III is the method of war via the use or threat of use of nuclear weapons and their long-range means of delivery—a dominating feature of the Cold War.

Currently, the most technologically dynamic method of war is RMA IV, i.e. the method of war fought through the use of silicon and all of the manifestations of the digital age including precision-guided munitions, active and passive sensors, cyberspace, and robotics. It covers the development of guided munitions, Command, Control, Communications, Computer technology, Intelligence (C4I).

The ICT developments of the last three decades have altered the way states pursue their military goals. In the predigital age, information

was difficult to collect and to manage. Hierarchically organized structures were the means of choice for information storage and management. This has been a slow system where political and military decisionmakers at the political-strategic and even at the operational level were often several days behind the actual situation in the battle. Today, states and armed forces all over the world have undergone a transformation process to capitalize on the enabling capabilities of the digital world. Concepts of Electronic and Information Warfare emerged and can be considered as a harbinger of hybrid operations.

In this context, the emergence of military technological competitors, such as China and Russia, constitutes a new strategic challenge to the West. China has developed and deployed its armed forces, with modern RMA-I techniques, and it is also exploiting the advances in RMA-IV. In view of this, NATO and the EU face the prospect that a near-peer continental power will soon be able to exploit the tools and techniques of RMA-IV. Against this backdrop, the Anti-Access / Area Denial (A2/AD) challenge has become a centrepiece of Western defence investment. Much of the U.S. response to China and Russia's improved A2/AD capabilities will manifest via the further development and exploitation of the tools and techniques of RMA-IV. This will include significant investments in long-range strike systems to provide large combat platforms with increased survivability and hitting power, enhanced missile defences, and a robust capacity to conduct offensive operations in space and cyberspace. Furthermore, the tools and techniques of nuclear weapons (RMA-III) may see a renaissance.

Meanwhile, RMA V is lurking around the corner, as the technological revolution unfolds (Thiele 2019, 6). Artificial intelligence, autonomous systems, ubiquitous sensors, advanced manufacturing, and quantum science is about to transform warfare radically. Emerging technologies will enable new battle networks of sensors and shooters to rapidly accelerate the process of detecting, targeting, and striking threats, what the military call the "kill chain." More incredible still, so-called brain-computer interface technology is already enabling human beings to control complicated systems, such as robotic prosthetics and even unmanned aircraft, with their neural signals alone (Ather-

ton 2019). Obviously, it is becoming possible for a human operator to control multiple drones simply by thinking of what they want those systems to do.

Hybrid Warfare will engage a creative mix of all these RMAs. In particular we must expect stealthy operations such as clandestine operations to influence, coerce, sabotage, and other actions. The information and communications technologies are the key enabler of clandestine operations as an element of hybrid warfare. As the advances of information technologies are faster than the development of mechanical systems in a broad sense, we should expect a shift towards virtual threats.

Dealing adequately with hybrid warfare in all relevant domains requires understanding the tools of hybrid warfare. This implies understanding the complexity of the digital world and the need to include the abstract cyberspace in our security thinking. Here systems of systems thinking is key as hybrid actors fuse military and non-military means. Hybrid warfare applies strategies that seek superiority by systemic capabilities to boost efficiency. ICT enables a systemic approach to combine military operations with various means to destabilize a state and polarise the society by employing diverse combinations of power instruments to target an adversarial society, economy, infrastructure, and the military and to collect information. These power instruments have two prime functions: inflict selective damage and support of decision making: Superior decisions on the own side and misguided decisions on the adversary's part. The power available to political, civilian and military decisionmakers and the quality of their decisions will ultimately decide the outcome of every contest.

We can expect hybrid warriors to develop models of their perceived targets and to use them to make an attack. Aggressors will find much of the information needed for the design of own tools openly available on the internet to include information about critical infrastructures, personal information from social media accounts, corporate data, and information about politics and administration. This increases NATO´s, the EU´s and member nations' vulnerability. This is why we need to model own vulnerabilities and design response functions, a

defence system in the virtual world. This requires high system engineering skills and a highly qualified team of engineers, computer scientists, psychologists, and social scientists. We need a new approach to safeguard our security, now and in the future (Theile, 1-6).

Trends and Technologies

While digital challenges pose enormous change requirements, the world is already rapidly moving towards a post-digital era (Accenture 2019, 5). Governmental and non-governmental organizations have made enormous strides to realize the benefits of new digital business models and processes. With every business and organization investing in digital technologies, the next disruption is coming as the power of cloud and artificial intelligence continue to advance. Combined with technologies such as distributed ledger, extended reality, and quantum computing, new technologies will reshape not only prosperity and security, but also relationships – man-machine, between individuals, an entire ecosystem.

Computers are becoming faster and ubiquitous. Machines are getting smaller and more powerful each day. Fundamental breakthroughs include robotics, nano- and biotechnology, artificial intelligence, distributed ledgers, sensor technology, and 5G. Additive manufacturing methods provide for prototypes, parts for weapons and vehicles. The enormous potential of artificial intelligence (AI) is playing an ever-important role. People are adopting new technology with alacrity: customers and employees, governmental officials and criminal actors. We can expect a broad spectrum of technologies to contribute to hybrid warfare and its objectives (Callinan 2019, 44). The further development and integration of artificial intelligence in conventional weapons platforms, and the robotization of battlefields will progress rapidly.

How far can we realistically look into the future? How far must we look into the future? Certainly, researching trends and upcoming disruptive technologies is indispensable. Yet the focus should be on shorter timelines than in the past.

Three lines of thought need to be explored in particular:

- Where is the development of disruptive technologies going, and how fast? Who is driving this development, and in whose interest is it?
- What are the strategic and military implications? What kind of capacities are needed and how are they to be procured and funded? What kind of training and education is needed? What are the implications for the nature of military command and control?
- What is the political and ethical impact of these disruptive technologies on our democratic systems? What is the impact on the political control of armed forces and parliamentary oversight? - on international law? - on the value of human control in regard to AI, etc.?

NATO and Europe are at a crossroads. Hybrid warfare is threatening member nations and NATO´s and the EU`s neighbourhood. Countering hybrid warfare requires the ability to protect vulnerable interfaces and to operate in their grey areas by adopting a truly comprehensive approach. Against the backdrop of hybrid attacks primarily on non-military CoGs, the importance of high professional (particularly also) civilian leadership, civil preparedness, an educated public, and an effective legal framework cannot be overstated.

As hybrid threats put peace and prosperity, social cohesion and security at risk, responses need to include a whole-of- government approach, a whole-of-society approach, as well as international cooperation and coordination. The interfaces between internal and external security are of particular relevance. It is high time for the NATO, EU and the member states to improve their common and comprehensive awareness and understanding of hybrid warfare and related strategies as a precondition for common and comprehensive action in defence and response.

The given technological revolution must be orchestrated, for technical and operational reasons, but also with a view to the fundamental values represented by NATO and EU member nations. Three dimensions need to be tackled.

Conceptually, strategy, concepts and concrete initiatives need to enable successfully resisting and fighting hybrid aggression, as new technologies are fundamentally challenging politics and society, economy and production, prosperity and democracy, security and defence. They should guide stakeholders towards increased resilience against hybrid shock and stress and also towards comprehensive active measures. Each nation and organisation has to develop its own understanding of the kind of hybrid threats/warfare that can be directed against it and is required to thoroughly familiarise itself with its own vulnerabilities. This applies also to NATO, and the EU. All are well advised to develop a common understanding of how to deal with hybrid threats/warfare, so as to pull in the same direction (Hagelstam 2018).

Technologically, the possibilities of the technological revolution need to be exploited, their misuse limited. As technology meets doctrine and organization, training and material, leadership and education, personnel and facilities this constitutes an enormous challenge and must be managed well. Disruptive innovation can lead to new opportunities, or exacerbate existing conflicts, it can promote prosperity, or strengthen radicalisation. This is precisely why this technological revolution must be orchestrated in such a way that all benefit: people and societies, security and defence. The overlap between military and civilian capabilities of the technology revolution can serve as an early indication about what we might see in future security challenges (APA 2019).

Organisationally, as the technology revolution unfolds, there is reason for urgency in orchestrating and accelerating innovation in Europe. It needs to invest not just more manpower and money, but also to push focussed research and thought to achieve innovation acceleration, thus promoting:

- Its own capabilities for enhancing situational awareness as the precondition for viable action when it comes to hybrid threats;
- C4I infrastructures, providing the backbone to act comprehensively with all available instruments of national and international power on all levels of escalation;
- Real-time analytics and anomaly detection as elements to uncover hybrid operations; and
- Edges of our security and defence networks, thus enabling superior network enabled capabilities.

Both, hybrid warfare and disruptive technology constitute serious challenges to NATO, the EU and member states. Meeting these calls indeed for a determined, holistic and collaborative approach. Open, democratic societies that lack strategic vigilance are particularly vulnerable to hybrid methods of warfare (Schmid 2019b).

References

Accenture. 2019. "The Post-Digital Era is Upon Us. Are you ready for what´s next? Accenture Technology Vision 2019." May 17. Accessed May 29, 2019. https://www.accenture.com/t20190201T224653Z__w__/us-en/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf.

Die Presse. 2019. "BMW-Chef: Kommende Jahre unklar - 10 oder 10.000 Elektroautos." January 20. Accessed May 29, 2019. https://diepresse.com/home/Economist/Wirtschaftsnachrichten/5565742/BMWChef_Kommende-Jahre-unklar-10-oder-10000-Elektroautos.

Atherton, Kelsey D. 2019. "In this league, drone races are won by brainwaves alone. C4ISRNET." April 26. Accessed May 29, 2019. https://www.c4isrnet.com/unmanned/2019/04/26/league-races-drones-by-brainwaves-alone/.

Martin Callinan et al. 2019. Defence and security R&D: A sovereign strategic advantage. Barton: ASPI. Accessed May 29, 2019. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-01/SR 133 Defence and security R%26D.pdf?utm_medium=email&utm_source=FYI&dm_i=1ZJN,63GYS,RBW1B5,NXX58,1.

Hagelstam, Axel and Kirsti Narinen. 2018. "Cooperation to counter hybrid threats." NATO Review, November 23. Accessed May 29, 2019. https://www.nato.int/docu/review/2018/Also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm.

Schmid, Johann. 2017a. "Konfliktfeld Ukraine: Hybride Schattenkriegführung und das ´Center of Gravity´ der Entscheidung." In Krieg im 21. Jahrhundert, edited by HansGeorg Ehrhart, 141–162. Baden-Baden: Nomos Verlag.

Schmid, Johann. 2017b. „Hybride Kriegführung in Vietnam – Strategie und das center of gravity der Entscheidung." Zeitschrift für Außen- und Sicherheitspolitik (ZFAS) 10, no. 3: 373–390. DOI: 10.1007/s12399-017-0659-4.

Schmid, Johann. 2019a. "The Hybrid Face of Warfare in the 21st Century." Maanpuolustus, March 7. Accessed May 29, 2019. https://www.maanpuolustus-lehti.fi/single-post/The-Hybrid-Face-of-Warfare-in-the-21st-Century.

Schmid, Johann. 2019b. "Hybrid Warfare – a very short introduction." COI S&D Conception Paper. Helsinki. ISBN: 978-952-7282-20-5.

Theile, Burkhard. 2019. "Hybrid Warfare in the 21st Century. Information and Communications Technology as Key Enabler." May 22, Berlin.

Thiele, Ralph. 2019. "Hybrid Warfare - Future & Technologies" (HYFUTEC). May 14. Inspiration Paper no. 2. Helsinki.

Wilson, Peter. 2019. "The Eurasian Four Ring Circus and the

Long War Against Salafist Jihadism Rapidly Emerging Military Technological Trends and Capabilities". RAND Arroyo Center, May 17.