Christoph Marischka

Artificial Intelligence in European Defence:

Autonomous Armament?

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

DIE LINKE.
IM EUROPAPARLAMENT

Christoph Marischka

Artificial Intelligence in European Defence:

Autonomous Armament?

Contents:

Introduction by Özlem Alev Demirel: Why resistance is necessary!

High-flying pseudo-satellites that monitor extensive areas for months; swarms of drones that secure the vicinity of field camps and "critical infrastructure"; computer systems that suggest targets to people and calculate the optimum line of fire; chat bots that are designed to get young people interested in military service and conceal the actual situation on distant battlefields; automated military logistics and (armaments) production: many of the current armament programmes of the European Union and its member states are related to artificial intelligence in one way or another.

The ongoing armament of the European Union, driven by digitalisation and artificial intelligence (AI), poses a threat to the populations of Europe. The COVID-19 pandemic has demonstrated that the money being poured into the armaments industry is urgently needed, for instance, in the care and health sectors. Furthermore, this specific form of armament not only has the potential to generate entirely new forms of surveillance and propaganda within Europe, but it also fuels a military escalation of latent conflicts among and with major powers and makes it more likely. While expectations of a "super AI" seem to be hype more than anything, propagated by industry and (venture) capital to mobilise public funds for their profits, AI applications are still finding their way into military systems and planning at all levels in the course of the current armament spiral.

There may not be a sudden, but certainly a creeping loss of control. After all, the current armament spiral not only involves the development of swarms of drones and killer robots, but it also threatens to do away with familiar distinctions between war and peace, civilians and combatants, and to completely lift the boundaries of the battlefield – as is already the case in cyber warfare. A study by RAND Cooperation, for example, which was commissioned by the European Defence Agency and included in the 2018 EU armament catalogue (2018 Capability Development Plan), predicts that international law will be almost entirely irrelevant after 2035. In it, national and international regulations primarily appear as obstacles to the realisation of technological possibilities. [1]

Instead of participating in this misguided arms race, it would be desirable for the security of us all if the EU were to devote its full energy to the regulation of autonomous weapons systems, cyber warfare and propaganda. In order to live in peace, we need a sharp demarcation of peace from war, which must be outlawed instead of anticipating and preparing for it at all levels, from transport and research policy to the circuit boards in our mobile phone networks. The "Cyber peace" and "Stop Killer Robots" campaigns provide important and feasible impulses in this regard. Unlike the armaments industry, however, they are not subsidised by the EU Commission with hundreds of millions of euros each year. Instead, the Commission has specifically promoted cooperation between civil universities and the armaments industry for many years. There is also resistance to this which starts at the right point: how much money is invested in solving social problems, and how much in the disastrous, accelerated and largely uncontrolled armament of the military apparatus?

[1] *Marta Kepe, James Black, Jack Melling, Jess Plumridge: Exploring Europe's capability requirements for 2035 and beyond (June 2018), www.rand.org.*

"The ongoing armament of the European Union, driven by digitalisation and artificial intelligence (AI), poses a threat to the populations of Europe."

1. A new Sputnik moment

In May 2017, an AI previously purchased and further developed by Google/Alphabet repeatedly won in the traditional Chinese board game Go against Ke Jie, the (Chinese) world champion at the time. This is considered a ground-breaking success in the field of machine learning, which seems to prove its almost unlimited potential. In the sphere of geopolitics, this and other games of Go between human and computer were later compared to the so-called Sputnik shock, when the USSR succeeded in sending a satellite into orbit around the earth before the USA. Just as this Sputnik shock at the time had resulted in massive US government investments in basic research and aerospace, China just two months later published an AI strategy with the declared goal of becoming the world leader in AI development by 2030. On 1 September 2017, Russian president Putin declared artificial intelligence to be the future of mankind in a speech to Russian students: "It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world".

Putin's words and the goals of China's strategy were widely echoed in the transatlantic sphere. They were picked up in the expectation of mobilising massive public investment and political support for relevant research at all levels on both sides of the Atlantic. In the USA, these calls were linked to the threat of losing the role as the only superpower and global technology leader. In Europe, on the other hand, they were linked to the vision of not only giving the European Union a new impetus for integration, but of making it a competitor on an equal footing with the USA and China in the global competition between powers. While Catherine Ashton, High Representative of the Union for Foreign Affairs and Security Policy at the time, had already stated the goal of catching up with the USA and China in terms of shaping power within the framework of traditional geopolitics when the European External Action Service was set up in 2011, the EU, China and the USA are also named as the most important competitors for the top position with regard to recent, AI-driven tech geopolitics beyond Europe. In May 2018, for instance, the business consulting firm Roland Berger in cooperation with a fund manager for venture capital, Asgard, published a study on AI in Europe. The introduction clearly stated: "We believe that Europe can become a third player in the 'arms race' between the United States and China."

One of the most important raw materials for the current hype surrounding AI is data available to China because of its comprehensive monitoring programmes, and to the USA because of the leading position of its tech/platform companies (Google/Alphabet, Amazon, Facebook, Microsoft). The EU, on the other hand, has a large domestic (and health) market with purchasing power that can at least potentially provide comparable amounts of data, as well as an efficient science and research infrastructure. In addition, a strategic and effective industrial policy has emerged in the EU in recent years, which enables the planning and implementation of entire value chains at European level and is consistently geared towards digitalisation and autonomy from the promotion of SMEs to politically driven mergers of existing corporations of international standing. The aim is to achieve so-called digital sovereignty in terms of independence from (pre-)products and services from third countries when building proprietary digital infrastructure. This is rightly regarded as an essential prerequisite for the desired global leadership position.

[2] *Cf. e.g. Paul Mozur: Google's AlphaGo Defeats Chinese Go Master in Win for A.I., NY Times (23 May 2017); Nicholas Thompson and Ian Bremmer: The AI Cold War That Threatens Us All, Wired.com (23.10.2018); Denise Feldner: Will a Chinese "Sputnik moment" in AI Unleash Dynamism in the West?, The Globalist (26.8.2018).*

[3] *James Vincent: Putin says the nation that leads in AI 'will be the ruler of the world' (4.9.2017), www.theverge.com.*

However, this idea of "digital sovereignty" is more than a model of industrial policy – it assumes a latent state of war between competing great powers. It therefore represents a departure from the liberal world view according to which global networking and value chains and the (inter)dependencies arising from them reduce the possibilities and probability of major armed conflicts. Instead, the concept amounts to the creation of blocks with self-contained information technology which consequently are capable of warfare in an era of hybrid strategies and cyber warfare.

This approach of tech geopolitics not only integrates the idea of the EU as a "competitive state" with an ultimately military concept of geopolitics, but is also seen as a prerequisite for competing in the race for the military application of artificial intelligence. AI-based weapons systems represent a promise, especially for a European Union that wants to become a power with military support, yet only disposes of armies with relatively small numbers of personnel, which are nationally fragmented, but technically well-equipped. Autonomous (weapon) systems and so-called manned-unmanned teaming characterise many of the current armament and research projects and are being pursued with the aim, among other things, of matching the USA, Russia and China in military terms even with a relatively small number of personnel.

Historically, there are numerous examples of how technological superiority does not necessarily lead to military or political dominance. Great hopes were placed in artificial intelligence on several occasions over the past decades and underpinned by extensive, military-inspired investment programmes – but ultimately disappointed. In the current race to develop disruptive military applications of artificial intelligence as well, it is by no means certain that said hopes or the strategic advantages associated with them will materialise. Therefore, at the end of this study, the question is raised as to the strategic consequences brought about the increased use of AI applications in the military, and the dangers they entail. From this perspective, it seems necessary to understand artificial intelligence and the expectations placed in it as an accumulation regime with which profit-oriented actors intend to achieve redistribution of public funds and re-regulation of the capital and labour market. After all, the more one moves away from discourses on AI which are global and, above all, motivated by economic policy, and focuses on concrete armament policy and military strategies of the EU and its Member States, the more one encounters old familiar visions of military superiority. Those are less related to the disruptive promise of "artificial intelligence" as a game changer than they are to the no longer quite so new expectations of warfare supported by information and communication technology (ICT). The following chapters will therefore outline the often rather fragmented expectations regarding digitalisation on the part of armed forces, followed by a detailed description of the role that corresponding technologies play and have played in the establishment and implementation of the European Defence Fund.

[4] *Roland Berger/Asgard: Artificial Intelligence – A Strategy for European startups, https://asgard.vc.*

Content

2. Expected "Military benefits" of Digitalisation

Many of the expectations placed by the military in digitalisation and artificial intelligence and fuelled by the armaments industry and developers are decades or even centuries old. The central vision of digitalised warfare is the creation of a "glass battlefield" or "information superiority". It is intended to enable superiors to issue and enforce commands on the basis of comprehensive situational awareness (**command and control, C2**). Just as early, heroic depictions of great commanders preferably ignored the fog of war, computer games today are still characterised by a tendency to convey the vision of complete information and control. Accordingly, the benefits that military personnel hope to gain from digitalisation can actually be compared to popular computer games. At command level, those provide an overview of the situation that is always available, and one's own forces as well as allied and enemy forces and other possible targets and obstacles will be precisely localised and receptive to new commands at all times. In many cases, this overview can also display indices such as combat strength, ammunition stock etc. not only for one's own forces but also of enemy troops and facilities, making the need for fire power easy to estimated or calculate. The extent to which this setup shapes popular notions of war, and, at the same time, how far removed it is from reality now – and probably in the future – can hardly be overestimated. However, to avoid veering off into distant visions of the gaming (and also armaments) industry, this publication will present some military concepts which are already in the phase of technical testing and tactical implementation. It shall determine that technological development very often takes place in civilian scenarios with a civilian context.

Situation awareness: An extremely fundamental question of artificial intelligence. Be it in speech recognition or computer vision, for instance, the inclusion of context is crucial to whether or not an event is categorised correctly. After decades of research failing to implement anything akin to situation awareness in information technology systems (ITS) by means of human-devised logical operations, hopes are now being placed in so-called machine learning methods based on Big Data.

For an unmanned aerial vehicle, it is of the utmost relevance whether a detected object is a small bird in its immediate vicinity or an aircraft in the distance. Machine learning could possibly be used to achieve a reasonably secure categorisation from the purely optically recorded data stream. However, this categorisation becomes more reliable if the data from the cameras is "fused" with that of a laser range finder or an infrared sensor, for example. While the added value of such "sensor-data fusion" is also evident in logical operations that can be understood by humans, methods of machine learning tend to be capable of including all available data for their "situation awareness". Research on sensor-data fusion or this form of pattern recognition currently takes place in countless civilian universities and also in medium-sized companies, for example in the context of autonomous driving. However, until a few years ago, it used to be a typical domain of military technology research, for which it remains of utmost interest.

The advantages offered by progress in machine learning and pattern recognition can be illustrated using the example of satellite reconnaissance. Research is currently being conducted on technologies in which satellites (or drones) can decide autonomously which areas are to be recorded with which resolution. "Regions of interest" are identified from large-scale, low-resolution monitoring, and then observed at high resolution. Those can be locations where changes are identified or where suspicious persons are present.[5] Changes can then be visualised in high resolution on the overall image. This brings

detailed monitoring of large spaces in quasi real time closer to the realm of possibility. At the same time, so-called pseudo-satellites are currently in development. The term refers to extremely lightweight aircraft which fly at high altitudes and can navigate and communicate using solar energy alone. This enables them to stay in the air and monitor areas for weeks or even months.[6] Artificial intelligence is intended to ensure that they carry out these tasks independently and e.g. also navigate according to weather conditions. Ground radars have long been in use, for example, to protect field camps. They can independently classify, track and identify objects over a distance of dozens of kilometres and identify them as possible targets. Network-centric warfare ideally assumes that the data from high-altitude pseudo-satellites, ground radars and many other reconnaissance systems can be merged into a common situation overview. One of the major remaining challenges will be the presentation of this enormous amount of data and the recommendations for action derived from it in an understandable way at a human-machine interface.

What has been described above for imaging reconnaissance also applies to signal intelligence and open-source intelligence (e.g. social media). Here, too, autonomous systems are increasingly collecting and processing data. Extensive research on this subject has been conducted in the USA since 2003 under the US Total Information Awareness Programme, which, among other things, has attempted to record and evaluate the activities of individuals on the Internet and social networks in a way which would facilitate forecasts regarding who might possibly carry out a terrorist attack in the future. Communication satellites over the Near and Middle East are being intercepted by satellite stations in Germany, Austria and Cyprus,[7] trying to identify patterns from the intercepted metadata that allow predictions about events.

Sensor-to-shooter: Network-centric warfare consists not only of networking reconnaissance systems, but also involves networking reconnaissance and weapons systems. The impact of the sensor-to-shooter concept – in combination with precise localisation possibilities – is enormous. To date, there has often been a considerable time lag between the collection of reconnaissance data and the impact of weapons systems. Even more time passes before the effect of the shelling is registered and the result can be used as a basis for deciding whether further shelling is required or e.g. ground troops can advance. Reconnaissance systems are supposed to be as small and agile as possible in order to be able to operate unnoticed behind enemy lines, in developed areas and, in the best case, even inside buildings. To achieve a great impact, however, weapons systems must carry a large explosive charge. They therefore tend to be conspicuous, inert and vulnerable and are therefore often used from a distance. Drones of the type currently used in so-called targeted kills, are ultimately armed reconnaissance drones, a hybrid form only used in more or less uncontested airspace. Their arms are sufficient to reliably kill individuals or disable unprotected vehicles in asymmetric conflicts, but not to attack armoured vehicles or buildings. They would be easy targets for an enemy air force or air defence. The "Eurodrone", which is currently under development, is also intended to be equipped with precision weapons. In the battlefield, however, its function will also include "target acquisition". This means that it would be able to detect or suggest targets according to the sensor-to-shooter concept and transmit their exact coordinates directly to weapons systems which can bring large amounts of kinetic energy to the target with virtually no time delay, even from great distances. Battle damage assessments could then also be carried out immediately.

Naturally, this also shortens the time available for (human) decision-making processes, which is why the technical literature speaks of "fight at machine speed".[8] Many EU governments to date continue to affirm that any use of force would still have to be confirmed by a human in the future. However, their armies have long been working conceptually on an approach in which humans define (or rather confirm) spatio-temporal corridors, but goals within these corridors are autonomously identified and fought. In the case of missile defence, for instance, this has been common practice on many warships of European states for years (with sensors and weapons not networked via cloud, but

[5] Corresponding research is carried out at the Institute for Information Processing (TNT) of the Leibniz University Hannover (Germany), among others. Cf. e.g. Holger Meuel et al: Low Bit Rate ROI Based Video Coding for HDTV Aerial Surveillance Video Sequences, http://ftp.tnt.uni-hannover.de/.

[6] An example of this is the solar high-altitude pseudo-satellite Zephyr by Airbus which is already being used by the British armed forces.

[7] Erich Möchel: Data from the Königswarte for NSA project (6 January 2016), https://fm4v3.orf.at.

[8] Lieutenant Colonel Thomas Doll, Uwe Beyer and Captain Thomas Schiller: Hyperwar – New Challenges for Army Development, Europäische Sicherheit und Technik (4 September 2019), https://esut.de/ .

integrated in one system).[9] Once it comes to defence against so-called overload attacks with autonomous systems, there will be no more time for human decisions, and humans will be out of the loop between sensor and shooter.

Electronic warfare/cyberdefence: Efforts to decode, disrupt and deceive enemy information and communication structures are a very old military task. Since said communication has been taking place primarily in the electromagnetic spectrum at the latest since World War II, attempts to decode, disrupt and deceive have often been subsumed under the term electronic warfare in recent decades. A central means of electronic warfare is jamming. Nowadays, it is used in asymmetric conflicts, among other purposes to protect against improvised explosive devices (IEDs) detonated via mobile phone networks. For jamming to work, it is necessary to know which frequencies the opponent is using to communicate. Military use of the electromagnetic spectrum has therefore, almost since its inception, been dependent on changing or scattering the use of frequencies according to principles that are as difficult as possible to reconstruct and/or to conceal the signal itself. Since then, a constant arms race has been underway in terms of obscuring one's own communication and exposing as well as disrupting the enemy's. As early as the 1980s, the United States Naval Academy described that progress in this field – at least among comparable opponents – would always "have only a finite time of superiority. Eventually an adversary will develop a counter technique and the superiority will pass to him [...] Technological superiority and constant development in the EW area are required to be consistently able to counter enemy advances".[10]

Identifying communication and interference signals has always been a field of pattern recognition, and the use of artificial intelligence in this regard is currently being tested intensively.[11] The digitalisation of the battlefield has increased dependence on functioning communication connections and multiplied said dependence in terms of complexity. Options for action depend almost entirely on access to satellite navigation systems and cyberspace. Although securing said access has not posed a major challenge in the asymmetric conflicts of recent decades, it is of fundamental relevance for military operations against opponents who are comparable to some extent. US military advisor Chris Scott wrote as early as 2012: "As we wind down and try to move these bandwidth-intensive technologies and advancements to counter other potential adversaries, we should understand that owning the cyberspace domain will not always be possible".[12]

Efforts to decode, disrupt and deceive enemy information and communication structures are a very old military task.

[9] An example of this is the close-in weapon system "Goalkeeper" by Thales, which according to the manufacturer is used by the Belgian, Dutch and Portuguese navies, among others. More detailed information on this: ICRC: Autonomous weapon systems: Technical, military, legal and humanitarian aspects (expert meeting report), (November 2014), www.icrc.org.

[10] United States Naval Academy: Fundamentals of Naval Weapons Systems – Countermeasures (1989), https://fas.org.

[11] In August 2018, IBM introduced its AI-based malware "Deeplocker". The company states on its website: "AI is changing the game for cybersecurity, analyzing massive quantities of risk data to speed response times", www.ibm.com/security/artificial-intelligence.

[12] Chris Scott: Anti-Access Area-Denial (A2AD) in Military Domains and in Cyberspace (17. Dezember 2012), www.fedcyber.com.

Efforts to prevent access to cyberspace or the combat cloud are increasingly discussed under the term cyber A2/AD: Anti Access/ Area Denial (A2/AD) strategies deal in making it more difficult for enemy forces to access and manoeuvre in an area. Although cyberspace is not a territorial space, access to it is bound to spatial confines. The effect and precision of jamming transmitters, for instance, decreases rapidly with distance and is therefore dependent on spatial proximity. Therefore, research efforts into the use of unmanned systems are increasing. In operations far beyond one's own territory, forces in the field are usually dependent on satellite links, which is why anti-satellite weapons will play a central role in possible future conflicts. Communication with distant commandos and data centres takes place via much faster cable connections, which, along with the associated infrastructure, can be attacked far away from one's own territory and the actual battlefield. Beyond this battle-related danger of cyber A2/AD, the NATO Centre of Excellence for Cooperative Cyber Defence in Tallinn, among others, points out that there is also a strategic level at which "a state can be connected and disconnected, sometimes against its will. Cyber blockades can occur and states can be denied access to cyberspace [...] Because of the serious impact of a cyber A2/AD strategy for society as a whole, it is likely that it would be applied during a military conflict, as one element of a larger campaign".[13] What is expressed through the (seemingly defensive) terms cybersecurity, cyberdefence and resilience is thus, on a tactical level, an extension of electronic warfare. On a strategic level, these efforts take place in expectation of a major international war, and with the intention of making it possible to fight said war. Since cyber and information space is a hybrid space – civil institutions and persons use the same infrastructure (cables etc.) as the military – research, development and implementation of corresponding concepts for its resilience also take place in a hybrid context, i.e. in close cooperation between civil and military (research) institutions.

Overload attacks: An important research area in artificial intelligence is cooperation between autonomous systems. This research also takes place with very similar questions at civil institutions under civil scenarios and at military facilities. So-called RoboCups, in which two opposing teams of robots play soccer against each other, offer a playful introduction to basic questions of self-localisation, sensor technology, object recognition and swarm behaviour of autonomous systems. They bring together young teams of (prospective) scientists and companies that are often also active in the armaments industry. Research with swarms of commercially available unmanned aerial vehicles is conducted at hundreds of universities throughout Europe and often takes place under purely playful tasks (dance, formation flight) or scenarios from agriculture, environmental protection or disaster control. The US Air Force, for example, had also commissioned the Department of Biology of the University of Marburg to conduct a study on the orientation of desert locusts at night in order to apply it to possible applications for the sensor technology of micro-UAVs.[14] For at least 15 years, the Chair of Aircraft Dynamics and Flight Guidance at the University of the Bundeswehr University Munich has been working on the conceptual development of a "cognitive agent" designed to coordinate swarms of larger, armed drones intended to autonomously eliminate previously determined and prioritised targets, compensate for losses and warn each other, for example, of enemy radar posts. Small swarms of commercial drones have already been used by militias in Libya and Syria to attack bases and drop explosive charges. In its attacks on Syria, the Israeli air force apparently also relies on overloading air defence by means of a combination of cruise missiles and drones.[15] In the early stages of the Syrian conflict, there was speculation about how extensive air strikes from the Mediterranean could be carried out by first overloading, locating and eliminating the Syrian air defence system in the densely populated coastal strip before attacking targets in the rear using manned aircraft.

[13] Alison Lawlor Russell: Strategic Anti-Access/ Area denial in cyberspace (2015), NATO CCD COE Publications, https://ccdcoe.org.

[14] Manfred Hitzeroth: Pentagon-funded research by the University of Marburg, Oberhessische Presse (25 November 2013), www.op-marburg.de.

[15] For an incomplete list of drone (swarming) missions by non-state actors, cf. Arthur Holland Michel: Counter-Drone Systems, Center for the Study of the Drone at Bard College (2019), https://dronecenter.bard.edu.

Swarms of smaller drones can be used to monitor larger areas and, combined with the sensor-to-shooter concept, can also be used for A2/AD purposes – i.e. to identify targets for shelling. Apparently, particularly high expectations are placed in swarms of small flying drones in the area of electronic warfare when it comes to overloading enemy sensor systems or disrupting communication (tactical cyber AD). The German Army Concepts and Capabilities Development Centre, for instance, describes the following scenario for the deployment of a tactical UAS battalion: "The hatches of the transport vehicles open, releasing 5,000 UAS, which form into different swarms. One swarm consisting of several hundred sensor UAS even extends over two kilometres in diameter and is equipped with high-resolution cameras. Some swarms have the job of jamming hostile drones or serve as relays for communication among friendly UAS. Others are fitted with micro munitions to attack hostile sensor systems and to mark or track targets, and are also capable of forming a deployable UAS barrier. A counter-UAS swarm is trained to intercept and destroy hostile UAS".[16]

Manned-Unmanned-Teaming: Major European armaments projects place special emphasis on so-called manned-unmanned teaming (MUM-T). In both the Future Combat Air System (FCAS) and the Main Ground Combat System (MGCS), which are currently developed in the EU, the manned combat aircraft or tank is intended to be at the heart of a system that includes otherwise unmanned vehicles. The systems can be assembled and expanded in a modular fashion. Drones can then e.g. fly or drive ahead, reconnoitre the situation and mark targets or even fight them autonomously. In principle, the overall system thus has a greater variety of different weapons systems and weapon types at its disposal. Especially in the case of the ground system, autonomous vehicles can transport additional fuel and ammunition. They are also intended to be capable of cooperating with detached soldiers and special forces and e.g. provide them with cover or salvage the wounded.[17] Germany and France, the driving forces behind both projects, are already standardising and updating the communication technologies of their armed forces. The respective projects feature the implementation of a Battle Management Language through which unmanned systems can be integrated and communicate with humans. Since 2019, the Bundeswehr has been testing the software Fire Weaver from Israeli supplier Rafael, with the support of Atos. According to the manufacturer, this provides "tactical forces with a GPS-independent, geopixel-based tactical common language between all sensors and shooters, which ensures optimal situation awareness and improved understanding of the battlefield. Targets, emergency services, sensitive locations and other points of interest are immediately and precisely categorised and transferred to the system's sight elements on the basis of 3D models [...]."[18] The system "improves human analysis and decision-making by automatically and instantly selecting the most relevant effector for each target, taking into account rules of engagement, location, line of sight, current ammunition status and many other parameters".[19] It uses "the advanced algorithms of artificial intelligence" and "processes combat data, analyses it and prioritises fire allocation".[20] At least from the manufacturers' point of view, the relationship between systems and humans has already been reversed on the battlefield: algorithms analyse the situation and make suggestions for the use of weapons – which humans then usually have to confirm.

It is true that MUM-T conceptually still differentiates between different levels of control from full control to merely informing operating personnel.[21] However, if the crews of ground and air systems, supported by a large number of unmanned systems, should actually find themselves in a combat situation, they will inevitably have to relinquish a great degree of control. This is especially true in air combat and when the opponent also employs autonomous systems. According to the French-German Research Institute of Saint-Louis, a central advantage of the MUM-T is the fact that it "can significantly increase the overall system effectiveness, while enhancing personnel protection, a crux for many decision-makers, not least because Western societies resilience to casualties in their own armed forces decline".[22]

[16] German Army Concepts and Capabilities Development Centre: Artificial Intelligence in Land Forces (2019), www.bundeswehr.de.

[17] Within the EDIDP project iMUGS (see below), swarms of robots are developed on the basis of Milrem Robotics' Tracked Hybrid Modular Infantry System (TheMIS), which can also be equipped with machine guns and rocket launchers, cf. "Milrem Robotics led consortium awarded 30.6 MEUR by the European Commission to develop a European standardized unmanned ground system" (17.6.2020), www.edrmagazine.eu.

[18] „"Die IDF wählen Rafaels Fire Weaver" ("IDF opt for Rafael's Fire Weaver"), Spartanat (February, 2020), www.spartanat.com.

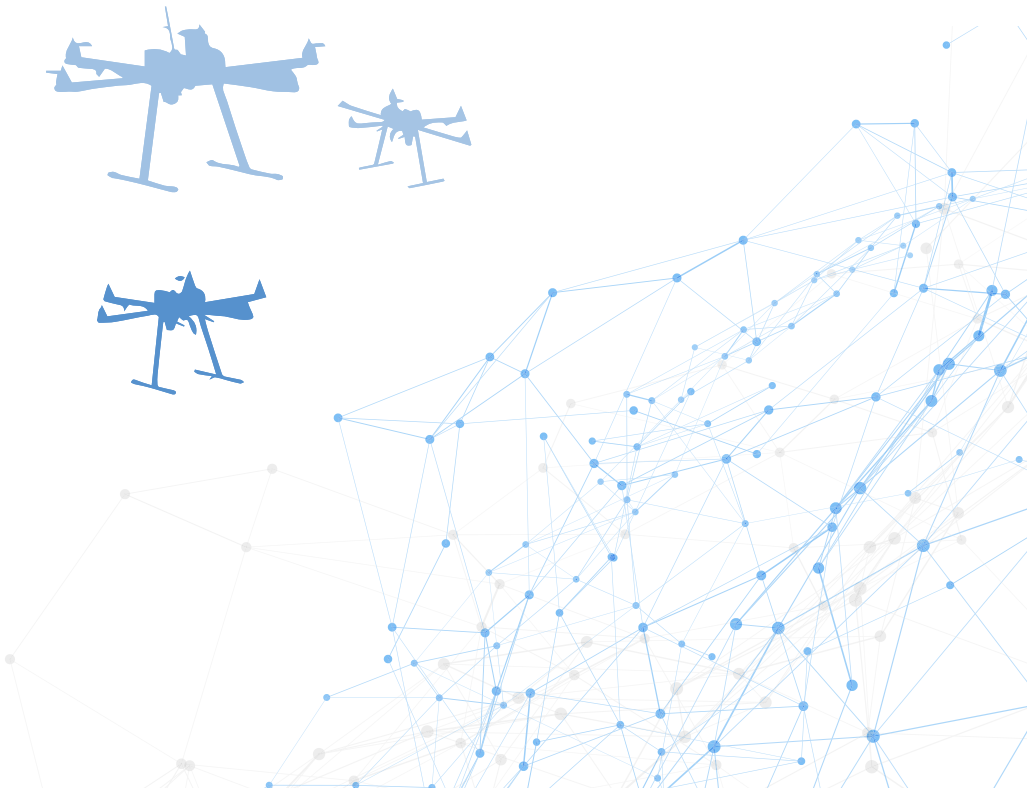
[19] "Interview with Yoav Har-Even, president of RAFAEL Advanced Defense Systems", Europäische Sicherheit und Technik (4 December 2019), https://esut.de.

[20] Cf. FN 18.

[21] Marius Pletsch: "Mensch-Maschine – EU-Großprojekte zum Manned-Unmanned-Teaming" ("Man-machine – Major EU projects regarding manned-unmanned teaming"), AUSDRUCK #100 (March 2020), www.imi-online.de.

Autonomous logistics and production: Many areas in which computer systems are clearly superior to humans and have been making decisions for decades are related to logistics. Storage and transport of people and material is a central task of the military, which sometimes equates effective warfare with effective logistics: "Successful command and decision-making is based primarily on correctly deploying a sufficient amount of the right resources at the right time, those resources having to be deployed effectively at a distance, or in force-on-force situations".[23] It therefore suggests itself that digitalisation and also artificial intelligence are already extensively used to plan and implement supply chains. Machine learning methods are developed and increasingly applied on a large scale for preventive and predictive maintenance, especially in industrial applications. Corresponding systems that predict the failure of parts on the basis of sensor data and pattern recognition and initiate appropriate maintenance are also available for military uses – often in connection with assistance systems that support personnel with extended or virtual reality regarding maintenance, among other things, and thus reduce demands in terms of required qualification.[24]

Autonomous systems could, however, herald a fundamental turn of events far beyond this, if they were used not only in warehousing – as is already the case – but also in transport. In 2017, the EUISS described the situation as follows: "Now the question is: for the first time since the Industrial Revolution, can emerging technologies reverse the trend of the evergrowing logistics tail of modern armed forces" by „rebalancing the ratio between combat and logistics forces" and „get 'more bang for the buck'?"[25] Transport aircraft and container ships already operate with a variety of assistance systems, which make crews almost superfluous. The industry has been developing autonomous Zeppelin drones for air transport of large loads over long distances, and quadcopters for the transport of light freight over short distances, for many years. Since 2011, the USA has been using unmanned transport helicopters (K-MAX) in Afghanistan for medium-size freight over medium distances. In numerous European countries, the military supports developments in the field of autonomous driving and is currently experimenting, above all, with implementing it in convoys with e.g. only one driver in the first vehicle. The European defence industry also pursues projects regarding tactical transport to the battlefield, also in the context of MUM-T.



[22] French-German Research Institute of Saint-Louis (ISL): ISL's Research and Technology serving the future French-German Main Ground Combat System, www.isl.eu.

[23] Cf. FN 16.

[24] The expectations associated with or fuelled by this can be seen, for example, on the blog of company C3.ai, which was established with venture capital and now serves many large companies in addition to the US Air Force. Predictive maintenance is only one of the services the company offers to the military and private sector, another is AI-based planning and management of procurement, cf. Philong Duong: AI-Based Predictive Maintenance to Enhance Readiness, Reduce In-Flight Failures (21 July 2020), https://c3.ai/.

[25] Torben Schütz and Zoe Stanley-Lockman: Smart logistics for future armed forces, EUISS Brief 30 (November 2017), www.iss.europa.eu.

Under the heading "Enhanced Logistics", the European Defence Agency (EDA) is working on mapping and harmonising national and commercial logistics systems and the IT infrastructure used for them. This could one day turn out to be the backbone of a "'nervous system' for military logistics",[26] which could then facilitate quick integration of concepts developed primarily for civilian use. IT and AI-supported supply chain management was a focus of the EU Commission research programmes FRP7 and Horizon2020. As the EUISS already stated in 2017, "[c]ommercial companies have ... helped transform logistics through vital R&D investments. While some requirements are uniquely military, many technologies and processes for military logistics can also be borrowed from the commercial realm". It talks about "[b]orrowing tactics from companies like Amazon and DHL" as "unmanned vehicles [may] also help minimise inventories, therein reducing the required manpower for convoys and thus the supply of combat troops".[27] From a technical standpoint, military logistics largely based on autonomous vehicles would be feasible quite quickly as soon as legal and administrative hurdles to autonomous driving in civilian, private use are removed. As will become apparent, this has been a topic of discussion from the very beginning in the projects in the run-up to and then within the framework of the European Defence Fund.

Regarding the logistics of use, outstanding importance is also attached to additive processes, which above all are intended to facilitate spare parts manufacturing on site to avoid long-distance transports from (domestic) production sites to the area of use. Since 2016, the US Army has been testing small drones that can be produced completely by a 3-D printer. The German-led support battalion of Operation Resolute Support in Afghanistan operates the Bundeswehr's first 3-D printer on location: "The force stationed in the far north of Afghanistan thus has an effective and flexible source for the short-term provision of small parts".[28] Here, the European Defence Agency is trying to develop joint solutions for the member states and prepared a study on additive manufacturing (AM) for logistics support in 2018.

As early as the following year, as part of the NATO exercise Capable Logistician 2019 and in cooperation with France and Spain, it presented a "fully equipped AM container ... with the aim of testing and demonstrating AM in real conditions in the land domain".[29] It is currently pursuing three projects (AMALIA, AMTEM, PACKOOL) targeting different applications under the heading "Additive Manufacturing for logistic support", but also dealing with "appropriate materials ... with a view to producing new types of warheads and propellants with enhanced performances".[30]

In the name of competitiveness, EU research policy also supports the switch to robotics and artificial intelligence in production. A ground-breaking project for this purpose was financed by the European Commission starting in 2012 and significantly promoted the cooperation between Airbus Defence & Space and robotics company Kuka. The Fraunhofer Institute for Factory Operation and Automation, which was also involved, wrote about this project – referred to as VALERI – which was promoted by the Commission with 3.6 million euros: "The factory of the future is becoming established in the aerospace industry: a consortium consisting of European research organizations and industry partners is presently developing mobile and autonomous robots that will be used to manufacture aircraft components and will work hand-in-hand with people". The companies that offer and provide cloud infrastructures for Industry 4.0 are partly identical to those that provide corresponding services for the military.[32]

[26] Ibid.

[27] Ibid.

[28] "Innovation in Afghanistan: Ersatzteile per 3D-Drucker" ("Innovation in Afghanistan: spare parts via 3-D printer"), Bundeswehr (20 August 2020), www.bundeswehr.de.

[29] European Defence Agency (EDA): Enhanced Logistics (10 July 2020), https://eda.europa.eu.

[30] Ibid.

[31] Fraunhofer Institute for Factory Operation and Automation: Robotics in Aircraft Manufacturing (VALERI), www.iff.fraunhofer.de.

[32] Cf. FN 24 regarding C3.ai.

In the medium term it is conceivable that battle management software (green IT) will be integrated with military logistics data management (white IT). The EDA is also working on AI-based systems in procurement. Although these are likely still a long way off, the digitalisation of the battlefield will only unfold its full potential once it is combined with the digitalisation of logistics and production and takes decisions away from people. Production and (military) logistics can then be immediately adapted to the respective anticipated situation on the battlefields and the resulting demand for resources.

Information warfare: Russia in particular, but also other geopolitical rivals of NATO and the EU are currently accused of hybrid warfare based on cyber attacks and disinformation campaigns aimed at destabilising Western societies, the EU and its member states. The USA has announced and reported several times that it will carry out undefined cyber attacks against the Islamic State of Iraq and Syria. There are also credible reports from Germany, France and other European states about offensive cyber operations already carried out.

Information warfare, which has not primarily relied on military structures to date, is closely related to the aforementioned cyber warfare (cf. electronic warfare). Both were a focus of the exercise "European Union Hybrid Exercise Multilayer 18".[33] In recent years, the EU has developed extensive efforts to combat hostile "disinformation" and instead reach defined target groups with so-called strategic communication. The catalysts for this were, on the one hand, the conflict with Russia in the course of the Ukraine crisis in 2014 and, on the other, the emergence of the so-called Islamic State, both of which were accused of deliberate disinformation. Reactions ranged from efforts to have corresponding profiles blocked by social media providers to the company itself exerting influence through specifically placed messages.

[33] Regarding the underlying scenario, cf. Note from the General Secretariat of the Council "EU HEX-ML 18 (PACE)", European Union Hybrid Exercise Multilayer 18 (Parallel and Coordinated Exercise) Exercise Instructions (EXINST) (26 October 2018), https://data.consilium.europa.eu.

A perspective that is increasingly prevalent continuously monitors the flow of information in analogy to cyber security, identifying not only malicious software, but also malicious information and excluding it from one's own information space. This is currently carried out in cooperation with social media providers such as Facebook, who are influenced to stop content under the guise of "fake news" or "hate speech". The announcement by US President Trump that he would deny social media providers like TikTok and WeChat access to the American market is an expression of similar efforts. The goal of "monitoring and removing unlawful content from the media" set out in the EU's Global Strategy (cf. 3.1.) is therefore only a vague, legalistic hint at what lies ahead.

In this context, a 2016 European Parliament resolution on "EU strategic communication to counteract anti-EU propaganda by third parties" should be highlighted. It states that "disinformation and propaganda are part of hybrid warfare … which is a combination of military and non-military measures of a covert and overt nature". Which is why Member States should "increase capacity sharing and counterintelligence efforts aimed at countering such operations". It requires EU institutions to "closely monitor the sources of financing of anti-European propaganda" and "to compile data and facts about the consumption of propaganda". The EU Parliament also stresses "that strategic communication and information warfare is not only an external EU issue but also an internal one", and „voices its concern at the number of hostile propaganda multipliers existing within the Union". Which is why Member States should "be active, preventative, and cooperative in countering hostile information operations on their territories or aimed at undermining their interests". This includes, among other things, "curtailing financial flows aimed at financing individuals and entities engaged in stratcom activities, incitement to violence and hatred". On the other hand, demands include that "special attention and sufficient resources [should] be provided for media pluralism, local media, investigative journalism and foreign language media, particularly in Russian, Arabic, Farsi, Turkish and Urdu as well as other languages spoken by populations vulnerable to propaganda" and "provide direct support to independent media outlets, think tanks and NGOs especially in the target group native language and enable the channelling of additional resources to organisations that have the ability to do so".[34]

[34] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), https://eur-lex.europa.eu.

European armies have long been experimenting with so-called "chat bots" and AI-based micro-targeting in their public relations work and in recruiting their own populations. This is done predominantly in cooperation with private companies specialising in this area.[35] It goes without saying that the objective of the information – approval of or interest in a military career – has priority over its objective truthfulness. The same applies to strategic communication towards the populations of competing or hostile states, which are encouraged to dissent quite openly from their governments. In this context, it should be pointed out that deceiving enemy forces under international law of war is recognised as a completely legitimate act and that propaganda in peacetime is not regulated in any significant way under international law. Since both (!) are currently no longer primarily promoted and developed in a military context under the title "Defence",[36] this publication will not go into further detail regarding information warfare. Therefore it should be stated at this point that the use of artificial intelligence in strategic communication can have the most dramatic effects: if different parties, with the help of private companies, finance autonomous or AI-based systems intended to spread mistrust and dissatisfaction towards opposing societies in increasingly closed information spaces, this has potentially disastrous consequences. In contrast to cyber warfare and autonomous weapons systems, there is not even a rudimentary discussion on the international regulation of information warfare and propaganda, nor are there ideas on how a further escalation of geopolitically motivated by increasingly automatically generated "fake news" could be stopped at this point. This is where civil society would need to step in. An international, non-governmental movement of "non-aligned" journalists and media could be a start.

European armies have long been experimenting with so-called "chat bots" and AI-based micro-targeting in their public relations work and in recruiting their own populations.

[35] PR agency Castenow, for instance, reported on its campaign on behalf of the German Federal Ministry of Defence on the Bundeswehr deployment in Mali: "The chat bot addresses users directly via Facebook Messenger and reports in real time [...] In addition to social activities, media close to the target group (Spotify, X-Box, DMAX, cinema) were used to anchor both the deployment and the series in the minds of potential applicants." The largest German-language chat bot took centre stage: "The YouTube series MALI takes the community on the soldiers' deployment abroad and answers their questions in direct dialogue via a chat bot integrated into Facebook Messenger. The deployment of the soldiers thus becomes part of the reality of young people's lives – transparent and as close as if a friend were there." Cf. www.castenow.de/.

[36] One exception is the 2020 call for proposals within the EDIDP programme (see below), which explicitly addresses AI applications for strategic communication (or logistics planning or airspace management...), cf. European Commission (EC): C(2019) 2205 final – Annex.

Content

3. Artificial Intelligence in the Genealogy of the European Defence Fund

3.1 Strategic Autonomy of a Global Europe

In 2003, the Council of the European Union for the first time adopted a joint foreign policy strategy (ESS) entitled "A Secure Europe in a Better World". The title alone suggests that the new actor has an ultimately global claim to shape the world, and that it almost inevitably has to assume the role of a global power: "As a union of 25 states with over 450 million people producing a quarter of the world's Gross National Product (GNP) […] the European Union is inevitably a global player".[37] Three years later, the European Defence Agency (EDA) published its Initial Long Term Vision (ILTV), which sounded out the military prerequisites for implementing this strategy – and was much more sceptical. Demography is addressed as early as the second paragraph and elaborated on further into the text: "Europe will in particular be held back by low fertility rates (currently 1.5) [...] Europeans will by 2025 comprise a mere 6% of the world population [...] The Armed Forces recruitment pool (16 - 30 age group) will fall by over 15% by 2025". To facilitate establishing and maintaining global manoeuvrability in spite of this, the ILTV emphasises the role of science and technology, especially information technology, in achieving "[t]he necessary degree of information superiority", which makes it possible to prevail even with limited, yet precisely and optimally dosed kinetic energy: "Warfare has been described as a mixture of intelligence and kinetic energy. The opening campaigns in Afghanistan and Iraq have confirmed beyond doubt that we are transitioning from the industrial age to the information age of war – that intelligence (or knowledge, or information) will become an ever more important resource for successful operations ...".[38]

In both the ESS and the ILTV, scenarios of a classic, cross-national confrontation between almost equal opponents indeed did not play a significant role. Reference is made to the foreseeable economic rise of China and India as well as to the need to maintain and strengthen one's own armament-industry base vis-à-vis the USA. However, primarily non-state actors are seen as opponents in military confrontations, and so-called failing states, in which the EU would intervene on behalf of a largely consensual community of states, are referenced as possible areas of operation. This capacity would consequently substantiate the role of the emerging global power EU vis-à-vis the USA, China and other actors who see themselves or attempt to position themselves as global players. In early strategy papers, this involved an understanding of technology that still differed significantly from the tech geopolitics on the rise today.

Private providers, who largely evade political control and whose services and infrastructures can be used almost equally by competing states and non-state actors, are seen as central actors in this context: "The proliferation of technology and knowledge is proceeding outside the control of governments and with the commercial sector fully in the driving seat […] Our own universal means of communication are already thoroughly exploited by opponents both as platforms for propagating ideas and ideologies and as communication networks". In contrast to current discourses of "cyber sovereignty", no thought at all is given to whether this could be changed or if such a change would even be desirable. On the contrary, the liberal paradigm of interdependence still reigns in the ILTV, for instance: "All this has reduced the plausibility of scenarios, at least in the European context and for the foreseeable future, involving traditional state-on-state warfare, with conventional forces pitted against comparable opponents".

[37] Council of the European Union: European Security Strategy – A Secure Europe in a Better World (2003), https://data.consilium.europa.eu.

[38] EDA: An initial long-term vision of European defence capability and capacity needs (2006), www.consilium.europa.eu.

However, particularly in the course of the implementation of the foreign and defence policy innovations of the Lisbon Treaty, in the following years there was already more open talk of international, geopolitical competition and of the need to represent European interests offensively. In a speech to the European Parliament on 10 March 2010, Catherine Ashton, High Representative of the Union for Foreign Affairs and Security Policy at the time, explicitly justified the establishment of the European External Action Service (EEAS) and the need for Europe to pool its capabilities with "the rise of China and others as major political players […] Europe's share of the world's population is 7%, down from 25% a century ago. In the last 60 years, our share of global GDP has shrunk from 28% to 21%. The economies of China, India and others are racing ahead at 10% per year. Economic weight is translating into political clout and self-confidence. You feel it everywhere: from negotiations on climate change to Iran, to big energy deals in Africa or Central Asia. If we pull together we can safeguard our interests. If not, others will make decisions for us. It really is that simple".[39]

Roughly around the same time as the EEAS, the Group on Grand Strategy began its work in 2011. This group brings together some of the most important strategists from the EU as well as representatives of the main think tanks. Since it is not an official EU institution, it did not have to mince matters when it came to its publications. One of its founders, James Rogers, phrased the following in his proposal for a "New Geography of European Power": "While some of the individual European powers are likely to remain in the top rankings of world economic output and military spending well into the current century, the gulf between them and the largest five actors – China, India, the United States, Brazil and Russia – is projected to grow. Moreover, the position and standing of the European powers relative to a ream of smaller powers – such as Turkey, Mexico, Indonesia, Iran, Nigeria, South Africa – is also projected to decline. These rising powers are giving considerable attention to their political and economic reach over geography, not only their domestic territories, but the world beyond them". According to Rogers, the EU should behave in a similar way in the future and define, develop and defend its own sphere of influence against "its adversaries": "Given that certain powers have sought to take advantage of key regions and entrench themselves – often to the disadvantage of others – the European Union should do more to ascertain the minimal geographic area required to sustain the continued expansion of its own economy".[40] This "Grand Area" is intended to encompass the "minimal geographic area required to sustain the continued expansion" and includes large parts of Africa, the oil-rich Caspian region, the Middle East and large parts of the Indian Ocean, where controlling shipping and trade routes is of the essence. It is defined by five criteria. One of those criteria is for the area to "hold all the basic resources necessary to fuel European manufacturing needs and future industrial requirements"; another requirement is that the "European Union can work towards defending [it] most cost-effectively through the expansion of the Common Security and Defence Policy".

In the years since 2011, the struggle for spheres of influence between the European powers, their allies and competitors has escalated, at least in Syria and Ukraine, to such an extent that conflict parties supported by them openly fought each other on the ground. Since then, Russia in particular has been accused of active hybrid warfare aimed at destabilising the European Union and its societies. Accordingly, scenarios of a direct military confrontation between NATO or the EU and Russia have increasingly played role in strategic discourse. The increasingly aggressive discourse suggesting that the EU must have its own nuclear weapons also underlines that military planning is not limited to crisis management operations and confrontations with clearly inferior opponents in terms of military as well as technology, but that military confrontation with other global powers is not ruled out (any longer).

[39] Catherine Ashton, High Representative of the Union for Foreign Affairs and Security Policy: Speech to the European Parliament on 10 March 2010 in Strasbourg, www.europarl.europa.eu.

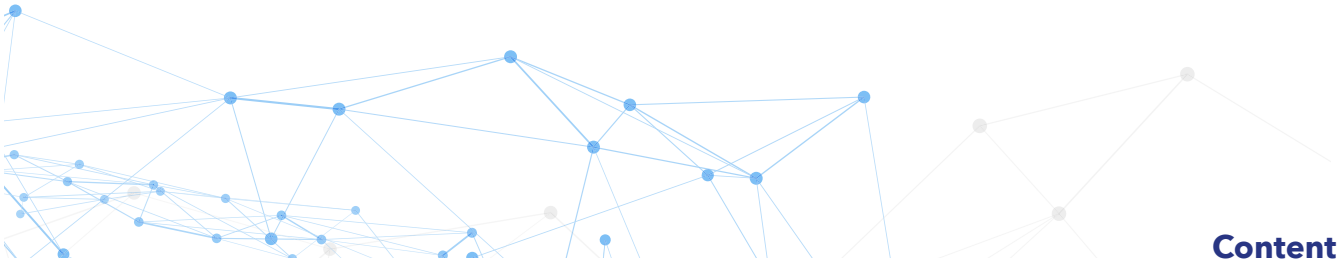
[40] James Rogers: A new geography of European Power, Egmont Paper #42 (January 2011), http://aei.pitt.edu.

This new orientation is reflected primarily in the Global Strategy for European Foreign and Security Policy adopted in 2016,[41] which replaced the 2003 ESS and, in direct comparison, features a significantly different tone. Early on in the introduction by Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy at the time, the range of challenges is described as follows: "Our foreign and security policy has to handle global pressures and local dynamics, it has to cope with super-powers as well as with increasingly fractured identities". The document itself not only announces with astonishing frankness an increased military presence in South and East Asia and the armament of China's competitors there, but also hints at the necessity of preparing for tough confrontations in Europe and the immediate vicinity: "While NATO exists to defend its members – most of which are European – from external attack, Europeans must be better equipped, trained and organised to contribute decisively to such collective efforts, as well as to act autonomously if and when necessary". The objective, as stated both in the foreword and in various places, is "strategic autonomy", which includes the EU securing its access to raw materials and energy and creating an independent armaments-industry base for any conceivable military capacities: "Full spectrum defence capabilities are necessary to respond to external crises, build our partners' capacities, and to guarantee Europe's safety".

In this respect, the Global Strategy already indicates a paradigm shift to tech geopolitics by increasingly striving for autonomous production chains in the armaments industry and formulating an active, geopolitically motivated technology and industrial policy as a prerequisite for "strategic autonomy" and thus the "security" of Europe: "This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services". Here, the idea of a "European Digital Space" to an extent still seems to be at odds with the "free and secure Internet", which the EU is called on to support. However, the task of "monitoring and removing unlawful content from the media", which is set out in the same strategy document, underlines that there has already been a significant shift in emphasis towards cyber sovereignty.

[41] European External Action Service: Shared Vision, Common Action – A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy, https://eeas.europa.eu.

“The proliferation of technology and knowledge is proceeding outside the control of governments and with the commercial sector fully in the driving seat”



Content

3.2 The Capability Development Plan

Almost simultaneously with the publication of the EU Global Strategy (EUSG), revisions began on the Capability Development Plan (CDP), which is supposed "to support decision-making processes at EU and national levels regarding military capability development, thus contributing to increased coherence between Member States' defence planning".[42] The first CDP was published in 2008 with earlier revisions made in 2012 and 2014. However, the identified shortfalls so far "were based mainly on CSDP military operations and missions". With the EUGS, a new "set of possible types of scenarios for the EU's military planners to grapple with [emerged]: the need to protect the Union and its citizens", as Daniel Fiott from the EUISS put it.[43] This means that armament should no longer focus primarily on so-called crisis management tasks in asymmetric conflicts, but also on cyber attacks and hybrid warfare engaged in by more sophisticated adversaries as well as classical defence in the sense of a tangible war with a more or less equal adversary. Since armaments projects in the field of classical defence have so far been carried out primarily within the framework of NATO on the one hand, but also mainly under national responsibility, this means more than just a gradual upgrading of the CDP. It is no longer limited to Member States' capabilities beyond defence to participate in EU missions worldwide through individual capacity. Instead, it ultimately calls for a fundamental reform and modernisation of the respective armed forces in the sense of a common European defence through participation in joint armament projects and specialisation in individual capabilities. In the end, this would require a combat cloud as extensive as possible with a connection to civilian logistics and production, which would cement Franco-German dominance in a "European Defence Identity" – and is contested accordingly.

One mechanism intended to drive this cooperation and modernisation is the "Coordinated Annual Review on Defence" (CARD), which was also adopted by the Council in late 2016. CARD is supposed to provide a "bird's eye view" of Member States' defence spending and projects and thus to "foster more consistent defence planning between Member States".[44] The EDA, in cooperation with the EEAS, then developed a methodology and implemented it starting in 2017 – parallel to the development of the CDP – for a one-year trial run that was still based on the 2014 CDP. According to the methodology, a review cycle consists of four stages. To begin with, (1) initial information from individual Member States in existing EDA databases is processed by the EDA and then (2) serves as the basis for a bilateral dialogue with the Member States in order to validate and complete the EDA's analysis. This is followed by (3) a cross-Member-State analysis, in which the EDA will "identify trends regarding defence spending plans ... as well as opportunities for defence cooperation". Upon further discussion with the Member States (4), a report with recommendations is drafted and submitted to the Council. In the process, CARD will "not function simply as a snapshot of today's defence landscape. It will also point to future likely developments in defence capability development such as technology trends and the industrial capacities to exploit them".[45] "[T]he first full CARD cycle" was intended to start in September 2019, to be based on the 2018 CDP, albeit significantly expanded with regard to armaments, and present its report to the Member States in autumn 2020.[46]

[42] *EDA: Fact sheet Capability Development Plan (28 June 2018), www.eda.europa.eu.*

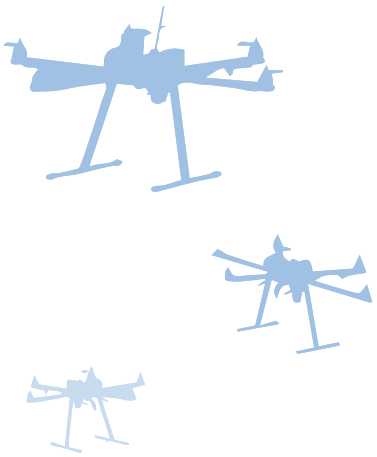
[43] *Daniel Fiott: EU defence capability development – Plans, priorities, projects, EUISS Brief #6 (June 2018), www.iss.europa.eu.*

[44] *EDA: CARD's on the table, European Defence Matters #18 (November 2019), www.eda.europa.eu.*

[45] *Ibid.*

[46] *Council of the EU: Council Conclusions on Security and Defence (17 June 2019), www.consilium.europa.eu.*

The CDP presented in June 2018 identified "a set of EU capability development priorities … with a reinforced focus on high-end warfare". It is important to note that those priorities encompass a "short-term perspective" (based on lessons learned and identified shortfalls from recent CSDP missions), "a mid-term perspective" (2018-2030, based on the collaborative database hosted by EDA as well as national plans and programmes) as well as a "longer-term perspective" (2035 and beyond). That said, the eleven identified and agreed priorities still look comprehensive and demonstrate a clear commitment to arm and prepare for a full-scale war in the future. For example, one of the priorities is referred to as "air superiority" and calls – among other things – for European "air combat capability", "ballistic missile defence" and "anti access/area denial (A2/AD) capability".



Content

3.3 Autonomous Systems and AI in the Priorities

Almost all of the eleven priorities' detailed descriptions[47] feature references, some closer than others, to digitalisation and often also to AI. This is particularly true for the "Capabilities for cyber responsive operations", which include "cyber situational awareness technologies, defensive cyber technologies, autonomous cyber response systems, cyber threat intelligence capabilities", and deal with rapid analysis of large amounts of code and data. Among the "ground combat capabilities", unmanned systems are prominently mentioned and highlighted: "All capabilities [under this priority] are to be considered within an operational environment, which will include manned and unmanned systems and the related manned-unmanned teaming". The same applies to the areas of "Naval manoeuvrability" and "Underwater control", the domain of space and all matters entitled "Air superiority". The latter explicitly state: "In the future, all [air combat systems] will be operated through a combination of manned and unmanned platforms, integrated in larger operational systems". Artificial intelligence is explicitly mentioned when it comes to the "integration of military air capabilities in a changing aviation sector", alongside a prediction of "automated airspace management activities" and the establishment of "the need to ensure access to the European airspace for existing and future manned and unmanned air capabilities for training, transport, deployment and operational purposes". As in this section, unmanned transport capacities for tactical and strategic air transport and especially for medical evacuation are anticipated at various points without any prominent emphasis. In addition, autonomous systems and artificial intelligence find prominent mention in the container category of "cross-domain capabilities", which lists technologies that the EU considers central to its future warfare without any concrete application reference: "artificial intelligence (AI), unmanned systems, remotely-operated or autonomous medical systems, autonomous and automated guidance, navigation and control (GNC) and decision-making techniques for manned and unmanned systems, multi-robot control or advanced materials, processes and technologies".[48]

[47] *EDA: The EU Capability Development Priorities (2018 CDP revision), www.eda.europa.eu.*

[48] *Ibid.*

Content

3.4 The European Defence Action Plan

The new tone of the EU Global Strategy in November 2016 was by no means accidental, but rather linked to other, concrete initiatives which ultimately led to the establishment of a separate EU armament budget and forceful promotion of joint armament projects. The State of the European Union speech of the then-Commission President Juncker in September 2016 proclaimed in its very title the intent to build "A Europe that protects, empowers and defends". It contained, among other things, the following reference with regard to Syria at the time: "Europe needs to toughen up. Nowhere is this truer than in our defence policy […]. For European defence to be strong, the European defence industry needs to innovate. That is why we will propose before the end of the year a European Defence Fund, to turbo boost research and innovation." Plans for this were intended to be submitted as early as the same year, "as part of the European defence action plan" (EDAP).[49] The EDAP appeared in November 2016 and refers to the USA's heightened armament spending and the "unprecedented" armament budget increases of China, Russia and Saudi Arabia, among others. In keeping with strategic autonomy, it calls for the "Member States' joint acquisition, development and retention of the full spectrum of land, air, space and maritime capabilities". It is explicitly geared to the priorities expressed in the Global Strategy: "intelligence-surveillance reconnaissance, remotely piloted aircraft systems, satellite communications and autonomous access to space and permanent earth observation; high end military capabilities including strategic enablers, as well as capabilities to ensure cyber and maritime security".[50]

While a large part of the EDAP deals with the military relevance of EU space programmes and outlines how existing (civil) financial programmes such as the European Fund for Strategic Investments (EFSI) or even Erasmus+ can be used to expand and staff supply chains of a high-tech defence industry, the core of the EDAP is the establishment of the European Defence Fund. This fund is supposed to consist of two "windows". One window was to focus on joint research projects and to be endowed with 90 million euros for the years 2017 to 2019 (PADR, cf. 3.6.). The other window was dedicated to the development of capabilities and was intended to create incentives for Member States to focus on individual capabilities and to introduce joint technologies, commission prototypes or feasibility studies on the (joint) European armaments market to this end (EDIDP, cf. 3.7.). A joint Coordination Board was supposed to ensure that both windows were interlinked, i.e. that the jointly initiated research would also translate to joint development and joint armament projects. This envisaged translation of joint research into concrete armament projects is a major innovation compared to previous Commission research programmes (FP7 and Horizon2020). The EDAP argues primarily in terms of savings and efficiency: not all countries on their own were to develop and maintain technological and industrial capabilities by ordering small margins from their respective national suppliers.[51] At the same time, however, it is obvious that it serves to establish the foundations of an EU army driven primarily by Germany and France starting at the industrial base. Accordingly, it promotes the expansion of an arms market dominated by the two countries, with value chains distributed throughout the Union and at the same time restricted to the latter as far as possible.

[49] *Jean-Claude Juncker: State of the Union 2016, https://publications.europa.eu.*

[50] *European Commission: European Defence Action Plan (COM(2016) 950 final), https://eur-lex.europa.eu.*

[51] *European Commission: European Defence Action Plan (COM(2016) 950 final), https://eur-lex.europa.eu.*

Content

3.5 The Pilot Project

To allocate the 90 million euros to research programmes intended to contribute to the establishment of the EDF, a Preparatory Action on Defence Research (PADR) was set up in 2017. This action, in turn, was based on a pilot project that the EDA had also launched in 2016 at the European Parliament's initiative. For the moderate amount of 1.4 million euros, the latter supported three activities, all of which were related to artificial intelligence and could build upon extensive civil research, but which were supposed to further develop this research under explicitly military premises:

Unmanned Heterogeneous Swarm of Sensor Platforms (EuroSWARM)

The EuroSWARM project was funded with a total of 434,000 euros and aimed at the design and cooperation of mobile and stationary airborne and ground-based sensor platforms. One part of it consisted in the autonomous allocation of tasks and targets, factoring in conditions in which individual platforms or sensors would fail or exhibit unexpected behaviour. Another portion consisted in fusing sensor data for identification and tracking of possible targets and the production of a situation overview. Tests were carried out with commercially available platforms both indoors and outdoors.[52]

In addition to the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut, FOI), participating institutions included the French aviation research authority ONERA (Office National d'Études et de Recherches Aérospatiales) as well as the universities of Patras (Greece) and Cranfield (UK). The University of Patras described the scenario as follows: "A mission scenario with a very strong interest by military and security/law enforcement agencies is the case in which a specific area of high interest requires persistent monitoring/surveillance. It is assumed that the scenario takes place at the battlefield in conflict with a well-armed and competent opponent. […] As the terrain limits the visibility in the protected area, centralized sensors are however ineffective. Instead the guards use ground sensors distributed in a large area around the camp that facilitates early indications on enemy reconnaissance or approaching formations. The ground sensors are sensitive for the presence of humans, vehicles and animals and give prompt alarms if potential targets are in the vicinity". If stationary sensors detect suspicious movements, the mobile unmanned systems are supposed to swarm out and provide security personnel with images (and other sensor data) and, at the same time, feature the capacity to detect "suspicious behaviours exhibited by the target" themselves.[53]

The Centre of Autonomous & Cyber-Physical Systems at Cranfield University, a university which originated, among other things, in the military-oriented College of Aeronautics and has its own research airport, received the most extensive EuroSWARM funding at 130,000 euros. Among its referenced clients for other projects are the defence companies BAE Systems, Lockheed Martin, Leonardo, Airbus and Thales as well as the European Space Agency. The Centre describes its main research areas as follows: "Recent research includes the airborne monitoring of ground traffic behaviour for hidden threats by autonomous sensor platforms, developing an analytical framework for understanding the behaviours of multiple unmanned aerial aircraft and creating collision avoidance and path-planning algorithms for Unmanned Surface Vessels operating out of human eye sight".[54]

[52] *E EDA: PP Call PP-15-INR-01 Information on the awarded project, www.eda.europa.eu.*

[53] *"EUROSWARM", www.aml.euroswarm.upatras.gr.*

[54] *"Centre for Autonomous and Cyber-Physical Systems", www.cranfield.ac.uk.*

Inside Building Awareness and Navigation for Urban Warfare (SPIDER)

The SPIDER project aims "to support urban warfare operations (urban combat or in trying to handle a terrorist hostage situation) by providing improved situational awareness inside buildings". For this purpose, radar sensors are intended to be used outside the buildings in question to register the presence and movements of people inside the building. In addition, robots are supposed to enter the buildings, "to provide in real-time an indoor map" and to be able to provide soldiers with images of the interior before they intervene.[55] This purpose also entails a fusion of data from various sensors. A central task for the unmanned ground vehicle inside the building is simultaneous localisation and mapping (SLAM), which is generally a central issue for autonomous systems operating in unfamiliar environments. SLAM places high demands on computer vision and object recognition. At the same time, it involves highly generalised questions of self-perception and modelling of the environment, which are of fundamental interest to AI research. Major breakthroughs have been expected in this field for some time, but have largely failed to materialise.

It is doubtful that such breakthroughs were an aim of SPIDER, as the project's funding and scope were also limited to 433,000 euros. Its largest recipient is the Portuguese company TEKEVER, which had already been involved in numerous "civil" research projects of the EU Commission in previous years. As early as 2004, the company started to receive funding from the EU Commission in the context of the AVITRACK project to monitor the airport apron, in detail "to model, interpret and check normal servicing operations and to track objects and persons over the airport parking area" by "exploit[ing] real-time information from video and infrared images".[56] From 2012, the company received funding, among other purposes, for research into novel gyroscopes (AGEN project)[57] and wing shapes[58] specifically for UAVs. This was followed in 2013 by a study on the use of private smartphones and other mobile devices by security authorities to generate situation overviews (iSAR+) as well as a (somewhat utopian) project on novel aircraft control by means of neuronal activities (BRAINFLIGHT).[59] In parallel to the participation in the EDA pilot project SPIDER, research with EU funding began in the context of the ROBORDER project, "a fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles, capable of functioning both as standalone and in swarms, which will incorporate multimodal sensors as part of an interoperable network". Since 2019, TEKEVER has been involved in the "civil" EU research project ARESIBO spearheaded by Airbus Defence and Space, which intends to utilise augmented reality to optimise "collaboration between human and sensors (fixed and mobile)" and to improve situation awareness, among other things, through "adapted processing of sensor data, correlation between heterogeneous data and information and creation of knowledge through deep learning techniques".[60] According to the company itself, TEKEVER is currently "leading the market in unmanned systems technology and services, developing next generation satellite systems, and helping customers to digitally transform their business". While offers for digital transformation on the company's website are vague, three drones of different sizes are offered in the UAV area. The largest model (AR5 – "The European Maritime Patroller") features "[a]utonomous surveillance of large maritime and land areas, with onboard multi-sensor pattern detection" for up to 20 hours. The smallest version (AR4) is advertised as "[v]alidated and battle proven by multiple security and military forces" and promises, among other benefits, "[c]ontinuous surveillance of sensitive areas, with automatic pattern recognition for target detection".[61]

Besides TEKEVER, SPIDER also involves the company Aralia Systems, a leading supplier of intelligent airport video surveillance according to its own accounts; the institute "Professor Tsvetan Lazarov" attached to the Bulgarian Ministry of Defence as well as the Instituto de Telecomunicações (IT – Aveiro). The latter is a joint research institute of six Portuguese universities, funded mainly by national and EU institutions (including ESA) and the private sector, including Siemens.

[55] *EDA: PP Call 15-INR-02_02 Information on the awarded project, www.eda.europa.eu.*

[56] *cordis.europa.eu/project/id/502818.*

[57] *cordis.europa.eu/project/id/322466.*

[58] *cordis.europa.eu/project/id/314139.*

[59] *cordis.europa.eu/project/id/308914.*

[60] *cordis.europa.eu/project/id/833805.*

[61] *"About", "AR5" and "AR4-EVO", http://uas.tekever.com.*

Standardisation of Remotely Piloted Aircraft System (RPAS) Detect and Avoid (TRAWA)

The TRAWA project deals with the integration of remote-controlled aircrafts into civil airspace. For instance, if private individuals control commercially available quadcopters, this does not constitute an integration into civil airspace, as the quadcopters are legally – and usually technically – restricted to altitudes without any manned air traffic. In the vicinity of airports, the operation of such drones is prohibited and, in the case of commercially available models, often prevented by means of technology (via geofencing). Integration into civil airspace, however, aims at an everyday coexistence of manned and unmanned systems with different flight characteristics, also e.g. in Western European airspace, which requires a high degree of standardisation. It is generally assumed, for instance, that RPAS can lose contact with human pilots, or must in certain conditions react without human control. Standardisation concerns therefore include the security of communication links and autonomous evasion systems for emergencies (sense & avoid).

The TRAWA project, however, starts at a more fundamental level, which precedes direct and autonomous collision avoidance. Its standardisation targets include the range of the sensor system (depending on speed) in order to detect any other aircraft approaching at an early stage and to "remain well clear".[62] Under the leadership of the Netherlands Aerospace Center (NLR), TRAWA involved two (closely interlinked, UAV-specialised) Italian consulting firms (EuroUSC and Deepblue), a British consulting firm and the German Aerospace Center (Deutsches Zentrum Luft- und Raumfahrt, DLR). According to the EDA, the project was carried out "in support of" the Working Group 105 of the European Organization for Civil Aviation Equipment (EUROCAE). The EUROCAE is an air traffic standardisation institution almost entirely supported by industry. Its Working Group 105 dedicated to unmanned aerial systems is clearly dominated by the defense companies Airbus Defence & Space, Thales and Safran. Little is publicly known about TRAWA's results;[63] merely the EuroUSC website indicates that, besides sensor technology, the project dealt with the presentation of possible evasion routes at human-machine interfaces to the pilots.[64] The DLR, which was also involved, in contrast refers to TRAWA in a "blueprint" entitled "Concept for Urban Airspace Integration". In it, the DLR outlines a vision featuring movement of "all aircraft in all airspaces": "[T]he proposed concept is that it opens up the airspace equally for UAS with low technical equipment levels as well as with high". This is supposed to be facilitated by a "U-space system", in which air traffic control manned and managed by humans no longer plays a role and seems to give way to a "central system" instead: "The U-space system would handle information provision (including traffic data and proximity warnings), airspace management and traffic flow control. A density-based airspace and traffic management system assures the optimal mission management of UAS/Air Taxi operations within a pre-defined time interval. Aircraft positions and mission data (4D trajectories) would be reported back to a central system after reviewing all airspace conditions. Higher priority missions (esp. rescue helicopters) would be reported to the system and any necessary dynamic adjustments to the affected airspace segments would be initiated. […] Different measures may be taken if the airspace user doesn't follow the given instructions and passes the innermost protection area. The airspace and traffic management system may try to take over control of the aircraft (precondition here is the availability of a control link) to terminate or re-route the flight. If this isn't possible, additional measures to terminate the flight (including defense actions) may be required".[65]

[62] EDA: PP Call 15-STAN-CERT-01_02 Information on the awarded project, www.eda.europa.eu.

[63] For a more detailed contextualisation, cf. Directorate General for External Policies of the Union: European armaments standardisation, study requested by the SEDE Subcommittee, www.iss.europa.eu.

[64] "TRAWA", www.eurousc-italia.it.

[65] DLR: Blueprint – Concept for Urban Airspace Integration (December 2017), www.dlr.de.

Content

3.6 Preparatory Action on Defence Research (PADR)

Subsequent to the pilot projects, which received 1.4 million euros of funding, the European Defence Fund began its work in 2017. For the first two years (until the end of 2019), it was funded with 90 million euros, which it allocated in the context of a Preparatory Action on Defence Research (PADR) – window one, i.e. "research". The first call for proposals (2017) stipulated three programme lines with a total budget of 25 million euros. The first and most important line targeted "the launch of one complex project" expected "to show the added value of unmanned systems in enhancing situational awareness while operating alongside and communicating with other manned and unmanned systems". This resulted in the Ocean2020 project aimed to further develop MUM-T to improve situation overviews at sea under the leadership of Italian company Leonardo. It brought together 43 companies and institutions from fifteen countries, including Indra (Spain), Safran (France), Saab (Sweden), MBDA and Hensoldt (Germany), many of Europe's leading armaments companies. The project disposed of a total funding amount of 35 million euros. It culminated in a demonstration led by the Italian Navy in November 2020, involving six naval vessels from four countries (Italy, France, Greece and Spain) and nine unmanned systems (air, surface and underwater) from various manufacturers. Four satellite systems and two ground communication networks ensured communication between the participating vehicles and with four Maritime Operations Centres (in Italy, Spain, Greece and Portugal) and "the prototype of a European operational centre" in Brussels. A second exercise of this nature was scheduled to take place in the Baltic Sea in 2020 under the leadership of the Swedish Navy.[66]

The second line was devoted to research related to force protection and soldier systems, including improved camouflage systems and "chemical, biological, radiological and nuclear (CBRN) protection". One of the programmes funded in this line was aimed at standardising the ICT worn by soldiers on their bodies (GOSSRA project) – and covered an armaments industry spectrum very similar to Ocean2020, with Rheinmetall (Germany), Leonardo, Indra and Saab. The third line served strategic technology foresight with the goal "to develop realistic scenarios of potential future conflicts which will help scoping EU-funded defence research".[67] In this context, the Italian company Engeneering Informatica won the contract for its promise of "simple and intuitive technology forecasting services exploiting Big Data Analytics and text mining techniques" in the PYTHIA project (Predictive methodologY for TecHnology Intelligence Analysis).

The second call (2018) promised 40 million euros and also comprised three lines, the first of which was aimed at a single, large project eligible to receive up to 12 million euros of funding. It aimed at developing a "mini computer" (system on a chip) compliant with military requirements to contribute to creating "a European supply chain for specific, critical electronic design technologies". The second line provided the prospect of up to 5.4 million euros for a project to design a "European high power laser effector" which could serve, among other things, to defend against conventional missiles, fast boats and "tactical manned and unmanned aerial vehicles". The third line earmarked up to 1.9 million euros for a project entitled "Strategic Technology Foresight", which was supposed to identify, among other things, "non EU sourced components and materials in the systems developed by the EU industry and used and to be used by the EU armed forces" to facilitate counteracting (future) dependence on third countries – including the USA.[68]

[66] *https://ocean2020.eu/.*

[67] *"Preparatory Action on Defence Research: 2017 research topics description", https://ec.europa.eu/.*

[68] *EDA: 2018 Calls for proposals on Preparatory Action on Defence Research, https://ec.europa.eu.*

The third call (2019) comprised 25 million euros and invited tenders for five studies on "emerging game-changers", including artificial intelligence, quantum computing, augmented reality, artillery weapons and satellite-independent navigation systems. Each study could be allocated up to 1.5 million euros for "stimulating the emergence of a European innovation eco-system with strong relations with the defence sector".[69] A second line of the programme called for further studies that would investigate "radically new future technologies of any kind with unexpected impact" that could produce "radical technological superiority over potential adversaries" without specifying any concrete topics. The explicit aim put forward was to activate "new actors in defence research and innovation", "including excellent young researchers, ambitious high-tech SMEs and visionary research centres of big companies and research and technology organisations".[70] Finally, a study on "interoperability and standardisation of systems, subsystems, components and procedures of complex [unmanned] platforms in a network centric environment" was put out to tender. In this third call as well, the eight (known) projects receiving funding are dominated by well-known grandees of the armaments industry: among them are Thales and Nexter (France) as well as Diehl and MBDA (Germany). The geographical distribution of the companies and institutions involved is particularly striking: France is involved 25 times in total, followed by Italy with seven, Spain and the Netherlands with four each, Germany and Belgium with three each and the Slovak Republic with two involvements. Furthermore, Portugal, the UK, Latvia, Austria, Poland, the Czech Republic and Greece are only represented once each.

[69] EDA: 2019 Calls for proposals and General Annexes, https://ec.europa.eu.

[70] Ibid.

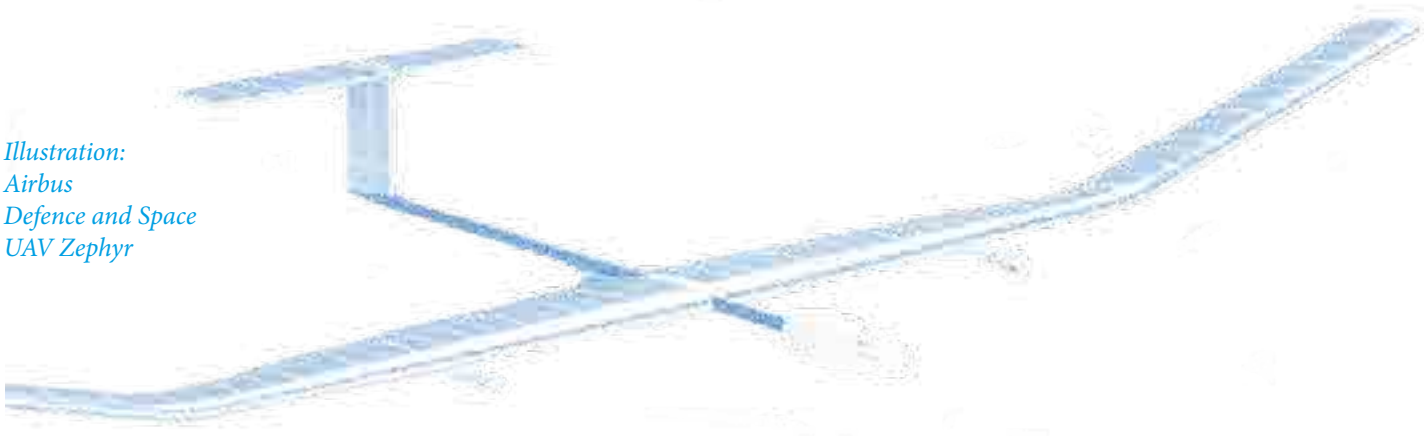


Illustration: Airbus Defence and Space UAV Zephyr

Content

3.7 The European Defence Industrial Development Programme (EDIDP)

While PADR, according to EDF design, was intended to be used for "research", follow-up efforts were supposed to focus on "development" projects. To this end, 500 million euros were made available by the EDF for the years 2019 and 2020 within the framework of the European Defence Industrial Development Programme (EDIDP). The corresponding implementing decision of the EU Commission of 19 March 2019 is strongly oriented towards the CDP of 2018 and lists a total of 19 subject areas for funds to be allocated. In two cases, these funds were awarded directly, i.e. without a call for proposals. For instance, a consortium comprising Airbus Defence & Space, Dassault (France) and Leonardo received a total of 100 million euros from the EDIDP for the years 2019 and 2020 – i.e. one-fifth of the total amount – to develop the so-called Eurodrone. This direct allocation of funds was justified by referencing the strategic relevance of the project and the high technical requirements for the system, which, according to the organisation, meant that the existing consortium had a quasi-monopoly on its implementation. A very similar justification was given for the direct award of 37 million euros for the "development of an interoperable secure defence communications system" (ESSOR) to a consortium of Thales, Leonardo, Indra, Radmor (Poland), Bittium (Finland) and Rhode & Schwarz (Germany).

Four subject areas were scheduled for project tenders, both in 2019 and 2020: cyber security of communication systems (32 million), air combat capabilities, including electronic warfare (34 million), artillery modernisation (13.5 million) and "[i]nnovative and future-oriented defence solutions" by SME (17.5 million). The latter is a special/container category of sorts, designed to give smaller (armaments) companies access to the EDF, again listing more than thirty topics in hopes of receiving "innovative" proposals. The largest amounts were earmarked in 2019 for the development of an autonomous European satellite navigation system, a permanent (AI-based) aerospace reconnaissance capacity and an architecture for the integration of various unmanned ground systems into MUM-T assemblies. In addition to Safran, Diehl and Bittium, this project, led by Estonian company Milrem Robotics, also involves the key players in the development of the Franco-German Main Ground Combat System (MGCS) project with Nexter and KMW. The situation is different in the DRONEDGE-E project, in which "automatic generation of algorithms through artificial intelligence" is supposed to contribute to an "autonomous control of swarms of drones in real-time". Four rather small companies, which have not yet made appearances in connection with armaments projects, are involved in the project, which is funded with almost 2 million euros.

The three subject areas receiving the most extensive funding in the 2020 calls for proposals are the development of underwater robots for various military applications, developments for improved surveillance of space and the further improvement of maritime surveillance capabilities, with just over 20 million euros each. The call for proposals dedicated to "defence technologies supported by artificial intelligence" comes in considerably lower at 5.7 million euros. Here, too, the Commission had suggested highly varied subtopics for project applications, among them systems to support decision-making, "predictive algorithms to anticipate threats/trends through analysis of big data and neural networks" or also support of "recurrent activities such as strategic communication (STRATCOM), logistics planning, airspace management ...".[71]

[71] *C(2019) 2205 final, https://ec.europa.eu.*

Content

3.8 PESCO

While funds under the EDF, i.e. PADR and EDIDP, are allocated supranationally by the Commission within the EU budget, the Permanent Structured Cooperation (PESCO) is an intergovernmental programme financed at least primarily by the Member States, from their armament budgets. However, the aim is to ensure that the two programmes are interlinked. For example, in its fact sheet on EDIDP 2019, the EU Commission emphasised that nine of the 16 funded projects were related to PESCO projects.[72] In the future, PESCO projects would be eligible for up to 100% EDF funding in the research phase, and for up to 30% in the development phase. The Commission and the EDA are thus creating incentives for more ambitious joint Member State armaments projects, at the same time, influencing their design.

PESCO was one of the core elements of the Treaty of Lisbon (2007) and one of the main reasons why this treaty was largely rejected by the peace movement in the European Member States. It enables "Member States whose military capabilities fulfil higher criteria and which have made more binding commitments to one another in this area" to "establish permanent structured cooperation within the Union framework". Within this structure, the principle of unanimity, which is otherwise predominant in defence policy, no longer applies but is replaced in many cases by a qualified majority. The prerequisite for participation is the acceptance of common guidelines for military spending, military projects and troop generation for joint operations, which is subject to regular monitoring and also sanctions regarding compliance. PESCO's declared aim is to strengthen the European defence identity as a prerequisite for a stronger role of the EU in international politics, which is also underpinned by military capacity. However, it was pointed out early on that PESCO could also be a vehicle for developing Franco-German leadership within the European Union and with regard to its armaments industry. It is therefore no wonder that PESCO's implementation took quite a long time after the Lisbon Treaty's entry into force, but advanced very quickly after the announcement of the UK's withdrawal from the EU. Four days after the Brexit referendum of 23 June 2016, the foreign ministers of Germany and France presented a joint paper calling for "Germany and France to work together to develop the EU into an independent and global player step by step. [...] Groups of Member States should be able to establish permanent structured cooperation in the field of defence as flexibly as possible, or to take the lead with individual operations".[73] Finally, this was precisely what occurred. Germany and France vehemently emphasised their intention to activate PESCO, thereby putting Italy and Spain under pressure and, once again, threatening the remaining Member States with a "two-speed Europe". In November 2017, 23 member states ended up signing the notification document – many of them "grudgingly", according to experts.[74] On 11 December 2017, the Council decided to activate PESCO. Since then, only participating states have had the right to vote in the Council in this context.

To participate in PESCO, the Treaty of Lisbon already required Member States, among other things, to

- "bring their defence apparatus into line with each other as far as possible, particularly by harmonising the identification of their military needs, by pooling and, where appropriate, specialising their defence means and capabilities",

- "proceed more intensively to develop [their] defence capacities through the development of [their] national contributions and participation, where appropriate, in multinational forces, in the main European equipment programmes, and in the activity of the Agency in the field of defence capabilities development, research, acquisition and armaments (European Defence Agency) and

[72] *EDA: Fact sheet European Defence Industrial Development Programme 2019, https://ec.europa.eu.*

[73] *Jean-Marc Ayrault and Frank-Walter Steinmeier: "Ein starkes Europa in einer unsicheren Welt" ("A strong Europe in an uncertain world" – 28 June 2016), https://www.diplomatie.gouv.fr.*

[74] *Cf. Jürgen Wagner: PESCO – The Militaristic Heart of the European Defence Union, European Studies on Foreign and Peace Policy No. 1/2019, www.imi-online.de.*

• "take part, where appropriate, in the development of major joint or European equipment programmes in the framework of the European Defence Agency".[75]

In the Council decision on the activation of PESCO, the following obligations, among others, were added or specified:

• regularly increasing defence budgets in real terms;
• successive medium-term increase in defence investment expenditure to 20% of total defence spending;
• increasing joint and 'collaborative' strategic defence capabilities projects;
• Increasing the share of expenditure allocated to defence research and technology with a view to nearing the 2% of total defence spending;

• commitment to support the CARD to the maximum extent possible;

• commitment to the intensive involvement of a future European Defence Fund in multinational procurement;

• commitment to drawing up harmonised requirements for all capability development projects agreed by participating Member States;

• commitment to considering the joint use of existing capabilities;

• Vcommitment to ensure increasing efforts in the cooperation on cyber defence, such as information sharing, training and operational support[76]

[75] *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (document C2007/306/01), https://eur-lex.europa.eu.*

[76] *European Council: Council Decision (CFSP) 2017/2315 (11. December 2017) establishing permanent structured cooperation (PESCO) and determining the list of participating Member States, https://eur-lex.europa.eu.*

Content

3.9 Digitalisation and AI in Early PESCO-Projects

When PESCO was officially activated, most of the first 17 projects were already in the planning stage.[77] Their implementation was decided by the countries participating in PESCO in March 2018. This initial package included the establishment of a "European Medical Command", which would centrally organise medical support and care for joint operations, a "European Union Training Mission Competence Centre" and a "network of logistics hubs in Europe". A central project is entitled "EUFOR Crisis Response Operation Core" and aims to record military capabilities of the Member States that are available for certain tasks and thus to recommend appropriate combinations of multinational forces for crisis operation plans drawn up at short notice.

No less than three projects concern maritime security or the creation of maritime situation overviews involving autonomous systems, which means that they can quite directly take up "civil" security research regarding border security. For instance, the project Harbour & Maritime Surveillance and Protection (HARMSPRO) is intended to "deliver an integrated system of maritime sensors, software and platforms (surface, underwater and aerial vehicles), which fuse and process data, to aid the detection and identification of a range of potential maritime threats". The project "Upgrade of Maritime Surveillance" is to "integrate land-based surveillance systems, maritime and air platforms in order to distribute real-time information to Member States", while another project deals with "Maritime (semi-) Autonomous Systems for Mine Countermeasures".

Two further projects could serve to establish or enable an EU combat cloud in the medium term: "The European Secure Software Defined Radio aims to develop common technologies for European military radios. The adoption of these technologies as a standard will guarantee the interoperability of EU forces [...] thereby reinforcing the European strategic autonomy". Another project (Strategic Command and Control (C2) System for CSDP Missions) aims to "connect users by delivering information systems and decision-making support tools that will assist strategic commanders carry out their missions. Integration of information systems would include intelligence, surveillance, command and control, and logistics systems".[78] Two other projects deal with cyber defence. On one hand, a platform is to be created for Member States to obtain information regarding possible attack vectors and countermeasures. On the other hand, cyber rapid response teams (CRRTs) equipped with "Deployable Cyber Toolkits" are to be set up to support Member States and EU institutions in cyber attacks.

[77] Lucie Béraud-Sudreau et al.: Keeping the momentum in European defence collaboration – an early assessment of PESCO implementation (May 2019), IISS Research Paper, www.iiss.org.

[78] The German Federal Ministry of Defence describes the added value of the envisaged system using the following scenario: "For example, the Council of the European Union might unanimously decide on a comprehensive approach to stabilising a country in the Sahel. Given this circumstance, both EU Member States' armed forces and their civilian police forces would be deployed to combat terrorists and to secure national borders, respectively. To ensure that the individual elements of this integrated approach of the EU/European Union are seamlessly interlinked, the uniform management system developed within the framework of the PESCO project Strategic C2 System would provide information for the decision-makers involved. This information would be provided, for example, in the form of situation overviews or by indicating possible logistics chains. Military and police forces could thus be deployed in a coordinated and effective manner for a sustainable stabilisation of the state in question". Cf. BMVg: Strategic C2 System for CSDP, www.bmvg.de.

Content

3.10 Digitalisation and AI in Later PESCO-Projects

Less than a year later, in November 2018, 17 further PESCO projects were decided. Unmanned systems, MUM-T and swarm behaviour also play a role in many of these projects. In addition to the Eurodrone project, which had already been promoted for years by Germany and France and was transferred to the PESCO framework through this effort, a reconnaissance balloon was intended to be developed as a pseudo-satellite. It is supposed to provide a "[p]ersistent Intelligence, Surveillance and Reconnaissance (ISR) Capability" with "outstanding dual use characteristics". Swarms of manned and unmanned systems were supposed to provide chemical, biological, radiological and nuclear (CBRN) surveillance as a service (CBRN SaaS). The project DIVEPACK is supposed to develop a modular MUM-T system to support divers with unmanned underwater vehicles (UUV). In addition, there are plans for the development of an "integrated unmanned ground system" which can be used for both transport and reconnaissance and features "autonomous navigation capability for route and mission planning with different options for manned-unmanned teaming". A further project aims to develop a separate, joint system to combat drones (counter unmanned aerial system, U-CAS). A new rocket system intended for development, which can be launched from the air as well as from the ground, will also feature "autonomous target designation capability".

Other programmes of the second PESCO package are aimed more towards harmonisation and standardisation. For instance, the Czech Republic and Germany intend to conduct a feasibility study to assess the capacities of the Member States for electronic warfare and to explore the possibilities of a joint system and a "joint EW unit". Two other projects aim to establish European networks for geospatial, meteorological and oceanographic (GeoMETOC) support of EU missions and "military space surveillance awareness", respectively, while another aims to develop terminals using the European satellite navigation network for positioning. In addition, standardisation is intended regarding the procedures for testing and evaluating (new) weapons systems. The upgrade of the Tiger combat helicopter (Mark III), which had been planned for some time and was transferred to the PESCO framework, also relates essentially to the modernisation and adaptation of its communication interfaces and capabilities. Greece and Cyprus announced their intention to jointly develop a C2 system for multinational special operations and to establish a joint EU intelligence school, which will also develop and test new technology. In May 2019 it was also decided to set up a "cyber rapid response team" under the leadership of Lithuania.

The third PESCO package with 13 projects was adopted in November 2019 and does not pursue any further development of unmanned vehicles apart from a maritime unmanned anti-submarine system (MUSAS). However, it again contains a project to prepare the integration of RPAS into civil airspace. The third package especially demonstrates a clear focus on electronic warfare and cyber defence. Spain, France and Sweden, for example, intend to develop a joint system for airborne electronic attacks, which is to be mounted on manned and unmanned aircraft and serves to suppress access to the electromagnetic spectrum and cyberspace over enemy territory. At the same time, an "EU Cyber Academia and Innovation Hub" is created "to develop a technologically skilled workforce, a cyber-savvy ecosystem, and an effective pipeline of future employees". A cyber and information domain coordination center (CIDCC) is planned under German leadership to serve "as a standing multinational military element". Hungary leads planning on the creation of a "tactical training and simulation cloud", "which could connect and integrate the geographically spared simulation sites and training capacities into one real time, joint level simulation platform". The acronym EcoWAR stands for a planned development of "EU Collaborative Warfare Capabilities": "The envisaged outcome of this project will allow the armed forces within the EU to engage together in actions requiring close interactions and interconnections between diverse current and future warfare platform, from sensors to the effectors, in order to foster their efficiency, interoperability, complementarity, responsiveness and their resilience".

In total, 47 PESCO projects have been decided to date. However, the International Institute for Strategic Studies (IISS), subsequent to the adoption of the second package, had already pointed out the fact that for most of the projects, there were no clear timelines and commitments of national budgets, and that the latter depended on further funding from the EDF, whose prioritisation had yet to be clarified.[79] An analysis by the Centre for European Policy Studies also pointed out in December 2019 that the average number of countries involved in a project had fallen from 7.6 in the first round to 3.6 in the third.[80] There is no doubt that the scope and objectives of the PESCO projects demonstrate a clear willingness to carry out extensive and increasingly harmonised modernisation and armament of the participating European armies. At the same time, however, they must also be seen as an expression of the gold rush of the national armaments industries triggered by the establishment of the EDF, and the fact that they are ultimately in competition for the 1 billion euros intended for annual distribution by the EDF going forward. This by no means indicates the extent to which the projects will deliver the proclaimed results. However, PESCO and EDF already have concrete consequences at another level: while national and transnational armaments companies have always had good access to decision-makers at EU level, representation of armaments industry interests has been made an elementary part of EU bureaucracy as well as the representatives of the Member States assigned to it.

[79] Cf. FN 77.

[80] Steven Blockmans and Dylan Macchiarini Crosson: Differentiated integration within PESCO – clusters and convergence in EU defence, CEPS Research Report No. 2019/04 (December 2019, www.ceps.eu.

There is no doubt that the scope and objectives of the PESCO projects demonstrate a clear willingness to carry out extensive and increasingly harmonised modernisation and armament of the participating European armies.

Content

3.11 The Fusion of Armament, Industry and Digitalisation Policy

Under Commission President Ursula von der Leyen which took office in December 2019 fundamental restructuring efforts were carried out in connection with the EDF and digitalisation issues. In her letter of appointment to the Members of the Commission, she clearly issued as a goal that this Commission "will be a 'Geopolitical Commission': what we do now will determine what kind of world our children live in and will define Europe's place in the world". This would also require to "better align the internal and external aspects of our work".[81]

The most significant restructuring measures concerned the Commission for the Internal Market and the newly created Commissioner's Office under the unwieldy title "Europe fit for the Digital Age", which was filled by Thierry Breton, who had previously served as Commissioner for Competition. As one of three Executive Vice Presidents, she will chair a Commissioners' Group. Her task will be "to ensure that Europe fully grasps the potential of the digital age and strengthens its industry and innovation capacity. This will be a key part of strengthening our technological leadership and strategic autonomy". Specifically, she was expected to develop a "long-term strategy for Europe's industrial future", a "new SME strategy", a "European strategy on data" and a "European approach on artificial intelligence". In this, she was to "ensure cross-fertilisation between civil, defence and space industries".[82] The (formerly very powerful) Commission "for the Internal Market", which was filled by Thierry Breton, was also massively restructured and subordinated to Executive Vice President Margrethe Vestager, who in turn is directly supported by the Secretariat-General of the Commission President. As a member of Vestager's working group, Breton is also supposed to participate in drafting the aforementioned industry, SME and AI strategies. Beyond this, Breton's area of responsibility is shaped by the idea of strategic autonomy and geopolitics. Concrete tasks assigned to him include "enhancing Europe's technological sovereignty", the development of a "single market for cybersecurity", strategies for "preventing and countering disinformation and fake information online", and the establishment of a "joint cyber unit".[83] Above all, however, Breton has the responsibilities of an armaments commissioner. He is supposed to promote the development of an "open and competitive European defence equipment market" and a "strong and innovative space industry", thereby improving the "crucial link between space and defence and security". He was also commissioned to implement the Action Plan on Military Mobility. For the first time in the history of the EU, the European Defence Fund has provided him with an armament budget for these tasks, which he is supposed to further design and build upon. He is supported in these tasks by three Directorates-General: the Directorate-General for Communications Networks, Content and Technology, the Directorate-General for Internal Market and the new Directorate-General for Defence Industry and Space.[84]

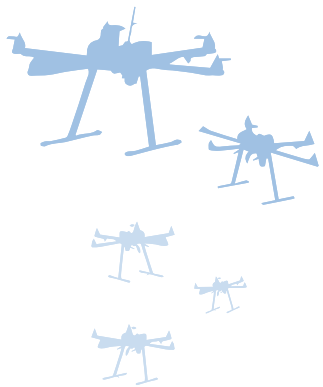
[81] *Ursula von der Leyen: Mission letter Margrethe Vestager (1 December 2019), https://ec.europa.eu.*

[82] *Ibid.*

[83] *Ursula von der Leyen: Mission letter Thierry Breton (1 December 2019), https://ec.europa.eu.*

[84] *Ibid.*

Although Sylvie Goulard had initially been destined for this post – an appointment finally rejected by the European Parliament due to possible conflicts of interest – Thierry Breton seems eminently suitable for a post that could also be called "EU Commissioner for Digital Armament". Before and after his position as French Minister for Economic Affairs under Jacques Chirac, he held top positions in French armaments and electronics corporations and played a leading role in strategic takeovers, mergers, spin-offs and corporate cooperation, which among others resulted in the creation of companies such as Thales and Atos.[85] While Thales is now one of the largest armaments companies in the world,[86] Atos describes itself as "the world leader in digital transformation with more than 110,000 employees in 73 countries and annual sales of more than 11 billion euros". In fact, Atos is active in many business areas in the field of digitalisation and systems integration. In 2011 and 2014 respectively, it acquired the German and French armed forces' most important (private) IT service providers by taking over Siemens IT Solutions and Services as well as the Bull group – both under Breton's leadership. Most recently, however, Atos has also positioned itself solidly in the market for digitalised healthcare services through further strategic acquisitions.



Thales heads the list of the biggest beneficiaries of the EU Commission's research programmes FP7 (2007-2013) and Horizon2020 (2014-2020), with Atos in fifth place.[87] Many of these research projects dealt with questions of sensor technology, sensor-data fusion and human-machine interfaces or even the integration of all these components in an overall system intended to meet cyber security requirements on a quasi-military level under more or less civil scenarios (disaster control, border security, etc.). From optimal circuit design in optical sensors to components for data centres and conceptual considerations of situation awareness in augmented reality, the research funding declared as civil supported projects which the companies were then able to quickly tailor to their military customers. Atos is currently entrusted with the implementation of the Scorpion CIS (combat information system) programme, which harmonises the IT infrastructure of the French armed forces through a common Battle Management Language. At the same time, Atos is not only the most important private provider of "white IT" for the German Bundeswehr, but is also entrusted with implementing a battle management software jointly with Rafael.[88] While Thales also manufactures missiles and warheads, the company plays a central role, at least in Europe, in "tactical radios and on-board communication solutions for land, air and naval forces" and in hardware for the aerospace industry. Supply chains in this field are well coordinated with Europe's largest defence contractor, Airbus (third among the largest beneficiaries of the Commission's civil research funding), with whom Thales is developing the Air Combat Cloud for the Future Combat Air System. This means that Atos, Thales and Airbus are the designated key players to represent the basis for a harmonised ICT among European armed forces, which can be regarded as a prerequisite for the major EU armament projects regarding MUM-T – and which will force the hand of other EU armed forces and bind them to the participating suppliers.

[85] Christoph Marischka: "(Diese) Industriepolitik ist Rüstungspolitik" ("(This) Industrial policy is armament policy"), Telepolis (12 November 2019), www.heise.de/tp/.

[86] In 2018, SIPRI ranked the company in tenth place among the top 15 arms producers worldwide (excluding China) with a turnover of 9.5 billion US dollars in the arms business out of a total turnover of 18.8 billion US dollars, cf. https://www.sipri.org.

[87] As of 2017, cf. Kai Biermann and Christian Fuchs: "800.000 Euro für einen Terror-Airbag, der nie fertig wurde" ("800,000 euros for a terror airbag that was never completed"), Die Zeit (23 February 2017), www.zeit.de.

[88] ATOS: Scorpion combat information system – Data at the Heart of the Battlefield, https://atos.net.

IIt is interesting to note that the appointment of Breton as Commissioner for Internal Market was made under a German Commission President. After all, Breton stands for an industrial policy which is often referred to and criticised by the German side as "state capitalism".[89] The strategic mergers that led, among other things, to the current position of Thales and Atos (and also, for example, of STMicroelectronics) were repeatedly driven and enabled by the French state under the interim Minister of Economic Affairs through share takeovers and other (industrial) policy measures, which is notoriously rejected in Germany as an intervention in competition. The most famous deviation from this course of the German governments consisted in the strategically and politically promoted foundation of Airbus, which was to intended to counteract the market power of Boeing – and, given its military relevance, was to form the basis of a European aerospace industry. However, the recent intensification of Franco-German cooperation and European leadership, especially as a result of the Brexit, encouraged a shift in thinking on the German side. In both countries, for instance, the joint venture of the two largest tank manufacturers – Krauss-Maffei Wegmann and Nexter Systems – received political support, particularly with a view to the joint development of the Main Combat Ground System.

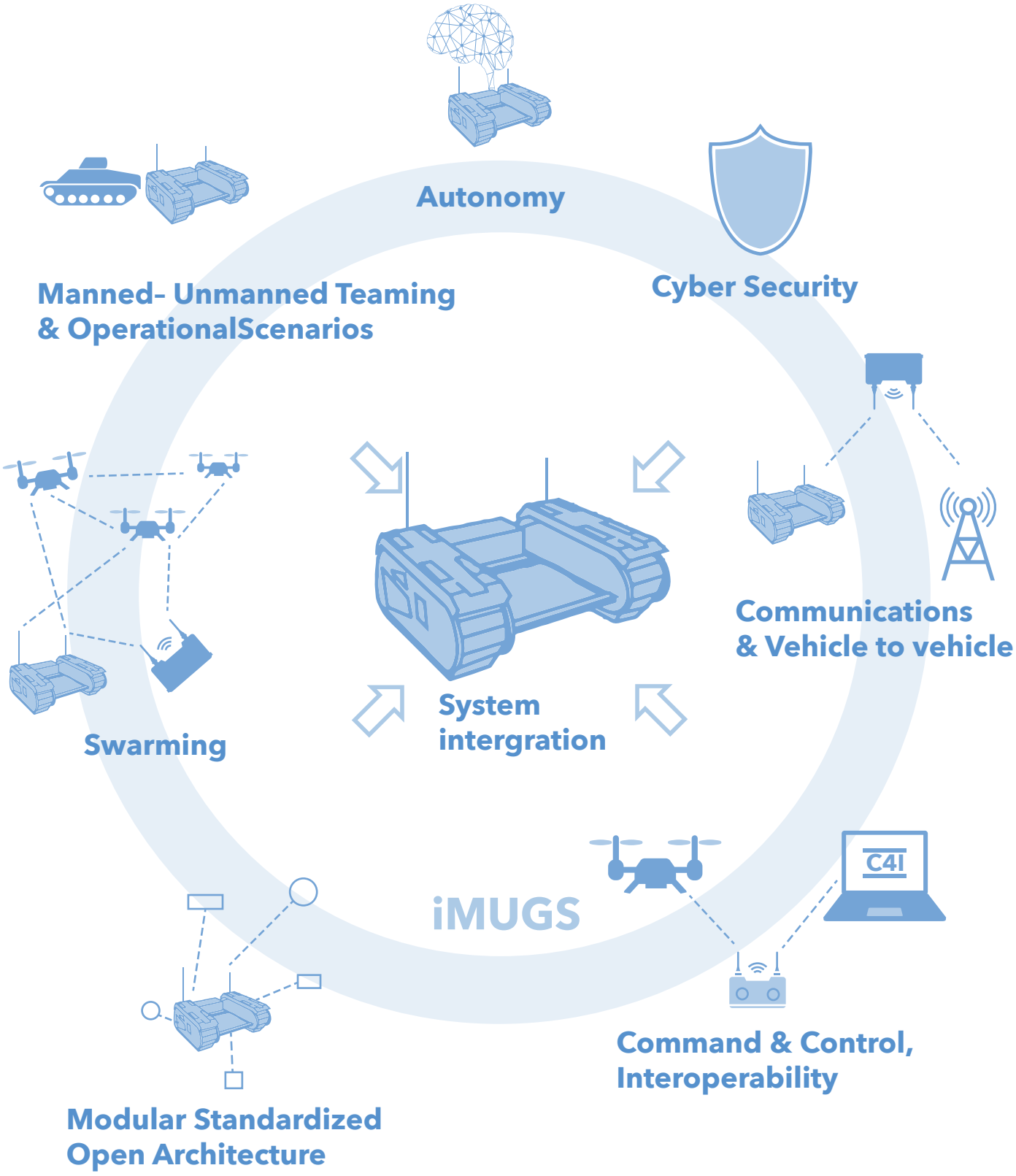
In February 2019, quite shortly after the new Commission under von der Leyen took office, German Minister for Economic Affairs and Energy Altmaier published a draft for a "National Industrial Strategy 2030",[90] which was castigated by more ideologically inclined liberal commentators as a departure from the principle of free competition. Indeed, the draft called for a review of existing state aid and competition rules and, where necessary, their reform to allow temporary aid "in areas of innovation with a highly innovative base effect". Particularly "regarding the overriding issues of platform economy, artificial intelligence and autonomous driving", "direct state involvement appears necessary and justified to achieve the goal, as in the case of Airbus at the time". In brackets, this possibility of state-sponsored or forced mergers to form a German-European corporation capable of rivalling "competitors from the USA or China on an equal footing" is referred to as "AI-Airbus".

As in the case of Airbus, a possible AI-Airbus would essentially result from a merger of German and French companies and would be under the joint political control of both states. In the field of research, at any rate, both countries are already making progress and are currently planning to establish a Franco-German research centre for artificial intelligence. In preparation, both countries are currently establishing corresponding research clusters, which are to be networked with each other in a second development stage.

[89] For instance, the article"France calls for revision of EU competition rules" by Aline Robert, Euractiv (4 June 2019), www.euractiv.de only features the polemic headline "Mehr Staatskapitalismus wagen" ("Taking a chance on more state capitalism") in its German version.

[90] Federal Ministry for Economic Affairs and Energy (BMWi): "Nationale Industriestrategie 2030" ("National Industrial Strategy 2030" – February 2019), www.bmwi.de.

Content


Autonomy
Cyber Security
Manned- Unmanned Teaming
& OperationalScenarios
Communications
& Vehicle to vehicle
Swarming
System
intergration
iMUGS
C4I
Command & Control,
Interoperability
Modular Standardized
Open Architecture

4.1 A Combat Cloud of Projects

The research programmes presented above, which should be understood as preparation and implementation of the EDF, suggest the following tactical and strategic consequences:

• There is a clear will to **massively arm and modernise** the European armies and to strengthen the capabilities and autonomy of the European Defence Technological and Industrial Base (EDTIB). Strategically, neither of these can be justified by the supposed necessity for (internationally uncontroversial) crisis management operations, but only by the goal of being perceived as a competitive military actor alongside the USA and China, and at least being able to control areas in which the latter two pursue opposing interests.

• **AI applications** play a role in almost all projects aimed at modernising and upgrading European armed forces and will significantly change them, particularly in the form of increasingly autonomous systems, an ever greater consolidation of situation overviews and the acceleration of warfare. Approaches to the development of a super AI based on Big Data and machine learning, which also characterises economic and, increasingly, popular discourse on AI, remain in their early stages to date. None of the armament projects examined are clearly aimed at collecting large amounts of data from manoeuvres, CSDP missions or real combat, if only for training and simulation purposes, let alone analysing them in combination with data sets from civilian environments using self-learning algorithms. Efforts to build the infrastructures considered necessary (in economic discourse) to bring together immense amounts of data and computing power remain indiscernible (cf. 4.3.).

• The central themes of the armament projects are **autonomous vehicles, swarms and manned-unmanned teaming**. The EU likely has a special interest in such technologies as "force multipliers" due to its relatively low mobilisation potential (or rather, share in the world population). Tactical restructuring of the armed forces around unmanned systems is already apparent and it seems realistic that these will be integrated as standard in many units within a foreseeable time frame of about ten years. This restructuring is already well advanced with regard to reconnaissance systems; rapid implementation can also be expected for assistance systems (e.g. for transport) and electronic warfare. Within the framework of the MGCS or the PESCO project iMUGS, systems approximating the popular idea of killer robots are also being developed. However, their realisation depends on the extent to which social resistance to such weapons systems can be overcome. From a strategic point of view, it can be noted that while most projects – as a side effect, so to speak – open up dystopian opportunities in terms of internal security, they are strategically oriented towards an offensive approach by assuming that they will be deployed in a hostile or at least contested area.

• This applies all the more to **capabilities in the domain of space**. Although the development of European pseudo-satellites explicitly addresses their "dual use", they are primarily useful for monitoring contested or hostile areas or corresponding border regions beyond the range of smaller (unmanned) reconnaissance systems in military terms. The same applies to satellite communication and the space awareness that is supposed to ensure said communication: it is of particular interest for missions beyond a state's own territory in scenarios in which other states (or similarly powerful actors) possess space weapons. As sensible as it may seem at first to develop satellite navigation systems that can operate independently of (US-controlled) GPS, this also includes, at least in the military context, the implication of taking military action against the will of the USA, if necessary.

• There are clear approaches to approximating a **European Combat Cloud** by means of a harmonised digitalisation of the European armed forces. Germany and France in particular are pursuing this goal primarily within the framework of their industrial policy and, on a small scale, through armament projects in which AI-based decision support systems are also being implemented. The PESCO programme "Strategic C2 System" at minimum aims at a corresponding networking of tactical and strategic levels (cf. FN 78). The harmonisation and standardisation of European armed forces' ICT also represents an attempt to move closer to the goal of a "European Army" starting from a base in technology and the armaments industry. Indeed, a rapid and inclusive modernisation of European armed forces' ICT could, in one fell swoop, give the EU a completely different military importance – were it possible. After all, the USA, following more than 20 years of massive and targeted armament efforts, is still far removed from the ideal of network-centric warfare that spans all armed forces branches and extends from the tactical to the strategic level. For the EU, obstacles are much greater, since (taking PESCO as a reference) it is a group of 25 sovereign governments with different political and strategic cultures and as many armies with different basic equipment. The implementation of a European Combat Cloud is therefore likely to remain a decade-long effort – and one that is likely to supply the armaments industry with extensive orders for just as long.

• Efforts to **influence regulation, logistics and organisational structures** are also highly discernible. This is particularly evident in the efforts to give unmanned military aircraft access to airspace by digitalising and automating the organisation and control of said airspace. Similar aspects are suggested by the projects Military Mobility (of the Commission) and Enhanced Logistics (of the DFA). In any case, it is striking that many projects implicitly assume that the integration of unmanned vehicles into civil (air) traffic will be realised in the foreseeable future.

• **Cyber and information warfare** is defined as the domain of warfare and a military task in the long term, entirely without question. A clear demarcation from civil institutions is not discernible, nor are efforts at international regulation. It must be expected that the numerous programmes of European cooperation at the level of military cyber defence will soon outrival the capacities of Member States' civil authorities. Since there is no conceptual distinction between states of war and states of peace in the cyber and information space, military or hybrid organisations are thus also assigned a permanent task.

Content

4.2 A Technology-Driven, Offensive Strategy

As mentioned several times, the current wave of armament and the goal of strategic autonomy can only be understood in the context of an offensive foreign and military policy strategy. The aim is to become independent of the USA, China and other major players in terms of armaments and industrial policy and to be able to compete with them on a global level. For some Member States, at least, this also includes pushing back NATO's role in defence in favour of an EU army being established – although this is already disputed among the Member States. It is less controversial to take a more confrontational approach to Russia and to back up said approach with threatening gestures and the development of corresponding military capabilities at EU level. This is particularly relevant since Russia is accused of hybrid warfare, which places the EU in a latent state of war that can serve as justification for the armament measures.

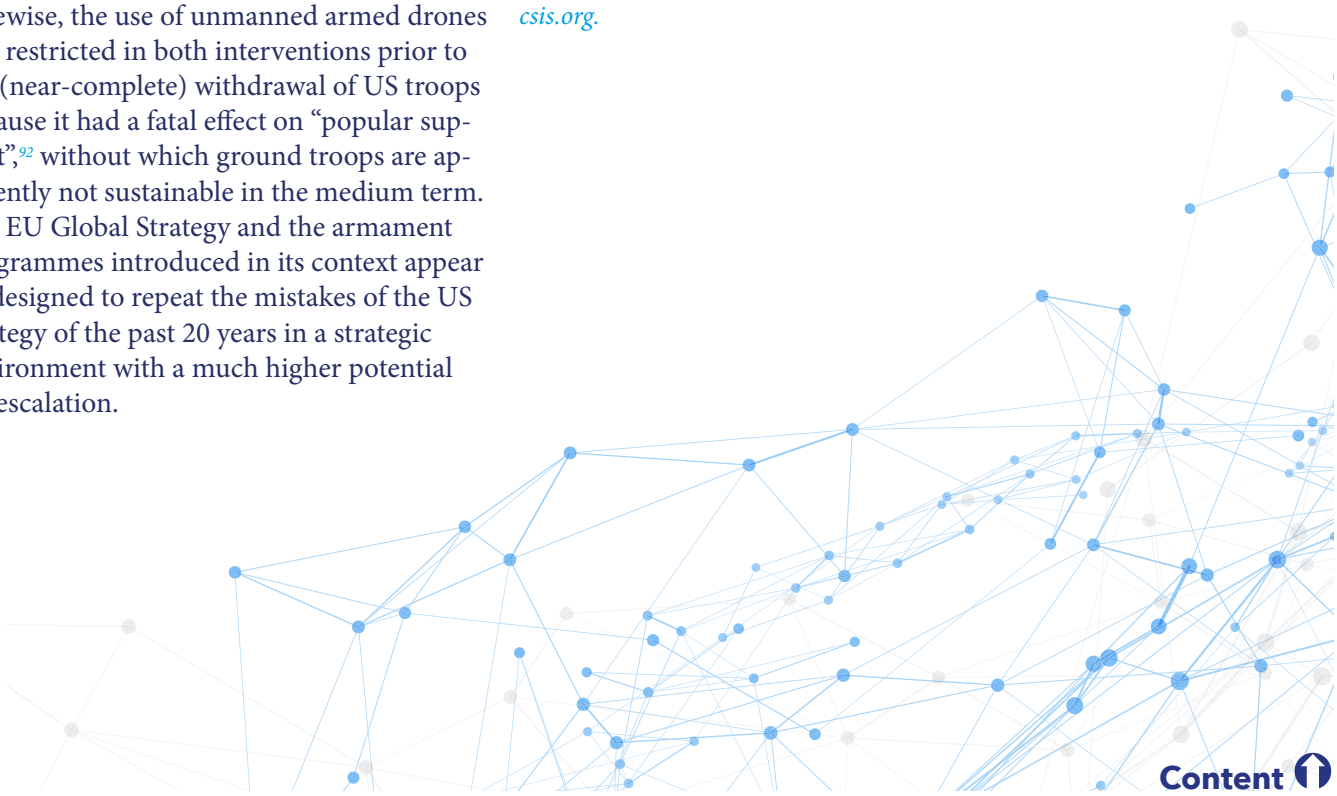
However, this strategy does not go much further. As stated, the concrete relationship with the USA and NATO is extremely controversial within the EU. A uniform strategy towards China – beyond economic containment, for instance in the course of strategic autonomy – is not yet discernible. The sabre-rattling towards Russia in principle is just as consensual as the expectations and the willingness to actually risk an immediate armed conflict in this regard are different. In short: a common strategic culture is still a long way off.

It is foreseeable, however, that the CSDP will increasingly focus on dominance in the area defined by James Rogers as the "Grand Area" in the future. This is also consistent with the more realistic of the targeted armament programmes. Unmanned systems and MUM-T are mainly used in the immediate vicinity of the EU, in the Mediterranean, where they are primarily used to combat illegal migration, but increasingly also to monitor and enforce embargo measures. The CSDP is already trying to gain control of large parts of northern and western Africa – which it has defined as the Sahel region – through the use of surveillance technology, training and instructing local "security forces" and a manageable number of ground troops. However, the deaths in the Mediterranean, the catastrophic situation in Libya, the escalation in the Sahel region and, most recently, the coup in Mali illustrate very clearly that information superiority or even a consolidated situation overview do not necessarily equal more control. The same applies to the Horn of Africa, parts of the Arabian Peninsula and the Persian Gulf, where European Member States, often in a NATO alliance, sometimes achieve massive degrees of reconnaissance consolidation without being able to claim any significant strategic successes. Massive investments in maritime armament also confirm an urge for a stronger presence in the Baltic Sea, the far north (Arctic) and the Indian Ocean as well as the South China Sea. It is unclear whether and under what conditions there is a willingness to use lethal force and to enter into armed conflict. However, the probability increases with the EU Global Strategy and the associated armament programmes.

Whether unmanned systems offer a tactical advantage in the event of a military conflict is by no means certain. The more salient question is if, like other technological innovations, they might instead have the potential to provoke strategic errors. For instance, the US-led 1991 Operation Desert Storm in Iraq, when an "impressive array of high-technology weapons ... allowed the U.S.-led coalition to overwhelm the world's fourth largest army in a remarkably short time … and with minimal losses",[91] to this day is classified as the most striking proof of the tactical advantages provided by (information) technological superiority. At the same time, however, it can be seen as the beginning of a type of US warfare, in which wars – at least in their initial phase – were associated with low losses and corresponding political costs on the part of the US, but ultimately resulted in costly and loss-ridden deployments of ground troops measured against expectations, as was the case in Afghanistan in 2001 and again in Iraq in 2003. Both interventions can now be clearly identified as strategic mistakes. Likewise, the use of unmanned armed drones was restricted in both interventions prior to the (near-complete) withdrawal of US troops because it had a fatal effect on "popular support",[92] without which ground troops are apparently not sustainable in the medium term. The EU Global Strategy and the armament programmes introduced in its context appear all designed to repeat the mistakes of the US strategy of the past 20 years in a strategic environment with a much higher potential for escalation.

[91] *Norman Davis: An Information-Based Revolution in Military Affairs (1996), U.S. Strategic Institute Strategic Review, Vol. 24, No. 1, www.rand.org.*

[92] *Cf. Anthony Cordesman: The Real Revolution in Military Affairs (5 August 2014), CSIS Commentary, www.csis.org.*



Content

4.3 The Real Drivers: Industry and (Venture) Capital

The journal European Defence Matters, published by the EDA, contains a small emphasis (5 of 44 pages) on the topic of artificial intelligence in its issue 19 of June 2020. It starts with a sort of special report by the EDA itself regarding its activities in this field and also includes an interview with Christian Hedelin, Chief Strategy Officer at Saab. After a brief introduction, the special report begins with a quote from Panagiotis Kikiras, the EDA's head of unit for technology and innovation: "AI is not new for the defence world. There have been a lot of expectations pinned to it since the end of the Second World War: many trends and crazy predictions that have promised so much, only to fade away". Hedelin also does not appear very excited: "AI is already integrated and working in today's systems … Traditionally, AI is often used for decision support … Our first steps in this area date back more than 25 years". The EDA, which was set up in 2004 and massively upgraded with the EDF and PESCO, describes its activities in the field of AI rather cautiously. Since early 2019, work had supposedly begun on a common definition, taxonomy and a glossary. Currently, the institution claims to be in consultation with the Member States and intending to present an AI action plan by the end of 2020. This much is conceded: "[T]his latest wave in AI's evolution has been different. Enablers that were not around in the 1980s and '90s such as massive processing power and huge databases of near-real time information are accelerating". This is why EDA has "proposed [...] to create a repository, or 'data lake', of less sensitive but anonymous military operational data on vehicles, air platforms and so on". In terms of application, the EDA sees predictive maintenance as a concrete area, and autonomous systems and decision support systems as a general one with regard to AI – albeit with limitations: "At the tactical level, AI is more about the intelligent automation of functions, like those on platforms aiming for autonomous systems. But at the strategic level, this goes straight to (AI-enabled) intelligence and support to decision-making, which immediately gets more complicated for cooperation, given the sensitivities from the different parties". Hedelin of Saab also mentions autonomous systems and predictive maintenance as possible fields of application in addition to the traditional application of "decision support". Yet, he does not neglect issuing a demand "to put even more effort and investments into AI and machine learning … This would include infrastructure for more computational power, both for crunching of Big Data and for training of Deep Learning networks. The EU could invest in Super Computer Centres for both the industry and the EU's Member States Armed Forces to use for testing different platforms. It would be very costly for companies to develop these themselves on a large scale".[93] Er antwortet dabei auf die Frage: „Was sollte getan werden, damit die Verteidigungsindustrie in der EU ihre führende Position bei KI zukünftig aufrechterhalten kann?".

This is his answer to the question "What should be done in order to keep Europe's defence industry in a leading position within AI in the future?".

The discourse reproduced here is an example of how the armament perspective differs from the prevailing discourse on AI, which suggests an ongoing arms race because of imminent disruptive innovations, and "Europe" having missed this development. In the armaments and military sector, where the relevant technologies have been in use for decades, the assumption seems to be that technological innovation will continue on its path and that Europe is well-positioned instead. Nevertheless, the hype naturally is utilised as an opportunity to call for more public innovation.

[93] *EDA: EDM – European Defence Matters #19 (June 2020), https://eda.europa.eu.*

So, where does the discourse about the impending disruptions and the impending decline of Europe originate? Its main sources are the pressure groups of industry and capital, as well as the politicians close to them.[94] It was the current Commission President von der Leyen, for instance, who is now pushing forward the integration of armaments and digitalisation with great energy at EU level, who had previously promoted it in her function as Defence Minister in Germany. To this end, she appointed Katrin Suder as State Secretary of Defence, who had previously headed the German branch of consulting firm McKinsey. During her term of office, numerous contracts were presumably awarded irregularly to this and other consulting firms in this context, which was the subject of an investigation committee of the German Bundestag until September 2020.

Like armament, digitalisation is a mechanism of redistribution and the motto "if you don't digitalise, you lose" ensures that it is the large companies and corporations that win. In times of austerity and also pandemic-related economic stimulus packages, the question arises very specifically whether to invest in the training of nurses, healthcare staff and teachers, or to digitalise health, education, etc. with the help of big industry and consulting firms, while at the same time providing billions of euros for industrial and industry-related research and development.

Companies such as Roland Berger and McKinsey are promoting the political creation of "ecosystems" for this purpose, particularly in the field of AI, with start-ups at the centre of attention, which are to transfer the results of (publicly funded) research into applications and commercialise them with the help of venture capital. Supposedly, this is the only way for Germany and Europe not to lose ground to China and the USA. Accordingly, the public sector is required to invest in technology research oriented to industry and application, establish research and start-up clusters, facilitate business start-ups through financial support and deregulation of labour and tax law, exempt capital yields from investments in these areas from tax or even oblige health insurance funds, pension funds and pension funds to invest in venture capital themselves.[95] Much of this is already implemented by means of European and national legislation and is included in the Corona economic stimulus packages. This is a gigantic redistribution programme according to the motto of socialise costs, privatise profits. It is advertised to the public using classical location logic, only enriched geopolitically with the fear of a Chinese or US-American super-AI.

[94] The author already elaborated on what has been observed here using the example of EDA and PESCO at the European level for the German discourse on disruptive innovations, with the management level of large research institutes and entrepreneurial scientists appearing as further actors here. Cf. Christoph Marischka: "KI und Geopolitik – Die unheilige Allianz von Risikokapital, Wissenschaft und Politik" ("AI and geopolitics – The unholy alliance of venture capital, science and politics" – 2020), AUSDRUCK No. 100, www.imi-online.de.

[95] Cf. Roland Berger/ Asgard: Artificial Intelligence – A Strategy for European startups, https://asgard.vc.

One example of many is Fabian Westerheide, who describes himself as an "international expert on Artificial Intelligence strategy, entrepreneur and venture capitalist" who "advises governmental institutions including the European Commission, European Space Agency, German parliament, Chinese ministry of technology and departments such as the secretary of defense and foreign ministry ...". One of his frequently held public speeches is entitled "Europe's Strategy for the Global AI Arms Race".[96] Medium.com reports on Westerheide's views as follows: "Europe, once caught in the middle of an epic arms race between two nuclear superpowers, now finds itself in the shadow of a race to master artificial intelligence, according to a German investor and AI expert, who adds that the stakes are just as high for Europe as they were during the Cold War, if not higher … Both the United States and China have big national defense budgets and strong research universities and institutions that facilitate investment in AI research and development. In the United States, billions of dollars in defense research projects and competitions — funded, for example, through DARPA — are eventually funneled into companies in the Silicon Valley and other American tech hubs".[97] On the surface, the "Joint European Disruptive Initiative" (JEDI) is an organisation that labels itself "The European DARPA". Yet, unlike DARPA, it is primarily a network of venture capitalists "powered by 3,700 leaders of Europe's deep tech ecosystem in 23 countries" according to its own statements, and has so far made rather unsuccessful efforts to obtain public funding and recognition.[98]

Boasting is a part of business in this area, since money is earned, or rather redistributed, with expectations. Naturally, the armaments industry is jumping on this hype, and naturally, technologies will emerge that will sooner or later be used on the battlefields. That is, unless the European Union abandons its policy of armament and digitalisation and instead seeks social solutions to social problems. This would also mean that less money would be available for armament programmes and states would have to disarm. Consequently, Europe would have to adopt a defensive strategy and contemplate how to achieve actual security through much simpler and cheaper means. For instance, this could mean banning autonomous weapons and disclosing (and thus enduringly disarming) all cyber weapons. Not against China, Russia and the USA, but alongside them and all states that cannot keep up in the arms race anyway.

[96] *Cf. www.fabian-westerheide.de.*

[97] *Matt Swayne: Investor, AI Expert Says Europe Must Act Now in Global AI Arms Race (11.9.2018), www.medium.com.*

[98] *Cf. https://jedi.group/. Occasionally, JEDI is referred to as a Franco-German initiative and suggests that the respective governments are involved. Regarding the German government's position on JEDI, however, cf, German Bundestag: Printed paper 19/5679.*

Content

Imprint

Author: Christoph Marischka

Design: Thorsten Hädicke

Printing: Der Faltschachtelprofi GmbH, Solingen

Edition: 250 copies, November 2020

The study can be downloaded from the websites indicated.

As a printed brochure, the study can also be requested by e-mail at
bestellungen@oezlem-demirel.de

Published by:
THE LEFT Group in the European Parliament
73, Rue Belliard
TRI 07V003
B-1000 Brussels (Belgium)

www.guengl.eu

GUE/NGL THE LEFT IN THE EUROPEAN PARLIAMENT

DIE LINKE. IM EUROPAPARLAMENT

Photos:
Titel: Milrem Robotics, THeMIS 5th generation UGV, CC BY-SA 4.0
Grafic: Starline, Freepik.com

Content