Technology and Resilience in the Munich Security Conference 2020 Discussions

Ralph D. Thiele

February 2020

Summary

The future prosperity and security of NATO, the European Union and its member states will be determined by the purposeful and decisive use of new technologies. Building on modern technological capabilities, an increasing number of states is relying on forms of deployment designed to prevent a large-scale conflict. They choose strategies and approaches with which Western democracies have so far been unable to cope adequately. Some speakers at the Munich Security Conference have highlighted that new technologies and digitalisation are not just the price of admission to participate competently and self-determinedly in economic and social networks today. They are also increasingly dominating core issues of security policy. President Macron stated "If we do not build our own champions in all areas - digital, artificial intelligence - our decisions will be dictated by others."

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Analysis

Destructive Dynamics

The 56th Munich Security Conference started on 14 February with a thoughtful speech by the German Federal President Steinmeier. He urgently warned against an increasingly destructive dynamic in world politics and requested: "Germany must contribute more to the security of Europe, including financially." German Minister of Defence Kramp-Karrenbauer, just like French President Macron, believes that Europe and Germany have a duty to develop a greater will to act.

China and Russia were at the centre of international criticism. Despite all the well-founded concern vis-à-vis countries such as Russia and China, Iran and North Korea - in NATO, the European Union and its member states, nobody seriously expects any of these states to prepare for a major war. However, this does not rule out the possibility of longer, less intense or even shorter, highly intensive aggression or attacks on companies and critical infrastructures. In fact, in many regions of the world the use of military force as a means of politics is on the rise; not only as a deterrent, but also as a means to change established power structures or as a lever to enforce other national goals and interests.

Below the Threshold of War

With the help of modern technological capabilities, many states are relying specifically on forms of deployment designed to prevent a large-scale conflict. They choose strategies and approaches with which Western democracies have so far been unable to cope adequately. The basic thinking in Russia, China, North Korea and Iran, for example, assumes that national goals cannot be achieved in conflicts with Western opponents if their own strategic approaches correspond to Western expectations and plans. Against this background, hybrid approaches have developed that make particular use of the information space.

Hybrid threats are not a completely new phenomenon, but against the background of powerful technologies they are a novel, demanding challenge that combines overt and covert military and non-military means and that should and can seriously hamper joint responses by Allies and partners. Hybrid actors seek to deceive the attacked state as well as the international community as a whole. New, disruptive technologies magnify the impact of hybrid actions as amplifiers or even as multipliers. It is difficult for those under attack to perceive attacks as such, to classify them correctly and to initiate appropriate countermeasures.

Inner Decay

Hybrid aggressions focus primarily on the cognitive and cyber-domain. They aim at the inner decay of the opponent. Traditional defence concepts and doctrines have not been able to meet such challenges sufficiently. In the Ukrainian conflict, Russia has demonstrated the seamless orchestration of military and non-military instruments: military threat scenarios beyond the Ukrainian border, deployment of paramilitary units without a national emblem, cyber-attacks against Ukrainian infrastructure and support for the "separatists" with military equipment. Mass communication channels were used to spread propaganda and false information on a large scale. Russia has perfected the interaction of editorial and social media.

Valery Gerasimov, the Russian Chief of General Staff, pointed out in an essay in 2017 that in the operational concepts of leading states, the conquest of information superiority will foreseeably become an indispensable prerequisite for successful operations. Media and social networks are decisive instruments in this context. In a hybrid conflict, mass communication channels are widely used to spread propaganda and false information. Non-military forms and combat equipment acquire a highly effective and sometimes violent nature through the use of unprecedented technological developments. Through a clever strategy, a cumulative systemic effect can be achieved, leading to a collapse of the state in the areas of energy, banking, economy, and information.

The Virtual Challenge

The discussions in Munich underlined that NATO and the European Union have not yet been able to cope with the leap from the analogue to the digital world. The technologies of the digital age have led us surprisingly quickly into virtual space. Powerful processing and storage devices and global information and communication infrastructures enable timely planning, geolocation and comprehensive communication, with far-reaching consequences for politics, business, society and the private life of almost every individual. Since the end of the last century, the global economy has been in a phase of transition from the industrial age to the information age. The creation of value follows technology. The economy follows value creation. Politics, which includes the legal system, follows the economy.

Cyber-space provides access to a wealth of information. Its processes make it possible to create value or cause damage even without the use of material. With the Internet as its backbone, it is populated by applications such as the World Wide Web, e-mail, cloud services or the Internet of Things. Other products and services such as global navigation satellite systems, sensors, software platforms, algorithms and artificial intelligence offer enormous potential for value creation, likewise for destruction or even imposed control.

The backbone of the digital age is the Internet, a global infrastructure for the transfer of information, a complex system of systems. Via data and communication networks, computers and automation are coming together with remote-controlled robotics in a new way. Industry and the armed forces use the same available technologies. Currently, the real and virtual worlds are converging to form the Internet of Things. This connectivity enables states and individuals to act across all elements of national power: diplomacy, information, military and economy.

Data is the New Oil

Information and communication technologies (ICT) have opened up new possibilities for collecting, storing, manipulating, using and distributing data and information, also for creating knowledge. They are proving to be a key factor in all human-controlled processes. They provide access to information and enable individuals, interest groups, companies and governments to exert global influence. In a world of constant connectivity, data is the new oil. Networks are the new oil platforms. Just as crude oil must be refined to produce useful products such as gasoline, data must be refined to provide useful information.

Against this background, the number of governmental and non-governmental, even virtual actors - e.g. trolls - in the cyber and information space is growing with enormous dynamism. Digital industrial espionage and cybercrime have long been part of everyday life. Yet the boundaries between simple crime on the net, state-controlled cyber espionage or hybrid attacks are not easy to discern.

In military terms, cyberspace enables global communication and control of armed forces and operations as well as the functioning of a globally distributed logistics system, without which modern military operations would not be possible. The use of information space is a multiplier for success in operations. The ICT developments of the last two decades, however, also enable war-like effects through non-military operations, such as the destruction of the centrifuges of the nuclear enrichment plant in Natanz/Iran by malicious software.

Accordingly, the armed forces of many countries are undergoing a process of change in order to capitalize on the opportunities offered by the digital world. Terms such as "network centric operations " and "force transformation" stand for this development.

Difficult to Grasp

Concepts of electronic and information warfare have emerged. They pave the way for future hybrid scenarios. They combine capabilities of two different epochs, achievements of the industrial age and the information age.

The real-world segment is the conventional military power. The physical dimension of hybrid warfare is well understood by many decision-makers and actors in the system, because conventional warfare makes extensive use of industrial age technologies.

In contrast, the virtual world segment is often difficult to understand, even for information specialists. Operations in the invisible world of computers and networks usually reveal their effects in the real world only at the end of the process and often to the surprise of an unprepared target. This abstract realm with its high-speed communication lines, data mountains and processing capabilities requires a systemic approach that links the material and virtual realms.

Invest in New Technologies

Anyone who followed the arguments of the speakers in Munich closely was able to see that new technologies and digitalisation are not just the price of admission to participate competently and self-determinedly in economic and social networks today. They are also increasingly dominating core issues of security policy.

At the Munich Security Conference, U.S. Secretary of Defense Esper pointed out not least for this reason that China was stealing Western intellectual property, intimidating smaller neighbours and thus becoming a growing threat to the world order. The People's Republic of China wants to complete its military modernization by 2035, and by 2049 it wants to dominate Asia as the "outstanding global military power," Esper said. Washington has therefore called on its allies to take a tougher stance against Beijing and to resist China's attempts to expand its influence in Europe with 5G technology, as it poses a particular security threat.

At the Munich Security Conference, the discussion about the technology was rarely - if ever - so closely linked to the discussion about the sovereignty of nation states. France's President Macron had already made it clear last year that "the battle we are fighting is a battle of sovereignty [...]. If we do not build our own champions in all areas - digital, artificial intelligence - our decisions will be dictated by others." Against this background, Europe sees its economic position increasingly "challenged by other global powers".

President Macron Calls for a Strong Europe

President Macron again and emphatically underlined this argumentation in this year. In Munich he called for a strong Europe. With reference to international economic and security policy developments and also Moscow's aggressive cyber-attacks and campaigns in online networks, he called for Europe to find sovereign answers not only in climate protection, but also in the development of the new mobile phone standard 5G or artificial intelligence. He called for significantly more public investment in the areas of technology and security. Only in this way could the European Union assert its sovereignty in the future.

Europe is increasingly losing ground as a location for leading companies in the world. Today, the USA is the leader in many technology sectors. China is positioning itself in the slipstream of the USA. This is reflected in the rise of Chinese technology giants such as Huawei, Alibaba, Baidu, Tencent and Xiaomi. China's catch-up process is impressive. The country has almost tripled its share of R&D spending on technology and hardware equipment between 2012 and 2019. However, the biggest challenge for Europe lies in its own structural disadvantages compared with China and the USA. Fragmented markets, including capital markets, and paralysing governance - e.g. with regard to taxation - have so far stood in the way of a rapid upturn.

Against this background, it is good news that Europe is currently preparing for the upcoming battle for industrial data. Disturbed by the dominance of American and Chinese technology companies such as Google, Amazon and Huawei, the European Union is leaving behind the "laissez-faire" attitude of the early 2000s and increasing regulatory pressure to protect its companies.

The Main Battlefield will be Europe

"The battle for industrial data starts now, and the main battlefield will be Europe," stated Thierry Breton, EU Commissioner for the Internal Market, at the Munich Security Conference. The EU has a unique opportunity to win the next phase of the digital revolution, which focuses on the collection, management and analysis of data from industrial sectors such as factories, transport, energy and healthcare. "Most of the industrial value chain, from large corporations to SMEs, is now located in Europe. That is why all eyes are on Europe," he added.

The 5G implementation, which was the subject of heated debate in Munich, is an example of how the economic and security policy significance of new technologies has been underestimated to date. Once the technology is mature, 5G will become the communicative backbone of system-critical communication processes. While the early generations of cyber-attacks were aimed at hacking databases, extortion or the theft of intellectual property, today there is much more at stake. Nation-state actors and their representatives can gain a foothold in the critical infrastructure of a target state and create attack platforms there, from where they can strike on demand.

5G will support critical use cases - from industrial automation to public safety and security services to support utilities or connected cars. As such, 5G-enabled - and/or dependent - government networks, utilities, transportation networks, health and other services will create new critical infrastructures that must be relied upon. Although rapid implementation of 5G is important, the availability, confidentiality and integrity of information on the network is even more important.

5G networks will be cloud-based, i.e. their infrastructure will consist of interconnected data centres or clouds. 5G has the potential to become a basic technology of the stature of steam engines, electricity or artificial intelligence. The technology will drastically change societies through its impact on already existing economic and social structures. With Ericsson and Nokia, there are two strong European players in 5G. As you can hear, this was one of the important topics discussed at the side-lines in Munich.

Resilience and Defence

In recent years, Russia, China and other states have not only modernized their armed forces, but in parallel have also developed the hybrid capabilities of their instruments of power in an impressive fashion. Russia's aggressions in Ukraine and Georgia, or China's activities in the South and East China Sea, show that the combination of limited political and military objectives in conjunction with low-intensity hybrid warfare currently leaves even the United States with few opportunities to actively support international partners and friends under pressure from powerful neighbours.

Hybrid aggression uses ambiguity. It operates in grey areas and targets the vulnerabilities of societies, their economies and infrastructures. In the era of "fake news", hybrid approaches can trigger unrest and protest movements through the use of new media. The use of the power of the Internet and social media serves as a powerful multiplier for the dissemination of propaganda and terror, influencing political outcomes and even enabling the recruitment of terrorists, as the Islamic state demonstrated. By undermining people's trust in the state and the ability of those in power to ensure its functioning and prosperity, the hybrid aggressor fights the target of the attack from both inside and outside. In the "ideal case", the attacked state implodes before it can defend itself.

NATO and the EU are entering unchartered and challenging territory in the defence against hybrid threats. Hybrid threats pose new and comprehensive challenges to all political, economic and social stakeholders, as they are designed to pursue political and military objectives without reaching a level of violence that would justify a large-scale military response by Allies or organisations such as NATO and the European Union.

The Gap Between Internal and External Security Requirements

Up to now, the political culture and bureaucratic structures and processes of Western democracies are not particularly well suited to bridging the gap between what have traditionally been constructed as "internal" and "external" security challenges.

International cooperation and solidarity are, however, an important basis for understanding new threats, improving deterrence and building resilience and defence. NATO and the EU must work on this. NATO and its member states should concentrate on improving their military capabilities in order to keep pace with potential opponents. Wolfgang Ischinger, the former German top diplomat who has been chairing the Munich Security Conference since 2009, rightly remarked: "The military should be one instrument among several in the toolbox. Without convincing military means, diplomacy would often degenerate into a "rhetorical shell". At the same time, he does not spare the Bundeswehr from his criticism. He said that Germany's military strength was too weak compared to its political weight in Europe. "I think the neighbours would all be happy, if Germany had at least used as many planes against the Islamic state as Denmark. Because we haven't used a single one that shoots. We've only taken photos."

Moreover, Europe urgently needs its own approach to small and large-scale innovation, building on its unique strengths and meeting its unique challenges. This requires identifying and funding useful programmes/ projects in the field of applied research, technology and product development. It became very clear in Munich: The future prosperity and security of NATO, the European Union and its member states will be determined by the purposeful and decisive use of new technologies.

***

Remarks: The opinions expressed in this contribution are those of the author.

About the Author of this Issue

Ralph D. Thiele, born in 1953, is President of EuroDefense, Germany, Managing Director StratByrd Consulting, Germany, Chairman Political-Military Society, Germany and Member Advisory Board German Employers Association, Wiesbaden. He is a retired Colonel, held in his 40-year military career in the German Armed Forces key national and international positions. He

- Commanded troops up to the battalion level;
- Developed concepts and capability requirements in the Ministry of Defence;
- Drafted speeches and policy papers for Federal Presidents, Ministers of Defence, Major NATO Commanders and Service Chiefs;
- Drove educational innovation at the German Armed Forces Command and Staff College (Director Faculty) and at the NATO Defense College (Chief of Staff);
- Shaped the Bundeswehr's path towards network enabled capabilities (Commander Bundeswehr Transformation Command).

In his honorary and business functions he advices on Defence Innovation and Cyber issues in times of digital transformation. He has been frequently consulting, publishing and lecturing in Europe, America and Asia.

Ralph D. Thiele is also a member of the ISPSW Speaker Management Team. Further information at ISPSW website: http://www.ispsw.com/en/speaker-management/

Ralph D. Thiele