Future Defence Policy Regarding the Emergence of New Military Technology Threats:

European Perspectives

Mats Engman

SPECIAL PAPER
January 2022

Institute for Security & Development Policy

Special Paper

Future Defence Policy Regarding Emergence of New Military Technology Threats: European Perspectives

Engman Mats

Institute for Security and Development Policy
Västra Finnbodavägen 2, 131 30 Stockholm-Nacka, Sweden
www.isdp.eu

"Future defence policy regarding emergence of new military technology threats - European perspectives" is an *Special Paper* published by the Institute for Security and Development Policy. This *Special Paper* was published

The Institute is based in Stockholm, Sweden, and cooperates closely with research centers worldwide. Through its Silk Road Studies Program, the Institute runs a joint Transatlantic Research and Policy Center with the Central Asia-Caucasus Institute of Johns Hopkins University's School of Advanced International Studies. The Institute serves a large and diverse community of analysts, scholars, policy-watchers, business leaders, and journalists. It is at the forefront of research on issues of conflict, security, and development. Through its applied research, publications, research cooperation, public lectures, and seminars, it functions as a focal point for academic, policy, and public discussion.

Distributed in Europe by:

Institute for Security and Development Policy
Västra Finnbodavägen 2, 131 30 Stockholm-Nacka, Sweden
Tel. +46-841056953; Fax. +46-86403370
Email: info@isdp.eu

Editorial correspondence should be directed to the address provided above (preferably by email)

Contents

Introduction and a few historic perspectives

Technology and innovation have historically been a constant driver for defence policy and operational developments. Nations able to identify new trends early on and adopt their military forces and defence policies are much more likely to gain the upper hand in any potential war or conflict in the future. The ability to combine technological advancements into new policies and operational doctrines and to organize, equip, train and employ forces accordingly will yield better results than simply introducing new high-tech equipment into existing structures.

Historic examples are plentiful with the development of the "Blitzkrieg" operational concept in Germany leading up to WW2, as a prime example. This type of warfare combined advances in airpower, improved tactical mobility and armour into one coherent operational concept and broke the traditional static defence systems from WW1. The combined effects of the development of steam-powered engines, the telegraph and industrialization meant that large armies could be deployed much quicker over much long distances and even be directed from overseas. However once embarked from steamships these forces had very limited tactical mobility. It took the invention of the combustion engine to improve tactical mobility as well. Another major technological development having a significant impact is the atomic bomb and the Mutual Assured Destruction (MAD) doctrine, which in essence made large war between nuclear powers, all but unthinkable.

Other technological innovations, including the machine gun and night vision equipment, have had far-reaching tactical consequences, although they may not have revolutionized military thinking and defence policy per se.

Today we are witnessing yet another technological development or rather a series of major innovations with among others, the emergence of artificial intelligence and autonomous weapons, robotics, cyber weapons, drones, hypersonic weapons, and space-based weapons. Coupled with political and societal changes and other civilian technological developments these may greatly transform military power.

For this paper I will focus my discussion on information technologies including artificial intelligence, unmanned systems, autonomous weapons

and robotics and cyber-related technologies because I would argue these technologies create some extraordinary challenges to defence policy and decision makers. I will also try to include advancement in hypersonic weapons in my discussion as an example of a more "traditional" area of military technological innovation. I will throughout the paper refer to these technologies as "Emerging Disruptive Technologies - EDTs" or just "new technologies".

The main question the paper aims to address is, if and what possible changes to defence policies these new technologies combined may require, or result in. I will do that by examining some of these new technologies and to assess common characteristics. The importance of combining new technology into operational doctrinal thinking is addressed in a separate chapter. Subsequent chapters will examine how some European nations are, from a policy perspective addressing EDTs and in the last chapter I will discuss what possible changes to defence policy these new technologies may require.

What are these new technologies or Emerging Disruptive Technologies (EDTs)?

The myriad of new technologies being developed that could have military applications make it difficult to comprehensively cover all these developments in detail.

One example of the scope of these new technologies can be found in the London based Defence Science and Technology Laboratory-DSTL 2020 report which refers to, quantum technologies, human enhancements and augmentation, artificial intelligence (AI), machine learning and data science, future of data, new computing paradigms, energy and power, drone detection and cyberpsychology, as such emerging technologies.[1] Additional example is the Israeli Defence Forces who identifies robots, multi-sensor autonomous vehicles for different arms and services, nanotechnology and nanomaterials, sensors and sensing technology, the networking of people and things, artificial intelligence (AI), technological human empowerment, electromagnetic pulse (EMP) weapons, and quantum technology.[2] A third example is Dr Michael O'Hanlon's prediction of technologies of a "revolutionary dimension". According to Dr O´Hanlon those five technologies are, computer hardware, computer software, offensive cyberoperations, internet of things, artificial intelligence and "big data" and robotics including autonomous systems.[3]

Common features

Examining some of the common features and characteristics of these new technologies may give us a direction in how they may impact defence policy and military operations.

Many of the new technologies are not primarily defence or military technologies. Major programs and large resources of research and development are conducted outside the defence sector and financed by private actors, not Governments. This may result in some of these technologies be used for unregulated purposes and by non-traditional actors, included by non-state actors with limited resources.

Possible military application or use may not be the prime objective during development or not even understood, as innovation happen outside the traditional defence sector. Further it may be difficult to assess the military and operational value of some of these technologies without conclusive testing and evaluation. And it is particularly challenging to measure speed, range, weight etcetera and impact for many of these EDTs, due to their non-kinetic nature. According to Sergei Chvarkov, professor at the Russian Academy of Military Sciences, cyber weapons have several critical advantages and may in some cases be much more potent than physical destruction brought on by conventional weapons.[4] But how do you verify or assess these new technologies in a credible way and allow the result to fund e.g., cyber weapons and quantum technology over aircraft, tanks or submarines? Ultimately, such fundamental differences, may delay or make it difficult to fully appreciate the potential impact of some of these EDTs. Rebalancing a nations defence budget and changing military structures and organisations to make room for "untested" non-kinetic weapons, at the expense of more familiar military equipment, may prove difficult.

A third feature of many of the EDTs is the speed of development. As we have witnessed over the last decade the speed of development within information technology and cyberspace is extremely high, which outpaces regulating their usage. These fast-paced innovations cycles moreover, challenge national decision making and budget processes. It also requires more of a constant ongoing review and assessment process to continuously feed result on the usage and application of EDTs in national decision-making processes. These innovations are also different as they are rarely based on the traditional top-down, long-term capability planning model where traditional defence industries often play an important and integral part. EDTs are often developed in a bottom-up model with a very short time span from development to actual operation or market introduction. And often within small or medium size start-ups and non-traditional defence companies. This will make it possible for actors with limited resources to acquire capabilities that can seriously affect a nation.

A fourth feature is the vulnerabilities these new technologies may expose. Adversaries will seek to avoid areas of strength and seek to test where they perceive the opponent to be weak. Such an approach is not new, but with some of the new technologies, it will reach well beyond the borders

of the traditional battlefield. The last few years have shed light on the sheer scale of severe aggressive actions taken place against critical infrastructure in the U.S. and elsewhere, unauthorised access to large amount of personal data, fake news being coordinated by Governments, targeted information operations, and various example of "denial of service" attacks. This has resulted in a renewed focus on national resilience including protection of critical infrastructure. Several countries in Europe, including Sweden, have introduced, or re-introduced, different versions of "Total Defence concepts" including psychological defence, where the whole society is included and increasing resilience is viewed as a deterrent, equally important to traditional military deterrent. Assessing these new vulnerabilities will be as important as the potential advantages.

A fifth feature is the 'blurring of the lines', these technologies create. It does not just blur the lines between and within traditional military operations, by creating new war-fighting domains (cyberspace, space and the cognitive domain), they also blur the lines between physical, digital and the human spheres. They also obscure the distinction between war and peace/ceasefire, the frontlines and the home front, combat and non-combat units, a valid military target and a civilian target. In essence they risk blurring the line between peace and conflict. As many of these new technologies are non-military in nature, it may even impact politicians´ perceptions about the role of military force and promote new models of civilian-military interaction.[5] Many of these new technologies make attribution more challenging or blur the line between the aggressor and non-aggressor. Without clear evidence of a hostile act and or evidence of a perpetrator it will be difficult for any decisionmaker to order counter measures or deploy military forces. Additionally, it will require states to develop new Rules of Engagement, that are both effective in combatting the new threat and are politically and publicly acceptable.

A sixth feature is that new technologies challenge our entire system of confidence and security measures including arms control regimes. Many of these new technologies, like cyber-space, artificial intelligence or automated and unmanned weapons are currently mostly unregulated, posing added risks and challenges to international stability. Their dual-use character further contributes to challenges to find practical and feasible solutions

to balance commercial use and possible regulations in their use and military application.

A seventh feature is that these new technologies, especially AI, automation and unmanned systems will raise difficult legal, moral, and ethical questions. Can we allow an automated system supported by artificial intelligence to be employed without a human decision maker in the loop? Indicative of this complexity was the establishment within the United Nations, of a group of governmental experts on Lethal Autonomous Weapon Systems (LAWS) in 2016. The group have been discussing what is an acceptable level of "autonomy" in a weapon system and issued 11 "guiding principles" in 2019.[6]

An eight feature is a more articulated focus on a new war-fighting domain, the cognitive domain. Knowing the thinking and intentions of your opponent gives a significant advantage in any potential conflict, and even in normal international diplomacy and business. Being able to collect large amount of data to be processed and analysed using automation and artificial intelligence could allow actors to predict behaviours of large groups or maybe even individuals. One key challenge, however, will be to develop reliable algorithms to support the calculations. You may need to conduct large scale tests and experiments, using real people. With strong regulations on ethical standards in research in the U.S. and Europe and many other countries these type of tests will be very sensitive and difficult to perform. Meanwhile, laxer regulations in both Russia and China to military applications of AI and autonomous weapons systems including large scale testing on people, will probably not emerge as a major constraining factor.

A ninth feature is that the EDTs will challenge the way we interact with and procure military equipment. Many of these new EDTs are researched and developed outside the normal military-industrial complex. Finding ways to reach out to small and medium size business and research centres will be required, as will finding less bureaucratic and faster processes to procure new equipment. An addition feature of many of these new technologies is the lack of understanding within traditional military organisations of their potential military utility.

Combining technology with operational thinking

The development of new technologies will likely change the way we conduct operations and possibly also alter defence policy and priorities. Yet, it is the combination of technology and operational thinking or operational art, that may bring major changes or even a revolution in military affairs. To illustrate this argument, I have selected some examples from China and Russia, but many similar doctrinal and policy-shifts have been developed in the U.S. and in Europe.

Written some two thousand years ago, Chinese military strategist and philosopher Sun Tzu stated, "The ideal strategy is whereby you can win without fighting and accomplish the most by doing the least". He continued to state that "a military operation has no standard form – it goes by way of deception and when the enemy is confused, you can use this opportunity to take them".[7]

This fundamental understanding of the use and utility of military force, as expressed by Sun Tzu and others, are equally important today when discussing the possible impact of new technologies. It illustrates the multi domain and grey-zone character of modern conflicts and warfare. A more recent example of similar thinking is the Russian Chief of the General staff, General Gerasimov who in a famous article from 2013, "The Value of Science Is in the Foresight," spelled out his new thinking.[8] General Gerasimov took tactics developed by the Soviet Armed Forces, assessed technological achievements and changes in our societies and blended them with strategic military thinking about total war. He then laid out a new theory of modern warfare, which emphasize hacking or attacking an enemy's society rather than attacking its armed forces head-on with boots-on-the ground. He noted, "The very 'rules of war' have changed". A shifting balance between tools of power. The role of nonmilitary means to realize political and strategic goals has perpetually increased, and, in many cases, they have exceeded the power and effectiveness of actual weapons. Important to understand is that these non-kinetic means are all supplemented by military means, many times of concealed nature and or difficult to attribute. The Russian military units fighting in Ukraine wearing uniforms without ranks and flags, or the use of maritime militias by China in the South China Sea are two such

examples. It is the combination of kinetic and non-kinetic power that is central and it´s asymmetric application.

The Gerasimov thinking is a vision of total warfare waged on all fronts using a range of actors and tools—such as, hackers, media, businessmen, leaks and fake news, as well as conventional and asymmetric military means. Non-military tactics are not auxiliary to the use of force but the preferred way to win. Much along Sun Tzu´s thinking of, "….accomplish the most by doing the least". Chaos is part of the strategy, to achieve an environment of permanent unrest and conflict within an enemy (nation). Modern technology already available like cyberspace, internet and social media, may have made it possible to upend the domestic affairs of a nation, solely with information.

China is equally acknowledging the importance of new technologies and there seemingly exists a shared understanding among Chinese military strategists that technological advances will increasingly reshape the nature of conflict in the future. Changing from "informatized toward intelligent warfare", China now emphasises the concept of information warfare and information dominance. With this extension of the battlefields into the digital and cognitive sphere, there is a real risk the speed and complexity of combat operations will increase substantially. Central to this strategy in China, is the concept of the "Three Warfare Principles".[9] It relates to a comprehensive approach were psychological, public opinion and legal "warfare" are critical element in military planning and operations. This comprehensive approach alludes to a strategy of "unrestricted warfare", that in many ways resembles General Gerasimov´s "Total War". To this end, the Chinese leadership has been supporting a techno-nationalist strategy whereby innovations in the fields of science and technology are meant to be the key drivers of military modernization. Building on foreign technological capital it has amassed in the past decades, China seeks to develop indigenous technology ecosystems that will allow the country to eventually become self-reliant and join the ranks of global innovation leaders.

To further underscore this strategy, the Chinese leadership has set out on a path to promote civil-military integration, aiming to strengthen national security. In this context, the Chinese leadership is engaged in sustained efforts to integrate cutting-edge technologies into all branches of the Chinese armed forces. This fusion model may enable the creation of a

resilient technological ecosystem whereby military, academic, and business actors are closely cooperating to accelerate the development of innovative technologies in strategically important fields, like cyberspace, the electromagnetic domain and outer space. The strict control of the party-state will likely compel these cooperation's to remain top priorities for all involved stakeholders.

What is being done within Europe to address EDT´s?

Most nations in Europe are in different ways and with different ambitions engaged in developing new technologies and adopting defence policies accordingly, either on a strictly national basis or through various collaborations or most common, a combination of the two. To illustrate this development, I have chosen the example of the United Kingdom, a dominant European military nation and Germany, a maybe less dominant military nation but a highly technological advanced nation. I have also included one of the smaller and military non-allied nations, Sweden, to identify possible commonalities and differences in addressing EDTs and some examples from the collaborative efforts in Europe, through the work of the European Union. I have chosen the EU because many of the new technologies civil-military characteristics.

United Kingdom

In the recent United Kingdom´s Integrated Defence review, emerging technologies and their implication for defence policy is a central element. According to London, science and technology "will be an arena of systemic competition and over the coming decade, the ability to advance and exploit science and technology will be an increasingly important metric of global power, conferring economic, political and military advantages".[10] Major nations are investing heavily in new technologies and at the same time, many smaller countries are now able to compete in certain sectors. Large technology companies can generate power that even challenge national governments as evident in recent cases in China, where major tech compa-nies have been forced by Beijing to step back, when becoming too powerful. London assesses that to maintain a competitive edge in the field of EDTs, access to human and natural resources linked to technology and innovation will be as crucial as the ability to protect intellectual property. The volume of data available will grow exponentially and with increased availability of surveillance technologies, privacy and individual rights will be challenged. Technological advances will also create new vulnerabilities especially in

domains such as cyberspace and space, as well as the spread of disinformation online.

In the UK defence paper, presented just one week after the Integrated review, the Ministry of Defence highlights, "These newer domains of cyberspace and space pose significant challenges".[11] It further stresses, that advanced technologies are already being developed for adoption in new arenas but with limited international agreement on norms and conventions to regulate them and a lack of ethical or moral standards to encourage their responsible use. Whitehall are equally concerned of the development of Hypersonic Glide Vehicles, capable of delivering a conventional or nuclear warhead and with an unpredictable flight path, allowing very little warning time and thereby posing a significant challenge for defensive systems. States will increasingly seek to integrate these new capabilities with the traditional military domains of maritime, land and air making multidomain (air, land, sea, space and cyberspace) integration a necessity and norm.

To address these developments London stresses "increased commitment to security and resilience". Throughout both documents, there is a strong focus on vulnerabilities, resilience, protection of critical national infrastructure as well as democratic institutions and way of life. As mentioned, resilience features prominently in the policy documents and the Government wants to improve national preparedness and readiness across the whole risk lifecycle, from anticipation to recovery. To do so, the Government will start developing a comprehensive national resilience strategy in 2021, in partnership with the devolved administrations and English regions, local government, the private sector and the public. One interesting feature of this strategy is its focus on "societal resilience" including a new regulatory framework under the Online Safety Bill and a media literacy strategy.

The UK Government will over the next four years "….invest at least £6.6 billion of defence funding in advanced and next-generation R&D to deliver an enduring military edge in areas including space, directed energy weapons, and advanced high-speed missiles". London will also establish a new Space Command and develop a commercial launch capability from the UK – launching a British satellite from Scotland by 2022 as part of the UK Space Agency's programme. Further, London will introduce an Integrated Operating Concept, a Situation Centre, a Counter Terrorism Operations Centre (CTOC) and a National Cyber Force (NCF). London argues that

information is the foundation of integration. Therefore, they will need to invest in the capabilities that enable them to obtain and exploit information at speed to give them an advantage over potential rivals. Through the Ministry of Defence (MoD) science and technology strategy 2020, Whitehall will prioritise higher-risk research to support the modernisation of UK armed forces. In conclusion, United Kingdom emphasises the importance of new technologies both as a driver for changes in its defence policy but equally important as a driver for industrial and economic development.

Germany

In German defence and security policy, EDTs do not occupy a similarly prominent role as in, for example, the U.K. Berlin however recognizes the importance of new technology, and its possible transformational effect. A defence ministry's position paper from early 2021 notes that "[a] rapidly evolving weaponry technology enormously impedes the defence of land borders, infrastructure, and the safety of our own armed forces, which we currently are not fully prepared for." Furthermore, the ministry emphasises that Germany "has the responsibility to defend its own territory […]" and needs to work towards being equally equipped to defend alliances, including in the cyber domain with "credible military deterrence and defence capabilities".[12]

The federal government's 2020 Strategy Paper "Strengthening the security and defence industry", notes that "one of the technological challenges for our [Germany's] security and defence are the realms of digitalisation and artificial intelligence. Cybersecurity is an imperative for the advancing digi-talisation of the state, the economy and society as well as the sovereignty of both Germany and Europe."[13] Like others, the German government recog-nises that EDTs have both military and civilian applications. Additionally, the paper outlines that "advances in the research and development of new technologies - e.g., digitalisation, artificial intelligence, unmanned systems, hypersonic tech, biotechnology and cyber technology – will have a profound impact on the future's security and defence systems. This includes questions about the possibly destabilising effects and the compatibility of international law when these new weaponry technologies are deployed".[14]

To effectively address the challenges posed by EDTs, the government pro-poses to invest more in R&D and in "competency centres", "elite research clusters" and "innovation laboratories" for knowledge transfer, improving civil-military cooperation and coordination.[15] In addition, the official stance places a similarly strong emphasis on strengthening already existing European institutions and bolster European cooperation, which is reflective of traditional German security policy. Domestically, Berlin will invest in fast-tracking the concurrently lengthy process of awarding defence contracts and seek to improve dialogue between civil society actors and defence contractors.[16] In comparison with the many concrete actions London is introducing what Germany is proposing is less ambitious and seems more directed to gaining understanding of possible implication rather than tak-ing firm action now. For years Germany has been struggling with a chroni-cally underfunded Bundeswehr [the German armed forces], which may explain that more fundamental structural issues are prioritized. With about 1,4 % of the German GDP, allocated for defence spending, the funding to both address the structural problems and challenges associated with new technology, is not enough.[17]

Nonetheless, awareness is growing among the political leadership in Berlin that some of these new technologies may pose a significant challenge to international stability. Already in 2018, the current ruling coalition issued a strongly worded rejection of the unchecked deployment of EDTs. In their joint coalition program, the parties vowed to "[…] reject autonomous weapon systems that are entirely removed from any type of human con-trol. We want to outlaw them globally." And in 2019, under the auspices of Foreign Minister Heiko Maas, Germany signed on to the UN's "11 Guiding Principles on LAWS [Lethal Autonomous Weapons Systems]".[18]

Sweden

In Sweden, a technologically advanced and military non-allied country with a sizable domestic defence industry, new technologies and it´s possible impact on defence policy and operational concepts, was analysed in the latest long-term defence study. The study was reported to the Government by the Chief of Defence in 2018.[19]

In his conclusion the Chief of Defence stressed four key considerations for the future development of the Swedish Armed Forces, two of which are directly connected to EDTs. First, a changing operational environment that will affect an attack's purpose, scope and character and secondly, non-linear or hybrid tactics that will be directed against the entire society, expos-ing new vulnerabilities. The report emphasises that the future operational environment will be significantly affected by technological changes and that these changes are rapidly advancing. Advances in single technologi-cal areas, like e.g., hypersonic weapons will have a major impact, but it is the combination of several EDTs that might have a revolutionary effect. A challenge for any defence force, it is argued, is to strike a balance between development, implementation, and financing of new and existing technologies. The report also highlights the importance of combining technological advances with tactics and doctrines and the challenge related to ethical and legal aspects when introducing some EDTs like autonomous weapon systems and artificial intelligence.

The technological development will change the scope of battle by compressing time and expanding "geography", through increases in range, increases in speed, improved precision but also through offensive action in cyber-space. Combined with unmanned systems this will make it more difficult for any defence to correctly assess the situation and to employ the correct defensive measures at the right time.

The report addresses several new technological areas of significant importance, some of which are:

- Information technology were improvements in automated analysis of huge amount of data, Artificial Intelligence-AI and self-learning systems will generate decision support. In parallel, continued digitization of our societies will continue and increase our dependence on critical digital infra-structure and increase our vulnerabilities.
- Cyber space will become an even more important condition for both information operations and conventional military operations. Access to cyber capabilities will be proliferated to less advanced and smaller nations and organizations.
- Developments in sensor technology and electronic warfare is rapidly advancing through miniaturization, signal and imagery process and auto-mation improving detection ranges and target resolution.

- Unmanned systems will be introduced into all the various war-fighting domains and the number of remotely controlled and/or autonomous system will increase. Unmanned systems will also be introduced into new functions like logistics, mine-clearing and electronic warfare. This development, according to the report, will raise several legal and ethical questions currently unanswered.
- Our societies will be more dependent on space-based systems as will the future operational environment. Space-based capabilities are becoming available for new actors both nations and private actors. The proliferation of space assets is creating a "traffic jam" in space both related to physical space and bandwidth. Space based system can improve existing capabilities but also develop new capabilities. The dependence of satellite navigation and global positioning systems will increase.

One conclusion of the technological developments and the general geopolitical development, according to the report, is for future conflicts to include a broader spectrum of actions and more elements of non-linear or hybrid actions. Over the last ten years numerous examples of these hybrid or non-linear actions have occurred, some of which have been difficult to predict. One recent such example is the "weaponization of migration" that is currently practiced by Belarus against the European Union and in par-ticular Lithuania and Poland. The attacker, through directed information operations and the use of proxies (refugees) have been able to expose some of our democratic and open societies vulnerabilities and stirring domestic political unrest. These grey-zone challenges will require a more comprehen-sive approach to security and defence and closer cooperation between the traditional defence sector, the civil society, business, and academia.

The new Defence Bill, does include elements related to EDTs, but is surprisingly short of formulating any new strategy, operational concepts, or changes in procurement strategy to address the potential challenges with EDTs.[20] It instead, emphasizes and allocates substantially more resources on traditional military defence, like an additional mechanized brigade, new garrisons and one additional submarine. The entire defence budget for military defence is increased from 66,1 billion SEK 2021 to 88,7 billion SEK 2025, which would allow for introducing some novel capabilities.[21] The most evi-dent change related to EDTs and the changing operational environment,

is the establishment of a new cyber defence unit and increased cooperation between the Armed Forces and Universities in training new "cyber soldiers". To address challenges related to information operation, social media etc, a new national agency for psychological defence will be established and the Government in general emphasise the importance of civil-military cooperation. Spending on civilian defence will increase from 1,0 billion SEK 2021 to 3,8 billion SEK 2025, a substantial increase in percentage but rather modest in absolute numbers.

The European Union

Also, within the European Union and in particular the European Defence Agency-EDA, the "procurement agency" of the European Union, coordinated and structured work on the EDT´s and their possible implications are ongoing. EDA has been working on a "Technology Watch & Foresight" program since 2015. The activities aim to provide the necessary input for technology evaluation and to identify and assess the long-term impact in of these new technologies. EDTs are widely considered in key EU-level defence prioritisation documents and processes like the Capability Development Plan (CDP), the Overarching Strategic Research Agenda (OSRA) and the EDA R&T Planning Process. One of the objectives of the program is to assess the impact of these technologies on future defence capabilities in the short, medium and long term. The activities are based on an extensive network of experts and supported by several innovative IT-tools. One such tool is the Defence Innovation Monitoring-DIM tool, which aims to monitor and support a better understanding of the different phases of scientific and technological developments that may impact defence capabilities. DIM maps technologies and innovations in fields identified by the EDA Research and Technology process. DIM also amalgamate different datasets from scientific publications (source: SCOPUS database), patents (source: PATSTAT) and EU funded Projects (source: CORDIS). It is not meant to be a predictive tool but aims at shortening the gap between technological development as it is reported in specialised databases and awareness of said developments by defence policy makers and the research community.

Part of the EDAs effort is to organize workshops and high-level meetings to foster information sharing and cooperative arrangements. In April

this year EDA in cooperation with the Ministry of Defence in Portugal organized such a high-level virtual conference.[22] The conference addressed Emerging Disruptive Technologies (EDTs) such as artificial intelligence, big data, quantum technology, robotics, autonomous systems, new advanced materials, blockchain, hypersonic weapons systems and biotechnologies applied to human enhancements which are expected to have a disruptive impact on defence and revolutionise future military capabilities, strategy, and operations. In his opening remark, Minister of Defence, Joao Gomes Cravinho stressed the need for cooperation and synergies between civil and military actors to get the most out of new emerging technologies for defence. "When it comes to EDTs, we need to stimulate synergies between NATO, the European Commission and EDA, taking advantage of civil-military cooperation and the dual-use nature of technological development", he stated. Very much in line with the Chinese thinking and approach. He continued to stress that "Emerging Disruptive Technologies, particularly the nexus between data, Artificial Intelligence and autonomous systems, promise to be enormously impactful. EDTs require constant monitoring of risks and opportunities, and we should not forget that some of our key strategic competitors have identified them as strategic priorities."

EDA has also organized exercises to try to identify and inform future revision of the European research and capability development priorities. One such exercise was held virtually in May this year, with more than 160 participants from Member States, research centres, business, and academia.[23] The exercise was innovative in that it tried to combine different methodologies and processes, along with best practices and lessons learned from the wide community of foresight practitioners. One likely outcome of the exercise is to inform the next revision of EDA's Capability Development Plan (CDP), which defines the European capability development priorities. To further address the rapid technological developments, EDA has been tasked to prepare an Emerging Disruptive Technology Action Plan which will support Member States in monitoring the technological landscape and identifying and exploring collaborative opportunities within the EU to avoid fragmentation and duplication. As the technological developments are very comprehensive and quickly moves information sharing, collaboration and prioritization becomes a necessity for most countries.

Conclusions from the work of EDA is that combined the EDTs will have "disruptive impact on defence and revolutionise future military capabilities, strategy and operations". Furthermore, EDA has highlighted that "the strategic importance of cross-fertilisation between civil-military industries", and to "facilitate the use of civil research and innovations into new European defence projects", are essential.

From a defence policy perspective there are many similarities in how the United Kingdom, Germany, Sweden, and the European Union are addressing and acting related to new technologies. They all seem to acknowledge the possible fundamental impact of new technologies on defence policy. While the UK is already making several changes to its defence policy, Germany and Sweden are much more cautious. All countries argue that more of a whole of government and comprehensive approach is needed, resembling a "a national total defence system". They also stress new vulnerabili-ties and the need to improve resilience across society including "societal resilience". Another key feature is the need to improve and find new cooperative structures between military and civilian structures and international cooperation, be it in research and development, training, or procurement. The nature of warfare will also change, they argue, with "blurring of lines", asymmetric operations and grey-zone operations becoming more common, multi-domain operations being the new norm, deterrence need to protect systems and critical infrastructure and not only territory and the proliferation of unmanned and autonomous systems as some important features of the new battlefield. All also highlights the challenge these new technologies pose to existing arms control systems and the legal and ethical aspects they carry. Control, protection, and exploitation of data is another crucial and common aspect as is access to human and natural resources.

One area that is not highlighted in the various reports and policy papers is the increase risks of low-intensity, long endurance conflicts. With the introduction of more autonomous systems, robotics and AI nations will be able to engage in a more constant stage of conflict, without jeopardizing traditional military capability.

What changes to defence policy will EDTs require?

In the beginning of this paper, I asked the question if emerging disruptive technologies may lead to a revolution in military affairs or be considered more as a constant, phased evolution. It is a daunting task to analyse and assess all of the different new technologies (EDTs) and to formulate a clear opinion on their potential impact. But I would argue that the depth and scope to current defence policies combined would constitute a revolution, requiring nations to make substantial changes to current defence policies and operational thinking. Ranging from how to define deterrence, how to improve civil-military interaction, new mission and tasks for the armed forces, the use of force and ethical and legal aspects. My main arguments and how this may impact defence policy are.

Many of the EDT´s now being developed, like AI, big data, automation, and cyberspace can be directed at critical infrastructure and our cognitive space. This makes it possible to seriously affect our critical infrastructure from a distance and without using kinetic weapons. Combined with an ability to collect large amounts of personal data, through increased dependence and use of social media, Internet of Things, a variety of applications for shopping, transportation, health, and economy an adversary can create favourable conditions for political pressure. Undermining the credibility of the political leadership, affecting social and communal cohesion and national identity to create "the chaos-situation" Sun Tzu talks about. Defence policy needs to assume a much broader "whole of society" approach and introduce some form of "Total Defence Concept". A strong military without an equally strong and resilient society will not be enough to deter a potential hostile actor. A well protected national electric grid system may be as important as a missile defence system. Such a "Total Defence System" need to begin with organising Government departments and national agencies into coherent structures to avoid silo thinking and decision making. One example would be by organising a Security and Resilience department rather than a traditional Defence department. National command and control systems need to focus on improved civilian-military integration, by e.g., using liaison teams, establish a fully integrated command and control system and or develop a deployable civil-military staff element. Much more attention needs to go

into limit the impact of "fake news" and information operations by establish dedicated organisations responsible for psychological defence and societal resilience. As much of our critical infrastructure, health services, transportation, communication, and other essential services normally are provided by private business, these businesses as a consequence, need to become an integral part of national crisis management systems.

As we have already witnessed with the debate on introducing 5 G, where possible vulnerabilities to national infrastructure is becoming as important as new capabilities, these new technologies like advances in information technology, cyber and space, may play a more geopolitical important role for the global balance of power. As countries becomes more aware of vulnerabilities to critical infrastructure (important also to conduct military operations as the development of the Russian navigation system Glonass and the Chinese navigation system BeiDou illustrates) and the importance to control this, a possible development is "geotechnological clusters" of like-minded countries. Control of technical systems will be as important as control of territory. Such "geotechnological cluster" may develop around major nations like China, the U.S. and in Europe. For countries geographical located in an area dominated by a country with a different political system, this development may become increasingly challenging.

A danger of considering an increasing number of challenges in terms of security and in particular as "hard security" is that it can lead governments to use military capabilities to solve problems for which there is no military solution. One such issues being discussed in Europe is migration, which partly is viewed as a security threat, having critics arguing this has led to a militarization of EU borders and migration policy. The tasks and missions for armed forces, related to these non-traditional military threats, needs to be discussed and clarified.

The development of EDTs is likely to have strategic implications on global governance systems, arms control regimes, rules of engagements (ROEs) and international norms and standards. Technological innovations have always driven global governance and rulemaking. However, the rapid speed of development of many of these new technologies, may result in a growing gap between what technological advances make possible and the limits of existing arms control regimes and international norms and standards. This will not only create an intense competition over the development

of rules, norms and standards and the availability and use of data, it will also increase risks to unintended incidents. Space and cyberspace are two domains where we still lack effective arms control and Confidence and Security Building Measures-CSBMs. With the introduction of AI, autonomous and unmanned system we will have yet another area where international norms and code of conducts on the operational use, is lacking. Do we want a situation where an algorithm decides to fire a weapon from an unmanned platform? With more autonomous systems supported by AI and remotely controlled systems being introduced, human feelings may be a lesser part of "decision making", increasing probability for accepting higher risks and increases in collateral damage. New rules of engagement need to be developed and discussed as attribution will become more difficult and the challenge of less warning time for defensive systems. This will of particular importance in crisis management and grey zone operations. For decades the international community have made substantial and successful efforts to control the proliferation and operational use of certain military technologies, to improve stability, predictability, and safety. Nuclear non-proliferation agreements are one such example. Nations will need to invest and engage in new research in arms-control and CSBM´s and international cooperation, to avoid a possible, destabilising, and unregulated situation with higher risks. Or as stated by the UN Secretary General, "We need a new vision for arms control in the complex international security environment of today".[24]

The development and introduction of EDTs will challenge how we interact with private business and academia. As many of these new technologies will be or are researched and developed outside traditional defence structures, how do we interact and cooperate with those new organisations? Finding innovative ways to reach out to small and medium size businesses and start-ups will be hugely important. Nations should be encouraged to work more with non-traditional defence sectors, and to create innovative partnerships with the drivers of EDT innovation. EDA´s approach as described in this paper is an example of such a systematic process to "screen the market" for good ideas. If not existing already, nations need to develop some form a systematic interaction and possible exchange programs with academia and private business, including finding solutions to issues of classification. A more seamless HR-development program where an individual can transfer

between academia, politics, business, and military should be encourage. A similar discussion needs to take place on how to balance between in-house development of new capabilities and what can be purchased directly from civilian sources. The lengthy and sometimes very bureaucratic models of government procurement processes may need to develop some form of speed-track process.

Current trends in new technologies will also requires nations to invest more resources in R&D (research and development). Not only to conduct research but equally important to develop methods to validate or assess the effectiveness of new technologies. Nations not only need to invest in technology research, equally important is to operationalise new technologies into new operational doctrines, tactics and training. Having a well-resourced and manned "Operational Doctrine and Concept Centre" tasked with operational research and development will become even more essential. Within this field is a potential for increased international cooperation between nations with similar national interests.

A likely consequence of these emerging technologies is also a requirement to make organisational and operational changes of the armed forces. To further encourage and improve multi-domain operations including in the cognitive domain, a stronger emphasis on joint procedures and organisational structures are likely needed. Organisational structures and hierarchies centred around the traditional three services may now become less attractive. Both changes in the operational environment, the asymmetric and grey-zone character of future conflicts will require new competences and a more flexible manning system in military units. A difficult and decisive question, with EDTs putting more emphasis on security of systems, is how likely and important the tactics of large-scale ground manoeuvres and seizing control of vast enemy territories, will be in the future. As such large operations may also for politically reasons become less attractive, alternative operation tactics may be developed. One such option would be to penetrate the enemy's territory using various types of long-range capabilities (unmanned, autonomous) to destroy critical military capabilities and various strategic infrastructures. Such a development would have far-reaching consequences for any military organisation.

The uncertainties and speed of development for many of the EDTs will provide an increased likelihood that the operation you will face is not what

you trained for. Adaptability and flexibility will be key requirements for military organisations. Force structures need to become more "task-force" oriented and the ability to re-configurate forces and command and control elements at ease, will become more important. As a consequence, this will also drive changes in education, training and manning of military units.

Combine developments in hypersonic weapons, and offensive cyber-weapons may result in an erosion of nuclear and conventional deterrence credibility. As pointed out by Dr Ogilvie-White in a Chatham house paper last year, the credibility of the U.S. extended deterrence towards South Korea and Japan may as well be affected.[25] These rapid changes may also blur the lines between nuclear and conventional deterrence.[26] Advances, particularly in cyberwarfare, have the potential to destabilize the assurance of second-strike capability, particularly for countries with smaller arsenals.[27] This development may be of particular importance in regions lacking strong traditions in arms control and not having an existing security architecture. Asia would be one such region, where the technological development is fast-paced, risks are multifaceted and collective security arrangements are less developed.

Introducing hypersonic weapons would challenge decision-making-cycle as time constraints would entice decisions to be made with incomplete or incorrect information. Similarly, as hypersonic weapons have improved manoeuvrability compared to traditional ballistic missiles commonly employed detection technology and existing defensive systems are ill-equipped to deal with these new technologies, which may further impede timely warning and defensive countermeasures.[28] Russia has invested significantly in hypersonic weapons making the country a global leader in two cutting-edge EDT´s: hypersonic boost-glide vehicles and hypersonic cruise missiles. This may add risks to unintended incidents and further erode predictability and stability. Nations need to simultaneously, focus on both risk management protocols and procedures, arms control agreements and the development of new weapons.

Conclusion

New technology is developing rapidly offering new ways to exercise power and new ways of using and organising military forces. Advances in automation, artificial intelligence, hyper-sonics, cyber and space and doctrinal developments (hybrid-tactics) will affect how military forces can be organised, led, and deployed, as well as how we defend and protect, both sovereignty (territory and critical systems) and national interests. In essence requiring substantial changes to defence policy, a revolution.

In short, we are entering into a period of "new uncharted waters" but this time not only about physical survival and territorial integrity, but more and more about influence, control and access of systems, narratives, and economy. We therefor need to rethink our approach to both nuclear and conventional deterrence and security. Occupying territory may not be the preferred method once you can achieve decisive influence from range, using long-range weapons, unmanned and autonomous systems, cyber methods, and social media. And, if control over territory is no longer decisive to exert influence, what deterrent effect does a conventional territorial defence offer? Nations will need to strike a balance between protection of territory and protection of critical systems.

New technologies being developed requires more civil-military interaction and cooperation. Both in developing new technologies, assessing vulnerabilities and improve protection of critical infrastructure, training and manning. Nations need to develop new business models to interact with private business both for research and development but equally important to fast-track procurement processes. A more comprehensive approach to security and stronger focus on total defence concepts, organisation and command and control systems will be required. Nations will need to invest more in research and development and in operational developments. This can preferably be done through international cooperation.

The introduction of these new technologies will blur the lines, between, peace and war, soldier and civilian, a valid target and a civilian target etc, causing a need to establish new crisis management systems and develop new rules of engagement. Employment and use of many of these technologies are still unregulated and nations need to invest significant resources

to come up with new confidence and security building measures and arms control regimes or running the risk of a more unstable and unpredictable future.

About the Author

Maj Gen (ret) Mats Engman is a Distinguished Military Fellow at ISDP. His expertise lies in security policy, military strategy and crisis management, and his work has a particular focus on developments in East Asia, and the Korean Peninsula.

Maj Gen Engman has more than forty years of active military service. His most recent assignment was as Head of the Swedish Delegation to the Neutral Nations Supervisory Commission, in South Korea between 2015-2017. He was commissioned in the Swedish Air Force in 1976 and has predominantly served in joint and international positions. Among those are; two times as a UN military observer in the Middle East, three years as the Defense attaché to the United Kingdom and the Republic of Ireland, Instructor in strategy at the National Defense College, Deputy Director of the Military and Security Directorate and Head of the International Department at the Joint Staff.

Maj Gen Engman is a graduate from the Swedish Command and Staff College, as well as the Geneva Centre for Security Policy. He has also attended the US International Intelligence Fellows program at Bolling AFB, the US Senior International Defense Management Course in Monterey and the United Nations Senior Mission Leaders Course in Amman, Jordan.

Amongst his many accolades, he has been awarded the US Legion of Merit and the Republic of Korea's Order of National Security Merit Cheonsu Medal.

Selected Biography

1. HM Government report 2020, pp2-3
2. Dr Yoram Evron, the Journal of Strategic Studies
3. "Forecasting Changes in Military Technology 2020-2050"pp 5, Dr Michael O`Hanlon, Foreign Policy, Brookings
4. Journal of Strategic Studies
5. Dr Yoram Evron, the Journal of Strategic Studies
6. United Nations Group of Government Expert, https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/
7. Sun Tzu, "The Art of War", Shambhala Boston and London, 1988
8. Gen Gerasimov´s article published in Feb 2013 in the Military-Industrial Courier
9. Sangkuk Lee (2014) China's 'Three Warfares': Origins, Applications, and Organizations, Journal of Strategic Studies, 37:2, 198-221, DOI: 10.1080/01402390.2013.870071
10. Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", 16 March 2021
11. Defence in a Competitive Age", presented to Parliament by the Secre-tary of State for Defence, 22 March 2021
12. "Positionspapier: Gedanken zur Bundeswehr der Zukunft [Position Paper: Thoughts on the Bundeswehr of the Future]," Bundesministerium der Verteidigung, Febuary 09, 2021, https://www.bmvg.de/resource/blob/5028534/44dcd6d650e6c1f19ab2b82fe1f9510f/20210210-dl-positionspapier-akk-gi-data.pdf.
13. "Strategiepaper der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie [Strategy Paper on the Strengthening of Security and Defense Industries]," Die Bundesregierung, February 14, 2020, https://www.bmwi.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4
14. Ibid.
15. "Forschung für die zivile Sicherheit 2018-2023 – Rahmenprogramm der Bundesregierung [Civil Security Research 2018-2023 – Framework

Program oft he Federal Government]," Bundesministerium für Bildung und Forschung, September, 2018, https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/pdf/forschung-fuer-die-zivile-sicherheit-2018-2023.pdf?__blob=publicationFile&v=2.
16. "Strategiepaper der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie [Strategy Paper on the Strengthening of Security and Defense Industries]."
17. SIPRI Military Expenditure Database, https://sipri.org/databases/milex
18. "Außenminister Maas zur Einigung auf Leitprinzipien zum Einsatz vollautonomer Waffensysteme [Foreign Minister Maas on the Adoption of Guiding Principles for the Deployment of Autonomous Weapons Systems]," Auswärtiges Amt, November 15, 2019, https://www.auswaertiges-amt.de/de/newsroom/maas-letale-autonome-waffensysteme/2276738.
19. The Swedish Armed Forces long-term study, "Slutlig redovisning av perspektivstudien 2016-2018", 22 February 2018.
20. Regeringens proposition 2020/21:30, adopted by Parliament 14 December 2020
21. SEK Swedish krona, 1 SEK is approx. 0,11 USD, 21-08-24
22. "Impact of disruptive technology on Defence", https://eda.europa.eu/search?searchQuery=emerging%20technologies
23. https://eda.europa.eu/search?searchQuery=emerging%20technologies
24. "Remarks to the Conference on Disarmament," United Nations, February 25, 2019, https://www.un.org/sg/en/content/sg/speeches/2019-02-25/remarks-the-conference-disarmament
25. Chatham house Research Paper, Perspectives on Nuclear Deterrence in the 21st Century, April 2020, Dr Tanya Ogilvie-White
26. Chatham House Research Paper, Perspectives on Nuclear Deterrence in the 21st Century, April 2020, Dr Tanya Ogilvie-White
27. Chatham House Research Paper, Perspectives on Nuclear Deterrence in the 21st Century, April 2020, Dr Maria Rost Rublee
28. ISDP Blog post "The development of hypersonic weapons; Japan´s catch 22", by Larissa Stünkel and Mats Engman, 28 May 2020