Turning Disruptive Technologies into Superior Capabilities

Ralph THIELE
President EuroDefense Germany
ralph.thiele@stratbyrd.de

Abstract: Several governmental and non-governmental actors have exploited current conceptual and technological gaps and resulting capability gaps of the West. They are making skilful use of inexpensive, commercially available technologies to further their own ambitions and power objectives. This development opens the floodgates to coercion and blackmail thus putting NATO and EU cohesion and solidarity at risk. As neither the European Union nor the USA will be able to win the technological competition on their own, the transatlantic partners should meet Russia's technological challenges and China's technological rise together.

Keywords: Geostrategic Competition, Cyber, Disruptive Technologies, Artificial Intelligence, Quantum, Space, Autonomous Systems, Drones, Hybrid Warfare, 5G.

COMPETITION AND HYBRID THREATS

From the Eastern Atlantic to the Middle East, the Caucasus, Russia, and the Arctic, Europe is spanned by an arc of crisis. The European region is home to some of the most important global shipping lanes, energy resources, and trade centers. At the same time, the economic center of European prosperity is moving towards Asia. The security challenges in and for Europe arise from a broad spectrum of geostrategic competition, including multiple hybrid threat situations, attacks on businesses and critical infrastructure, and the threat of prolonged, low-intensity or shorter, high-intensity conflicts (Thiele 2021).

Geostrategic competition is global in scope. The boundaries between civil and military competition are fluid. Russia and China in particular integrate civil and military competition at every level, including the development of their international trade, investment, national technology base, and political and diplomatic activities. Core challenges to European security include the continuing risk of Russian aggression against Eastern EU or NATO states, Russian activity in the Arctic, the growing Russian presence in the Mediterranean, and Russian efforts to destabilize Western cohesion. Hybrid scenarios are clearly gaining in importance as the preferred form of confrontation (Arcesati & Rasser, 2020).

In the meantime, China has also become the target of security concerns of the European Union and NATO. China is a geostrategic competitor that intimidates its immediate neighbors with its predatory economic policies while militarizing disputed territories in the South China Sea. Moreso, i+ts arm has long reached into the heart of Europe, felt in transportation, financial markets, investment and cutting-edge technologies, cyberspace, organized crime, and even misleading propaganda campaigns. China is trying to assert its own ideological, economic and military power ambitions through technological leadership (Arcesati & Rasser, 2020). This approach implicitly aims at a deterioration of the economic competitiveness of a European

Union that follows market rules, while China supports its innovation with market-distorting subsidies, protectionism or even the theft of intellectual property as well as forced technology transfer (Smith et al., 2020). Like Russia, China is using new, disruptive dual-use technologies as the key to advancing the capabilities of its own armed forces.

Along with Russia and China, Iran remains a major challenge to stability in the European neighborhood. It unabashedly promotes violence and terror in the Middle East. This not only threatens peace and stability in the region, but the reach of the terrorist groups extends to the whole of Europe. In addition, Turkey is pursuing a problematic foreign and security policy course.

The dynamics of this geostrategic environment present armed forces of EU and NATO Member States with a variety of demanding requirements. They must be able to respond at short notice and, if necessary, over long distances. At the same time, they must be able to maintain long-term operational commitments and respond competently to hybrid threats. In doing so, they will encounter both tried-and-tested military technology and high-end technologies. Last but not least, they must prepare for possible conflicts with major powers capable of deploying numerous and diverse modern weapon systems across the spectrum of conflict, including electronic warfare assets and hypersonic weapon delivery systems.

TECHNOLOGICAL DRIVERS

The Western allies on both sides of the Atlantic have been at the forefront of technological innovation for many decades. In particular, the state-dominated defense technology base was unparalleled. Today, concern is well founded. Technological innovation is booming with great momentum outside the West, leading to a shift of value creation toward Asia. Moreover, in key technologies - with a few exceptions, such as nuclear, hypersonic, and electronic warfare - the commercial sector now drives technology areas critical to the success of armed forces, including 5G, autonomous systems, biotechnology, cyber, augmented reality, artificial intelligence, laser technologies, quantum technologies, robotics, and space technologies (DoD, 2018). The required spin-off is not yet well organized in terms of defense technologies. Judgment in this regard is still on shaky ground, leading to inadequate mission concepts and requirements documentation. Moreover, the procurement process is much too slow for the given innovation dynamics.

The current renaissance of nuclear weapons increases the scope of opponents for intimidation and blackmail. At present, it is completely unclear whether and, above all, how NATO, for example, will close the emerging nuclear gap vis-à-vis Russia in a way that can continue to ensure "extended deterrence" by the potential of the USA for Europe in the future (Olshausen 2020).

While digital challenges are already placing enormous challenges on politics and society, business and the armed forces, the avantgarde of innovation is already setting course for a post-digital era (Accenture 2019). Disruptive and radically improved technologies will enable networks of sensors and effectors to vastly accelerate the cycle of target detection, evaluation, decision-making and action. They will radically change warfare once again (Thiele 2019a).

As per the Hybrid COE project Hybrid Warfare: Future & Technologies (Thiele 2020) among the technologies relevant to prosperity, security and defense, some stand out:

ARTIFICIAL INTELLIGENCE AS INNOVATION DRIVER

First and foremost is artificial intelligence (AI) - a key technology of digitalization (Harhoff et al., 2018). It is a driver and multiplier of technological developments. (PWC). AI unlocks the full potential of data, makes existing products and systems smarter, and it learns and adapts.

Artificial intelligence builds on computer power, data to learn from, and human talent to shape how systems work. Its particular potential lies in analyzing large amounts of data, optimizing processes, supporting decision-making processes at critical target engagement times, for example, and condensing an all-domain situational awareness (Schmidt & Work, 2019). It enables an optimal allocation of scarce resources to targets and tasks and initiates an immediate reallocation if necessary. Defense and security organizations use machine learning to permanently update knowledge about the operational environment. AI-driven autonomous tools become *useful teammates* for humans. Thanks to AI, human-machine teams are able to perform their tasks in a superior manner (Masuhr).

AI supports military applications from the tactical to the strategic level, in particular by analyzing Big Data, optimizing processes and supporting planning. AI-enabled systems are multitasking and can collect, categorize and transmit data, signals, images and videos collected by drones according to the requirements of multiple users. This greatly accelerates decision-making processes and leads to cross-domain situational awareness that can leverage any available data source in a structured manner. AI-enabled technologies reduce combat response times, improve force protection, maintenance and logistics (Horowitz). They enable the EU and NATO to achieve military superiority by leveraging data, i.e., fusing data into relevant information and actionable knowledge.

AI offers a wide range of capabilities to relieve soldiers of routine tasks, in addition to providing tremendous new complementary capabilities. AI technologies will:

- Support special operations forces (SOF), in language translation, scanning captured laptops and cell phones, visualizing tactical information, overcoming electromagnetic interference, or detecting emerging electromagnetic threats;
- Improve the cross-domain intelligence-guidance-action composite;
- Significantly upgrade decision support and course-of-action analysis (COA) using virtual teammates;
- Accelerate mission tempo and target engagement, and help find the best allocation of scarce resources. Pattern recognition and reasoning algorithms can combine available information into coherent suggestions;
- Drive the development and scaling of kinetic and non-kinetic weapons;
- Improve the visualization of available data and information;
- Generate new capabilities for predictive maintenance and autonomous transportation;
- Improve war gaming, modeling & simulation, education and training, and more.

The bottom line now is to rapidly build AI expertise in the Armed Forces so that it can then be fleshed out in specific applications. The Pentagon is taking an interesting approach with the Joint Artificial Intelligence Center (JAIC), which sees itself as a central service centre for all military users who want to apply AI (Eversden 2021). The armed forces in the USA can use JAIC tools, models and software to develop their own programs. It offers a wide range of services for this purpose.

TECHNOLOGIES OF THE MOMENT

The technologies of the moment are the fifth generation of mobile networks (5G) and space technologies, because their quite revolutionary implementation is already in the roll-out phase and therefore must be acted upon quickly and with overview.

The fifth generation of mobile networks is groundbreaking and new. It is the catalyst for further digitization and the resulting economic and social progress. Only with it will computationally intensive technologies such as artificial intelligence and quantum applications, facial recognition and cryptography also become usable with mobile devices. With 5G, the promise of the millennium will come true: Power to the Edge! The superfast 5G networks will drive the EU's economic progress, but also strengthen its security capabilities. Everyone will benefit from 5G.

Providers can dramatically expand their services to consumers based on 5G. This will benefit video streaming, smart homes, smart cities, autonomous driving, aircraft and ships, industrial applications, the Internet of Things and advanced data analytics. Not only speed, but also latency, capacity, power consumption and the number of supported connections will improve exponentially. This will enable real-time command and control applications, the transmission of sensor data collected by threats from operational areas to analytics centers around the world, and the use of services such as Extended Reality and Tactical Internet during missions.

Not without problems: 5G reaches critical processes. Its network properties, combined with the foreseeable multitude of applications, open up a wide range of gateways for malicious actors. This is already ensured by the large role that software plays in the 5G infrastructure (NIS 2019). The deep, symbiotic connection of 5G networks with government and administration, supply and transport networks, business and society generate new critical infrastructures, and thus prime targets for hybrid competitors and opponents (European Commission 2019).

Space technologies offer a highly innovative environment as an essential part of the digitalization of industry and armed forces. Over 80 countries have now entered the global space industry. They value space as a strategic industry with a highly technical workforce and spin-off effects for technology and economic growth. About 75 percent of the space industry's revenues are commercial (Ross 2019).

Space applications are both a prerequisite and an important driver for future technologies such as 5G, additive manufacturing, autonomous systems, AI, IoT and many others.

Satellites are getting smaller and cheaper; so it is getting easier and cheaper to put satellites into space; ground stations are evolving into service operations; ordering and receiving imagery is becoming more streamlined; imaging is moving to the cloud; venture capital is fueling entrepreneurship; new business models are driving a growing market. Satellites have long been part of a critical infrastructure that enables television, telecommunications, Internet of Things (IoT), commerce and financial networks, security and armed forces to function.

Currently, an almost revolutionary variety of satellites are taking off into space, especially low- and medium-orbit, digital-capable, largely interference-resistant, highly flexible in operation, with enormous bandwidths and low latency. SpaceX's Starlink program in particular shows how it is done. Every month, Elon Musk is currently launching up to 60 Starlink satellites into orbit simultaneously with the Falcon 9 launch system - already 955 in total by the end of 2020. The current license is for 12,000 satellites in low orbit. The application for another 30,000 has been filed. OneWeb and Kuiper (Amazon) are planning on a comparable scale. SpaceX, by the way, is putting additional satellites into low Earth orbit on behalf of the Pentagon, which will be able to transmit targeting information to fighter jets, track hypersonic weapons, and link sensors and effectors via a mesh network in orbit.

Unhindered access to space - and the freedom to maneuver there - is critical for the European Union and NATO (Thiele 2019b). Their military strength rests in large part on space-based Command, Control. Communication, Computer, Intelligence, Surveillance, Reconnaissance, timing and navigation. Emerging quantum technologies - including space-based sensors and secure communications and data processing based on quantum encryption - will add to the existing trend. Competitors and opponents understand this. Space has long been their focus of attack to weaken Western command and information systems.

Russian and Chinese satellites have repeatedly demonstrated their capabilities for precise maneuvers in space. These enable, for example, the repair of satellites in space, but also provide the capability to damage or destroy satellites of opponents without kinetic impact (DIA 2019). Anti-satellite (ASAT) capabilities using ground-based missiles remain a particular threat. China, Russia, as well as a number of other nations occasionally demonstrate their ASAT capability - including India, which tested its first ASAT missile in March 2019.

Space infrastructure is particularly vulnerable to hybrid threats, such as espionage or service disruption. The challenges ahead affect both world space and the cyber domain. Actors can use offensive cyberspace capabilities and other hybrid means to enable a range of reversible to non-reversible effects against space systems. In particular, hybrid warfare allows for the diffusion of opponents' SSA via information operations, i.e. electronic warfare, and cyber operations. In fact, upcoming challenges cross-cut space and cyber domains. Ground-based space infrastructure is particular vulnerable to cyber-attacks. There are plenty of access points which can be attacked – including the antennae on the satellites, the ground stations, and the earth-based user terminals. Such attacks range from stealing data to sending forged or corrupted data, from exploiting the physical vulnerabilities of a ground site to electronic warfare, to disrupting the connection between the space segment and the operator and completely shutting down all satellite operations (DIA 2019).

CYBER EVERYWHERE

Nothing works without cyber anymore. Today, cyberspace is at the center of almost all central social, economic, industrial and military fields of action. Information and communication technologies help to control a highly technical, complex world. At the same time, they enable theft, dysfunction and destruction.

Cyber space is constituted by combinations 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, data banks with geodata and geolocation services. As a dynamic system of systems, the underlying technologies and algorithms are developing previously unimaginable capabilities. Associated functions operate in the virtual world, elude the conscious perception of humans and only become noticeable through their effects in the real world.

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

Militarily, cyberspace enables global command, information, and control of military operations, as well as the operation of a globally distributed logistics system without which these operations would not be possible. Intelligence agencies, commanders, and ordinary soldiers alike benefit from the sustained flow of information, some of which is extraordinarily detailed. The use of the information space is a key multiplier for success in operations. The highly networked military platforms and weapon systems of high-tech armed forces also depend on the use of information and communication systems. Networking and the resulting constant availability of updated data and information accelerate decision-making processes. Accordingly, the availability, confidentiality and integrity of information are indispensable for military decision-making processes.

Processes can be orchestrated in a groundbreaking way via cyberspace. The vertical integration of all processes - the continuous cycle from situation awareness, mission planning, resource management to the mission itself and mission evaluation - revolutionizes the planning and operational management of armed forces. The organization's process levels - including task forces assembled on an order-by-order basis - are continuously linked to one another and can be constantly re-aligned on the basis of the most up-to-date process data.

Cyber enables the disruption of these processes and is at the same time indispensable for the fight against these disruptions. The number of state and non-state actors, including virtual ones, in the cyber and information space is growing at a breathtaking rate. Digital industrial espionage and cybercrime have long been part of everyday life. But the boundaries between simple online crime and state-controlled cyber espionage, between terrorist actions and state-controlled hybrid aggression are not easy to discern. For this reason, attribution and sanctioning have also been difficult up to now.

In this context, the European Union and NATO are focusing their attention in particular on Russia and China. Unlike the West, their objectives and activities are based on a broad understanding of information warfare that views information operations, electronic warfare (EW), and cyber operations as an interrelated continuum. In an overarching, orchestrated approach, their core purpose is to disrupt, deceive, and confuse decision-makers of adversary forces at all levels through a combination of cyber, information, and EW capabilities. The remarkable technological advances both states have made in electronic warfare enable their forces to disrupt, disengage, and degrade critical EU/NATO capabilities where appropriate.

The use of massed virtual agents enabled by AI makes it possible to roll out these concepts down to the individual level. Virtual and human analysts examine the vulnerabilities of target individuals and objects, respectively. The amount and quality of accessible information on social networking sites is rich. For example, the information available on social media can be used to create target profiles; sensors and microtargeting can then spy on targets through a selection and surveillance system and neutralize them if necessary.

A cyberattack, remarkable in its scale - the consequences of which cannot yet be assessed - attributed to Russia became known in mid-December 2020. The breach, which hijacked widely used software from the US software manufacturer SolarWinds Inc., has exposed the profound vulnerability of civilian government networks and the limitations of efforts to detect threats. Apparently for a long time, masses of Trojans from a Russian hacker group were infiltrated via the update servers of SolarWinds. Thousands of companies, authorities and organizations worldwide have been affected. According to reports in the New York Times (Sanger et al 2021), in the U.S. alone, the attackers have gained access to more than 250 federal agencies, companies that operate critical infrastructure and U.S. armed forces facilities, including research institutions that are developing new generations of nuclear weapons. In Germany, the Federal Ministry of Transport and Digital Infrastructure, the Federal Criminal Police Office, the Federal Office for Information Security and the Federal IT Service Provider (ITZ Bund), among others, use the affected Orion IT monitoring and management software from SolarWinds. In addition to espionage, the aim of the operation is also likely to have been to set up "backdoor" access points to the IT networks of the affected institutions. In sum, the cyberattack has highlighted the need to strengthen digital infrastructure and digital defenses, as these touch upon every part of the public and even the private sector (Gould 2021).

AUTONOMOUS COMPANIONS

For a long time now, the potential of autonomous systems, including robots and cyber-robots, unmanned vehicles, flight systems, ships, submarines and devices, has been growing with great momentum. The U.S. Air Force's future long-range fighter, which will replace the B-2 stealth bomber, will be able to operate both with and without a crew. Unmanned trucks and other utility vehicles have been developed to perform *boring and dangerous* tasks on the battlefield.

Technologies such as artificial intelligence, machine learning and Big Data, sensors, robotics and computers are enabling the development of a whole new class of systems. Other drivers include new materials and designs for improved efficiency and extended capabilities, such as longer ranges with powerful sensors, electromagnetic or kinetic agents. Biomimicry - incorporating animal characteristics into the design of threats and platforms - is a growing area of research in the context of autonomous systems.

The capability of autonomous systems relies primarily on software. AI supports the spectrum from semi-autonomous to fully autonomous systems (Burke 2020). It enables autonomous systems to make sophisticated decisions, to self-direct as an increasingly indispensable partner in complex human-machine teams, where virtual partners can contribute analysis, advice and courses of action very quickly (NATO 2020). Human-machine teams (MMT) are foreseeably becoming a critical capability for future military operations.

In particular, the advent of low-cost drones is enabling the mass deployment of autonomous systems, even entire drone swarms (Hruska 2018). Many armed forces, companies, even criminal and irregular actors such as terrorists now have unmanned systems in their inventories - systems that crawl, swim, and fly, used in mine disposal, surveillance, and fire support. What the use of intelligent and autonomous systems can mean for critical infrastructure and military operations was brought home to the world by the Sept. 14, 2019, airstrikes on oil facilities in Abqaiq and Churais in Saudi Arabia. The 18 drones used had an estimated purchase price of around €14,000 each. The attack inflicted such severe damage on Saudi Arabia's oil industry that its production had to be cut in half. The effect reached as far as European gas stations.

Drones are also shaping operations in other areas of the conflict spectrum. In the current civil wars in Syria and Libya, for example, the superiority of offensively deployed, low-cost autonomous systems over first-class, high-priced Russian air defense systems has been demonstrated in combination with good reconnaissance and electronic warfare: the offensive wins (Parachini & Wilson 2020).

Turkey has now positioned itself as one of the world's largest producers of armed drones and unmanned combat aerial vehicles (UCAVs) (Rocess 2020). It is using its drones with great success in northern Syria to destroy tanks, armored vehicles and artillery. In the conflict between Azerbaijan and Armenia, the same picture emerged. Wherever Azerbaijan's drones were able to move freely, because Armenia had no jammers as well as other means of electronic warfare to interrupt control signals, Armenian tanks, armored vehicles, artillery and radar stations were easy targets. The message: unmanned combat drones have a war-decisive role, providing inexpensive decisive reconnaissance, armor-piercing firepower, and indispensable fire protection for friendly forces (Gressel 2020).

In addition to physically intelligent things, disembodied cyber robots are spreading in the meantime across land, air, sea, world and cyber space. Some of them protect communications and information. Others gather information and knowledge. AI-driven cyber-attacks leverage malware's ability to self-propagate through a series of autonomous decisions and intelligently adapt to the parameters of infected systems. On the defensive, cyber robots can detect what is normal in their networks and thus respond early and autonomously to unknown threats. They protect technical systems and communication networks against attacks, e.g., by electronic warfare. They check information for facts and falsifications, filter and fuse them with a view to a realistic, comprehensive, action-oriented situation picture.

THE NEXT WAVE OF DISRUPTION

Quantum science promises the next big wave of disruption within the next two decades (NATO 2020). Quantum physics research has turned established notions of the fundamental laws of nature on their heads. With it comes enormous technological advances in areas such as computer science, sensors and metrology, simulations, cryptography and telecommunications. Quantum systems can be used with the highest precision to measure physical quantities such as pressure, temperature, position, time, speed, acceleration, electric and magnetic fields, or gravity.

Quantum physics is foreseeably generating unique new capabilities. But it also acts as an accelerator for existing technologies such as nano-, bio-, cyber-, and encryption technologies. New computer architectures and the parallelization of computing operations enable the processing and analysis of "Big Data", e.g. through pattern recognition based on artificial neural networks. This leads to better search algorithms and faster computations for a wide range of applications.

Defense and national security are among the first areas to use new quantum technologies: in particular, quantum-based clocks, navigators, imagery, and sensors that enable long-range detection of aircraft, submarines, or even activity below the Earth's surface. Quantum science will enable powerful networks of sensors and effectors to vastly accelerate the process of time-sensitive target observation and engagement in both the virtual and physical domains.

Quantum technologies will foreseeably be used in the development of new weapon systems, new materiel, and even in the development of new strategies, operational and tactical concepts. Because they significantly improve the speed of data computation and processing, the operational options of unmanned and autonomous military platforms will benefit because decisions can be made more quickly and a large number of targets can be engaged simultaneously.

Quantum communications technologies such as quantum key distribution-enabled cryptography (QKD) protect against future quantum attacks. Quantum communications cannot be hacked. Quantum key distribution is at the heart of quantum communications. The world's first integrated space-to-ground quantum communications network has been built in China, combining more than 700 fiber-optic QKD links on the ground with two high-speed satellite-to-ground QKD links. This will allow quantum keys there over a total distance of 4,600 kilometers to reach users across the country. There are plans to roll out this network globally with international partners from Austria, Italy, Russia and Canada. China also plans to develop small, cost-effective QKD satellites and ground-based receivers, as well as mid- and high-earth orbit satellites to reach QKD over a distance of tens of thousands of kilometers (Malewr 2021).

Quantum computing will enable computational capabilities far beyond the capacity of classical computers. This will strengthen situational awareness when military engagements need to be networked and orchestrated across multiple domains. Already, a number of actors are preparing to use quantum computers to hack into the opponents' encrypted servers or national infrastructure systems in near real time. The time for developing countermeasures is running out. It is necessarily shorter than the time frame for developing the technology and is at most 10 years.

CAPABILITY GAPS

New technologies and their associated skills and capabilities are developing at full speed. Computers are becoming faster and more powerful. Through the Internet of Things, humans and machines are symbiotically connecting to form powerful teams. Breakthroughs in artificial intelligence and sensor technology are multiplying the capabilities of security actors. Communications technologies are sustaining and driving this evolution. Nations and organizations best able to anticipate and exploit technological opportunities will have a decisive advantage in future competitions, crises, and conflicts.

While requirements are growing, the Western lead in military technology is currently shrinking, and with it, previous military superiority (Haas 2019). China and Russia, in particular, have narrowed their technological gap over the past two decades, in some cases by turning to commercially available technologies more quickly and effectively than their Western competitors and by accelerating their own innovation in the armed forces. Meanwhile, threatening EU and NATO capability gaps have emerged at the lower (hybrid threats) and upper (hypersonic and advanced nuclear weapons) ends of the conflict spectrum. They open the door to opponents and hybrid actors for coercion and blackmail.

Russia is not the only country that has modernized the critical capabilities of its armed forces in recent years. China, too, initially embarked on a broad military modernization program focused on traditional platforms and systems-including fifth-generation aircraft, aircraft carriers, rail guns, and ballistic missiles. Meanwhile, China, like Russia, has also developed its information warfare capabilities and built significant electronic warfare and offensive cyber capabilities.

Russia and China have combined the capabilities of new technologies with the advancement of their respective operational concepts, particularly in the context of anti-access and area denial (A2/AD), including ballistic and cruise missiles, hypersonic weapons, offensive cyber weapons, electronic warfare, and capabilities in all operational domains. On this basis, they can not only sink aircraft carriers or pose a nuclear threat to the West, but also protect hybrid, paramilitary, and low-intensity military operations with networks of sensors, air defenses, and offensive weapons (McDermott 2017).

The European Union and NATO are not well prepared for this, neither conceptually nor in their capability portfolios. While deterrence can still work in high-intensity conflicts, the lack of a defense capability against hypersonic weapons and the pending modernization of the U.S. nuclear potential, however, raise questions - hybrid actors can exploit existing capability gaps of the West in low-intensity conflicts without restraint. Opponents such as Russia, China or Iran will foreseeably use political, informational, criminal, and infrastructural means, as well as economic intimidation and manipulation, to discover and exploit Western vulnerabilities. This risks undermining the solidarity of NATO allies and partners.

Disruptive technologies will transform Armed Forces and their capabilities. Ultimately, the interplay between evolving technologies, associated weapon systems, military structures, processes, and concepts of operations will be critical to success (Rumsfeld 2001, pg. 6). In the private sector, digital transformation is driven by an almost unlimited imagination and creativity of designers and users. Accordingly, the civilian world is benefiting from exponential breakthroughs in digital technologies. In contrast, Armed Forces need certified, safer systems and weapon systems that are also reliable under operational conditions. As a result, there is a growing gap between the dynamic pace of innovation in industry and the economy and the careful, constantly reassuring procurement process in the military sector. It is precisely this dilemma that armed forces must resolve if they are to improve their own effectiveness in the face of the dynamics of technological innovation and keep pace with the threats posed by malicious actors with an affinity for technology.

The EU, NATO, and their Member States must coordinate and put pressure on their pace of innovation and organize themselves accordingly. This requires focus and competence. The European Defense Agency (EDA) already plays an important role in the development of the EU Members' military power tools. It is responsible for the development and coordination of EU and NATO capabilities in areas of common interest, and thus perfectly suited to lead cooperative projects that promote the rapid development of adaptive and agile situational awareness, a cross-domain ISTAR capability, and the further development of the C4I backbone needed for superior performance in cross-domain operations. The EU's Joint Research Centre (JRC), which supports the EU Commission with scientific expertise, could make important contributions to accelerating innovation with regard to the further development of non-military instruments of power. Technological focus could be on: 5G; artificial intelligence; autonomous systems; cyber and the electromagnetic spectrum; augmented reality; quantum science; and space. Both organizations should play key roles in the much-needed innovation acceleration ecosystem. They should also orchestrate the establishment of a modeling and simulation alliance that must carry sustainable innovation through to the education and training of policy, civil, and military decision makers. The added value of close cooperation with the NATO Science & Technology Organization and corresponding organizations of the Member States is obvious Thiele 2020).

TECHNOLOGY AS A TRANSATLANTIC COOPERATION PROJECT

Neither the European Union nor the USA will be able to win the technological competition on their own. They will have to hurry to keep up with the Chinese and Russian pace of modernization and their cross-domain deployment concepts. Therefore, transatlantic partners should meet Russia's technological challenges and China's technological rise together. With the new U.S. administration, the opportunity for a common transatlantic technology agenda is opening up. In any case, the European Union would be well advised to reflect its ambition for greater strategic autonomy not only in the economic strength of its members, but also in the technological portfolio of its Armed Forces. The EU and NATO need a new strategic concept and corresponding capabilities that can be convincingly effective across the entire conflict spectrum - from hybrid to joint/all-domain warfare.

The business model of the European Union and NATO forces is based on modern, interoperable, scalable and service-oriented information and communication technology. Key elements include command, control, communications, computing and intelligence, situational awareness, AI-assisted analysis and evaluation, planning and targeting, and precision strike capabilities. This business model has been a supporting foundation for superior Western military capabilities and decision-making. It is the primary reason for the professional respect it has received to date from opponents and potential peace disruptors.

Five functional themes should be the focus of joint efforts:

- **Innovation-supported conceptual approaches**

Innovation requires the Armed Forces and research institutions to work closely with the private sector, as the latter drives technological development and shapes the current disruptive innovation dynamic. In the short term, the focus should be on technologies that are already available or on the verge of becoming available, such as 5G, AI, autonomous systems, and space technology. In an operational environment of constant connectivity-with data as the new oil and networks as the new oil platforms-this focus would be particularly helpful in refining data and delivering actionable intelligence.

- **All-domain situational awareness**

This broad approach to situational awareness is the basis for the judgment of political, civilian, and military decision makers and their ability to perceive the relevant determinants in their environment and to use given instruments of power in a targeted and effective manner. Decision makers can only make accurate decisions if they fully understand the operational environment and all relevant areas. This includes the disruptive technologies that determine prosperity and security.

- **Information and media**

A whole new toolbox for malicious actors has emerged in the information and media space. These instrumentalize traditional, social and multimedia media into a destructive weapon, using them to influence through manipulated information, often in the form of disinformation campaigns. Moreover, by combining information from social and other media with spatial information from surveillance cameras, drones, and other omnipresent sensors, they can precisely locate and, if necessary, attack individuals, infrastructure, or weapons systems.

- **Serious Gaming**

In view of the complexity of technology-driven security challenges, political, civilian and military elites must be adequately prepared for their tasks. It can be assumed that opponents analyze and model the weak points of the EU, NATO and their Member States in detail in order to push through their respective goals. Serious gaming uses modeling and simulation as well as the possibilities of new technologies such as 5G, AI and augmented reality for education and training and thus promotes conceptual thinking and judgment of decision makers. It helps to develop a comprehensive understanding of actors, threats, risks, and applied concepts, but also of the EU's and NATO's own capabilities, effectively contributing to their use in an effective, well-orchestrated manner.

- **Resilience**

Resilience is an important means of reducing vulnerability and the attack surface for opponents. Open, democratic Western societies in particular offer multiple entry points for hybrid attackers. Critical infrastructure must be enabled to function reliably in the face of hybrid threats and attacks. Military forces and capabilities must be able to function under stress and shock. As new technologies increasingly become critical infrastructure themselves, and operational effectiveness depends on technology, this requires much closer cooperation between military forces and the private sector, including in the transatlantic context.

European nations and the United States should waste no time in pursuing closer cooperation in technological innovation. The EU's and the U.S.' own competitiveness is key to success in competing with China that, for example, already has a head start on AI and 5G. The country has set its sights on dominating other areas such as quantum computing and microelectronics in the future.

The fact that the offensive is winning in hybrid campaigns gives an indication of the urgency for boosting innovation in NATO and EU capability portfolios, leveraging emerging technologies and innovative approaches needed to ensure their own technological and military edge. Technology fields suitable for transatlantic cooperation include 5G, artificial intelligence, biotechnology, communications, cyber, semiconductors, microelectronics, space and quantum technologies. Practical approaches could underpin collaboration, such as joint concept development and experimentation, joint pilot projects, joint talent pools, or even a close alliance in the development of critical markets, e.g., in the context of space technology or 5G.

The EU in particular must accelerate technologically in order to keep up with the enormous pace of innovation of global competitors and opponents. For example, sustained investments in space SMEs and start-ups ensures long-term planning and would pay off as these are key players in technological innovation and developing new space value chains (Fiott 2021, pg. 28). Clearly, a strong Europe is also beneficial for the U.S., not only to maintain the Western lead in key technology areas, but also to protect the fundamental principles of basic values, freedom, democracy and the market economy.

REFERENCE LIST

Accenture (2019). The Post-Digital Era is Upon Us. Are you ready for what´s next? Accenture Technology Vision 2019. https://www.accenture.com/t20190201T224653Z__w__/us-en/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf . Access: 30 Jan 2020.

Arcesati, Rebecca; Rasser, Martijn. (2020). Europe needs democratic alliances to compete with China on technology. MERICS. https://www.merics.org/en/blog/europe-needs-democratic-alliances-compete-china-technology . Access: 22 Feb 2021.

Burke, Brian. (2020). Gartner: Top 10 strategic technology trends in 2020. Computer Weekly. 2 January 2020. https://www.computerweekly.com/opinion/Gartner-Top-10-strategic-technology-trends-in-2020?src=6059371&asrc=EM_ERU_124712826&utm_content=eru-rd2-rcpB&utm_medium=EM&utm_source=ERU&utm_campaign=20200312_ERU%20Transmission%20for%2003/12/2020%20(UserUniverse:%20717797) . Access: 22 Feb 2021.

Cordesman, Anthony. (2021). The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy. CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/2020811.Burke_Chair.AHC_.GH9_.pdf . Access: 9 Feb 2021.

Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America. Washington. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf . Access: 15 Feb 2021.

DIA. (2019). Challenges to Security in Space. January 2019. https://www.dia.mil/News/Articles/Article-View/Article/1754150/defense-intelligence-agency-releases-report-on-challenges-to-us-security-in-spa/ . Access: 15 Feb 2021.

European Commission. (2019). Member States publish a report on EU coordinated risk assessment of 5G networks security. Press release by the European Commission and the Finnish Presidency of the Council of the EU. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 . Access: 22 Feb 2021.

Eversden, Andrew. (2021). How the Defense Department wants to measure the success of its AI hub. C4ISRnet. https://www.c4isrnet.com/artificial-intelligence/2021/01/03/how-the-defense-department-wants-to-measure-the-success-of-its-ai-hub/ . Access: 22 Feb 2021.

Fiott, Daniel. (2020). The European Space Sector as enabler of EU strategic autonomy. https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/653620/EXPO_IDA(2020)653620_EN.pdf . Access: 23 Feb 2021.

Gould, Joe. (2021). After SolarWinds, US needs to toughen cyber defenses, says Microsoft president. C4isrnet. https://www.c4isrnet.com/2021/02/23/after-solarwinds-us-needs-to-toughen-cyber-defenses-says-microsoft-president/?utm_source=Sailthru&utm_medium=email&utm_campaign=C4ISRNET%202.24&utm_term=Editorial%20-%20Daily%20Brief . Access: 24 Feb 2021.

Gressel, Gustav. (2020). Military lessons from Nagorno-Karabakh: Reason for Europe to worry. ECFR. November 24, 2020. https://ecfr.eu/article/military-lessons-from-nagorno-karabakh-reason-for-europe-to-worry/?amp . Access: 23 Feb 2021.

Haas, Michael. (2019). Der westliche Vorsprung in der Militärtechnologie schwindet. Neue Zürcher Zeitung. April 12, 2019. https://www.nzz.ch/international/militaer-technologie-westlicher-vorsprung-schwindet-ld.1474351 . Access: 9 Feb 2019.

Harhoff, Dietmar; Heumann, Stefan; Jentzsch, Nicola Lorenz, Philippe. (2018). Outline for a German Strategy for Artificial Intelligence. July 2018, 6, https://www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/Outline_for_a_German_Artificial_Intelligence_Strategy.pdf Access: 9 Feb 2021.

Horowitz, Michael C. (2018). The Promise and Peril of Military Applications of Artificial Intelligence. Bulletin of the Atomic Scientists, April 23, 2018, https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/. Access: 16 Feb 2021.

Hruska, Joel. (2018). Think One Military Drone is Bad? Drone Swarms Are Terrifyingly Difficult to Stop. Extreme Tech. March 8, 2018. https://www.extremetech.com/extreme/265216-think-one-military-drone-bad-drone-swarms-terrifyingly-difficult-stop . Access: 13 Feb 2021.

Malewar, Amit. (2021). TechExplorist. January 7, 2021. https://www.techexplorist.com/world-first-integrated-quantum-communication-network-established/37174/?fbclid=IwAR0LJj9hpsy8KrDrgaMSXUVGnAGloexkTjunmqwWzxFc2uYqTa8J9h6jlwg . Access: 23 Feb 2021.

Masuhr, Niklas. (2019). AI in Military Enabling Applications. CSS Analyses in Security Policy No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf.

McDermott, Roger N. (2017). Russia´s Electronic Warfare Capabilities to 2025. RKK ICDS. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf . https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf . Access:3 Feb 2021.

NATO Science & Technology Organization. (2020). Science & Technology Trends: 2020-2040. March 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf . Access:3 Feb 2021.

NIS Cooperation Group. (2019). EU coordinated risk assessment of the cybersecurity of 5G networks. Brussels, 9 October 2019. https://europa.eu/rapid/press-release_IP-19-6049_en.htm. Access: 9 Feb 2019.

Olshausen, Klaus. (2020). Nukleare Herausforderungen – Nukleare Anforderungen. 2020. Denkwürdigkeiten Nr. 115. https://www.pmg-ev.com/denkwuerdigkeiten-nr-115-februar-20/ . Access: 9 Feb 2020.

John Parachini, Peter Wilson. (2020). Drone-Era Warfare Shows the Operational Limits of Air Defense Systems. RAND Blog. July 2, 2020. https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html . Access: 23 Feb 2021.

PWC. (2018). Nations will spar over AI. 2018 AI predictions. https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions/ai-arms-race.html . Access: 23 Feb 2021.

Rocess, Glenn. (2020). The World Has Just Witnessed A “Pearl Harbor Moment” In Armenia. Medium. October 28, 2020- https://glennrocess.medium.com/the-world-has-just-witnessed-a-pearl-harbor-moment-in-armenia-953f0ad3f31d . Access: 23 Feb 2021.

Ross, Wilbur. (2019). Remarks at the Sixth National Space Council Meeting. US Department of Commerce. Washington, Tuesday, August 20, 2019. https://www.commerce.gov/news/speeches/2019/08/remarks-us-commerce-secretary-wilbur-l-ross-sixth-national-space-council . Access: 15 Feb 2021.

Rumsfeld, Donald H. (2001). Quadrennial Defense Review Report. Washington. D.C, 2001. www.comw.org/qdr/qdr2001.pdf. www.comw.org/qdr/qdr2001.pdf. Access: 9 Feb 2021.

Sanger, David E.; Perlroth, Nicole; Barnes, Julian E. (2021). As Understanding of Russian Hacking Grows, So Does Alarm. NYT. Jan 2. 2021. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html?referringSource=articleShare . Access: 23 Feb 2021.

Schmidt, Eric; Work, Robert. (2019). In Search of Ideas: The National Security Commission on Artificial Intelligence Wants You. War on the Rocks, July 18, 2019, https://warontherocks.com/2019/07/in-search-of-ideas-the-national-security-commission-on-artificial-intelligence-wants-you/ . Access: 23 Feb 2021.

Smith, Julie; Kendall-Taylor, Andrea; Nietsche, Carisa; Laskowski, Ellison. (2020). Charting a Transatlantic Course to Address China. CNAS. GMF. https://www.gmfus.org/publications/charting-transatlantic-course-address-china . Access: 20 Oct 2020.

Thiele, Ralph. (2021). Disruptive Technologien - Chancen und Risiken im Kontext hybrider Gefahrenlagen. In Jäger, Thomas, Daun, Anna, Freudenberg, Dirk (Hrsg.). „Politisches Krisenmanagement 3: Führung, Recht, Organisationen". 2021.

Thiele, Ralph. (2019a). Hybrid Warfare – Future & Technologies Horizon Scan & Assessment. Inspiration Paper no. 2 (updated): Helsinki, Sep 2019.

Thiele, Ralph. (2020). Mind the Gaps. Project report. Hybrid Warfare: Future & Technologies. Hybrid COE. Helsinki Sep 2020.

Thiele, Ralph. (2019b). Space and Hybrid Warfare – Part One. Spacewatch Global. 2019. https://spacewatch.global/2019/12/spacewatch-oped-space-in-hybrid-warfare/ . Access: 23 Feb 2021.

Ralph THIELE

He is the President of EuroDefense (Germany, Bonn), the Chairman of the Political-Military Society (Berlin), the Managing Director of StratByrd Consulting (Andernach), the Advisory Board of the German Employers Association (Wiesbaden) and the host of "Space Cafe: Black Ops by Ralph Thiele".

He was born in 1953 and he is a retired Colonel who held key national and international positions in his 40-year military career in the German Armed Forces. He commanded troops up to the battalion level, developed concepts and capability requirements in the Ministry of Defence and drafted speeches and policy papers for Federal Presidents, Ministers of Defence, Major NATO Commanders and Service Chiefs. He also drove educational innovation at the German Armed Forces Command and Staff College (Director Faculty) and at the NATO Defense College (Chief of Staff) and shaped the Bundeswehr's path towards network enabled capabilities (Commander Bundeswehr Transformation Command). In his honorary and business functions, he advices on Defence Innovation in times of digital transformation. He has been frequently consulting, publishing and lecturing in Europe, America and Asia.