NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

SCIENCE AND TECHNOLOGY COMMITTEE (STC)
SUB-COMMITTEE ON TECHNOLOGY TRENDS AND SECURITY (STCTTS)
REPORT

TECHNOLOGICAL INNOVATION FOR FUTURE WARFARE

Report
Njall Trausti FRIDBERTSSON (Iceland)
Rapporteur

025 STCTTS 22 E rev.1 fin – Original: English – 20 November 2022

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This report was adopted by the Committee at the 68th Annual Session of the NATO Parliamentary Assembly. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.

EXECUTIVE SUMMARY

The future is fraught with uncertainties and envisioning the future of warfare is a difficult task, particularly as warfare is shaped by geopolitical, societal, technological, economic, environmental and military trends. Too many analyses focus on the issues of today and do not include the unexpected changes in society, technology or politics.

In contemplating warfare, we tend to prepare for the last war, think in obsolete military concepts or focus on previous battle-winning capabilities, which are, or will soon be, outdated. The international security environment is rapidly changing, and Russia’s unprovoked invasion of Ukraine has created a seismic shift in the security landscape. The Alliance therefore needs to anticipate and adapt to new, emerging security risks while maintaining its focus on deterrence, defence and cooperative security.

The Rapporteur raises the question of as to what warfare of the future may look like. He focuses on technological aspects, particularly on the likely impact of Emerging and Disruptive Technologies (EDTs). He also offers some preliminary observations of the Ukraine war and its possible implications for future warfare. Moreover, the report also provides a brief overview of NATO’s continuing adaptation process to make the Alliance fit for future warfare.

TABLE OF CONTENTS

I- INTRODUCTION

1. NATO Allies face an increasingly complex security environment. An aggressive Russia started a full-blown war against a close NATO partner nation in Europe, China is pursuing assertive policies, which challenge the interests and the security of Allies. Moreover, the threat posed by terrorist groups continues. At the same time, NATO's potential adversaries continue to develop and improve their military capabilities. Finally, other factors like climate change and the ongoing COVID-19 pandemic impact our security.

2. In Article 3 of the Washington Treaty, NATO member states commit to develop their military capabilities: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." To advance the adaptation of the Alliance to this fast-changing security environment, NATO Heads of State and Government endorsed the Secretary General's NATO 2030 agenda at the 2021 Summit. The new 2022 Strategic Concept is another key document that will guide NATO's future strategic adaptation. Moreover, as an important part of this adaptation process, NATO military authorities have developed a strategic framework for the future, in which Allied Command Transformation's (ACT) NATO Warfighting Capstone Concept (NWCC) plays an integral role.

3. The future conduct of warfare will be shaped by geopolitical, societal, technological, economic and military trends. However, many of the future threats the Alliance will face will result from technological developments. Emerging and Disruptive Technologies (EDT) can revolutionise future military capabilities and the ability to conduct warfare. The promotion of technological innovations and their timely introduction into the military will therefore play a major role in the development of military capacities of NATO countries. The focus of this report is therefore on technological issues.

II- THE CHANGING CHARACTER OF WARFARE

4. Warfare can take place in many different forms, ranging from high-intensity conventional warfare between near-peer adversaries to counter-terrorism and counter-insurgency operations to warfare in the digital sphere. As security risks evolve and the nature of warfare is changing, NATO Allies need to adapt their capabilities accordingly. After the 9/11 attacks against the United States, NATO militaries started to focus on the threat posed by terrorist groups and instability, gearing their armed forces for counter-terrorism and counter-insurgency operations as well as stability missions. Russia's invasion of Crimea in 2014 led to a change in priorities and NATO nations began to readjust their militaries for major wars again. Russia's unprovoked war against Ukraine vindicated this adjustment as it was a stark reminder that a full-scale war between European nation states is still possible.

A. TRENDS SHAPING CONFLICT AND WAR

5. **The transition from conflict to full-scale warfare is fluid**. Russia's warfare against Ukraine is primarily a conventional war in which traditional weapon systems, especially artillery, play a decisive role. At the same time, warfare and violent conflicts are also increasingly taking place below the kinetic level. Hostilities are not formally declared, what defines "victory" may not even be clear. The Russian attack against Ukraine was waged without a declaration of war. President Vladimir Putin described the invasion of Ukraine as a "special operation". Russia has pursued "grey-zone warfare" since 2014 with its direct support of the so-called "Donetsk and Luhansk People's

Republics". In the grey zone, attackers use disinformation, cyber-attacks, organised crime and other soft tools, often unnoticed and without possible attribution, to undermine the institutions and political processes of their adversaries and their will to fight. Examples include Russian efforts to influence elections in NATO member states and continuing disinformation campaigns by Russia, China and others to undermine confidence in the measures taken by governments in the COVID-19 pandemic. Mis- and disinformation campaigns are increasingly relevant. Even private companies start offering "disinformation as a service" to governments and private customers (Uchill, 2019).

6. **The role of non-state actors in warfare is increasing**. The Wagner Group, a private mercenary group created in 2014 by Yevgeny Prigozhin, a Russian oligarch with close ties to Vladimir Putin, has been active in numerous conflicts around the world, including in Syria, Libya, the Central African Republic and also in Ukraine. The involvement of non-state actors in warfare offers plausible deniability for the states who support their activities. In particular, autocratic states may use these groups more frequently in future conflicts. The "declaration of war against the Russian government" by the hacker group "Anonymous" following the Russian invasion of Ukraine in February 2022 is another example of the increasing role of non-state actors in warfare. "Anonymous" claimed that it successfully pulled down websites of several Russian government agencies as well as those of Gazprom and Russia Today, the state-controlled Russian news agency. Moreover, Ukraine generated an "IT Army of Ukraine", comprising many thousand civilians with IT and internet expertise who volunteered to fight a "digital war" against Russia. This was made possible because Ukraine's comparatively advanced IT sector fields numerous cybersecurity companies and a relatively large pool of talented engineers (Labott, 2022). Moreover, Ukraine has also been pursuing a cryptocurrency crowdfunding effort designed to fund Ukraine's civilian resistance. By mid-March the fund had raised about USD 70 million in crypto donations (Labott, 2022).

7. **Urbanisation** is one of the most prevalent global trends of the 21st century. An estimated 55% of the world's population live in urban areas; according to the 2016 United Nations World Cities report, this figure will increase to about two-thirds of the global population by 2050. More than half of the world's violent armed conflicts take place in cities, affecting some 50 million people (ICRC, 2020; UN 2020). The continuing instability on NATO's southern and south-eastern flanks and the trend towards urbanisation make it likely that the urban environment will be a relevant factor in many future conflicts involving NATO forces (Michel-Kleisbauer, 2020).

8. **Climate change** presents an increasing risk for international security. (GMACCC, 2014). Extreme and variable weather conditions, higher temperatures, droughts, floods, wildfires, storms, sea-level rise, soil degradation and acidifying oceans threaten infrastructure, health, water and food security (Coats, 2019; Lavikainen, 2021; Migdon, 2021). Climate change is already affecting the planning and conduct of military operations, damaging military bases and infrastructure and straining military forces' resources when providing support for dealing with climate change-related disasters (Cohen et al., 2020). Moreover, the role and contribution of the military and of operations to climate change and questions on military carbon emissions and military efforts to reduce their carbon footprint come to the fore. Experts now start tracking direct and indirect emissions during and after conflicts and examine direct emissions from military operations[1] (Darbyshire, 2021). **Climate change** and **high population growth** in some parts of the world may lead to growing competition

[1] This includes, for example, monitoring the energy use at military bases and fuel use from the operation of military equipment – such as aircraft, naval vessels and land vehicles – are often seen as the main contributors to military greenhouse gas emissions (GHG); military equipment procurement and other supply chains that account for the majority of military emissions; military estates especially in vulnerable areas, waste management.

over natural resources, which could lead to state failure, violent conflicts and uncontrolled migration movements.

9. However, **the changing character of warfare is primarily driven by progress in and access to technologies**. The adoption and application of technology, often in novel ways, plays a crucial role in the changing character or warfare.

10. **Data and digitalisation become ever more important**. Digitalisation turned the digital, information and cyber domain into an operational environment and a new theatre of contestation, unlimited by geography. New technology will shape new military concepts and add another layer to our very understanding of proximity. Potential threats from cyber-attacks or attacks on our space assets are not measured by their geographical closeness. They can be launched from the most remote and distant corners.

11. Conflicts will increasingly revolve around information control and include cyber information operations to counter an adversary's narratives. Ransomware and malware attacks are increasing at a rate of 400% per year and have spread globally (Brown, 2021; Goddard, 2021). Cyber espionage and cyber sabotage will take a more prominent place on the agenda, requiring strengthening cyber defences and cyber intrusion detection methods, as well as resilient and redundant networks (Cohen et al., 2020). Critical infrastructure and hi-tech companies are prime targets for state and non-state actors. According to the annual risk survey of the international insurance broker WTW, nearly 75% of companies expressed concern about state-sponsored cyber-attacks, while over 50% are worried about government-led retaliation against private companies in international diplomatic disputes (Braw, 2022). Allies are facing the challenge of addressing cyber-linked vulnerabilities in weapons systems. (GAO, 2021). The increasing interconnectivity that 5G provides allows for the combining of multiple services and covers the entire frequency spectrum through one single and unified technology.

12. **The importance of geography, particularly geographical distance from potential opponents, is changing**. While warfare in the past involved, first and foremost, soldiers on the front lines, warfare can now be waged over long distances, affecting both military and civilian targets. Technological progress in the **cybersphere and** in **space** undermines the relevance of geography and adds new critical security frontiers. In fact, NATO has designated both cyber and space as operational domains, where an attack can trigger Article 5 of the Washington Treaty. In the **space** domain, decreasing launch costs and technology transfers will progressively enable other nations like Iran or North Korea as well as private companies and non-state actors to engage in space activities (Brunner, 2021). Both a possible "weaponisation" of space and the application of cyber tools would enable potential adversaries to attack NATO member states' military and civilian infrastructure from afar, so resilience is becoming of crucial importance.

13. **Easy access to technologies**. The easy and increasing availability of ever more sophisticated commercial off-the-shelf technology empowers weaker and technologically inferior opponents, including terrorist groups and other armed non-state actors. For example, in Iraq and Afghanistan, insurgents have used mobile phones to activate Improvised Explosive Devices (IEDs). IEDs have caused the most casualties in operations among Allied soldiers and thus became a significant operational threat. Unmanned Aerial Vehicles (UAVs) are being used by both national militaries and non-state actors and are becoming ever more capable and miniaturised. The digital transformation empowers new actors and incites new competition. The number of state and non-state actors empowered and equipped to use cyber toolkits, for instance, has been increasing significantly (Coats, 2018). Thus, the availability of sophisticated dual-use technology to one party of a conflict can make it difficult for the opponent to utilise its technological advantage.

Ukraine war – preliminary observations

Russia’s war against Ukraine is the largest military conflict in Europe since the Second World War. Although it has brought to bear the importance of conventional capabilities, the war in Ukraine is the first fully-fledged hybrid war. Approximately seven months into the war, the following preliminary observations can be made.

The war in Ukraine shows the importance of mastering **multi-domain operations and the implications of not being able to do this**. The ubiquitous presence of mobile phone cameras amongst the occupied populations and their ability to disseminate targeting information via cellular networks provides additional intelligence to the Ukrainian defenders.

Satellites play an important role in intelligence gathering in the war. Ukraine, which does not have satellites of its own, benefits from intelligence derived from satellite imaging provided by Western countries and private companies.

As Russia struggles to achieve air control, let alone air superiority, it has used **hypersonic missiles** against selected Ukrainian targets.

Both Ukraine and Russia are using **drones** in the conflict: they are employed by both sides for reconnaissance and close air support. Ukraine is using the Bayraktar TB-2 and commercial off-the-shelf drones effectively against advancing Russian forces. Civilian drones are now being used more extensively than ever before in a war, mostly for reconnaissance but also to transport smaller weapons such as Molotov cocktails or grenades. **Electronic warfare capabilities** and air defence systems have played an important role in limiting Russia’s ability to use drones.

Cyberspace: Cyber-attacks are a central part of warfare in the Ukraine war. Russia launched multiple cyber-attacks against Ukraine before and during the war, including advanced attacks on government websites and infrastructure such as rail systems. The damage has thus far been limited, as Ukraine strengthened its cyber defences significantly before the war with Western support, particularly from the United States. During the war, Ukraine has also received support from private companies, which have shielded networks and critical infrastructure. Ukraine established an “IT army” comprising of “hundreds of thousands” of IT professionals from all over the world to fight Russian cyber-attacks and to counter the Kremlin’s disinformation campaigns. Fears that Russia would release severe cyber-attacks against Ukraine and the West have thus far not materialised. It is unclear if Russia is holding its best cyber weapons in reserve or whether Russian capabilities have been vastly overestimated. Ukraine, too, is using cyber tools against Russia. Primary targets are railways and the electricity grid in order to prevent Russia from getting weapons and supplies to the front in Ukraine, as well as government and financial institution websites. Ukraine is also using cyberspace to flag and contest Russian propaganda.

Ukraine also dominates in the **information war**. The Ukrainian leadership’s communication strategy has been crucial in upholding morale among Ukrainians and garnering international support. **Open Source Intelligence** (OSINT) is playing a key role in the war in Ukraine and has allowed the public to follow the events almost in real time. Publicly available satellite images, social media videos and other data reveal a lot about the course of the war and expose Putin’s propaganda of lies. Though the war is being fought largely with conventional weapons, it is documented with highly modern methods.

B. TECHNOLOGICAL PROGRESS AND IMPLICATIONS FOR MILITARY CAPABILITIES: EMERGING AND DISRUPTIVE TECHNOLOGIES

14. Emerging and Disruptive Technologies (EDTs) are expected to play a crucial role in developing NATO's military capabilities. Each of the EDTs is ingenious, but combined they create significant military disruption, which will allow NATO to maintain the technological edge necessary for its operational and organisational effectiveness (STO, 2020; Wells, 2022). Moreover, military capabilities will increasingly depend on intelligent, interconnected, distributed and digital networks (STO, 2020).

15. The NATO Science and Technology Organization (STO) defined eight "major strategic disruptors" relevant to NATO's capabilities between 2020 and 2040: 1) data; 2) artificial intelligence; 3) autonomy; 4) quantum technology; 5) space technologies; 6) hypersonics; 7) biotechnology and human enhancement (BHE), and; 8) novel materials and manufacturing (NMM).

16. Data, AI, Autonomy, Space and Hypersonics already have disruptive effects on military capabilities, which are expected to increase significantly over the next 5–10 years. With regard to quantum technologies, biotechnology and novel materials, the STO assess new developments in those areas as "emergent", thus requiring another 10–20 years in order to have a significant impact on military capabilities (STO, 2020).

17. **Data** which presents substantial volume, velocity, variety, veracity and visualisation[2] challenges is defined as "Big Data" (BD). Driven by digitalisation, a proliferation of new sensors, new communication modes, the Internet of Things (IoT) and virtualisation of socio-cognitive spaces (e.g. social media), it has become increasingly challenging to make sense of information, i.e. data deluge. The increasing amount of data thus requires analysis to understand, describe and predict events. Techniques making sense of and visualising large volumes of information are called Advanced Data Analytics (STO, 2020).

18. **Big Data Advanced Analytics** (BDAA) combines BD with Advanced (data) Analytics: the latter describes advanced analytical methods for making sense of and visualising large volumes of information. BDAA has the potential to give NATO a decision-making and knowledge advantage, based on the innovative gathering, processing, exploitation, distribution and synthesis of vast and diverse data sources and information products. Areas most likely to be affected by BDAA development are: information; surveillance; reconnaissance (ISR); situational awareness; training and readiness; enterprise management; logistics; support to operations; S&T; and information management (STO, 2020).

19. **Artificial Intelligence** (AI) has been identified as the biggest technological challenge to NATO and refers to a machine's ability to autonomously perform tasks that would normally require human intelligence such as planning, understanding language, recognising objects and sounds, learning and problem solving. Data explosion and information deluge will make the use of AI a necessity for BDAA in order to turn data into actionable knowledge (STO, 2020).

20. The impact of AI on allied military capabilities will mainly occur through the use of embedded AI in other associated technologies such as: virtual/augmented reality; quantum computing; autonomy, modelling & simulation; space; materials research; manufacturing & logistics; and BDAA.

[2] Visualisation of big data the presentation of these data of any type in a graphical format to facilitate understanding of these data and allow for correct, contextual interpretation.

Progress in AI will also create new vulnerabilities and might result in a possible AI arms race (Simonite, 2017).

21. C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) will benefit from an increased use of virtual assistance, AI-enabled decision support to war-games, enhanced indications and warnings, as well as better information and knowledge management tools. AI will further the evolution and use of unmanned vehicles (UxV)[3] and affect the general use of weapons and their impact (e.g. improved trajectory planning, collision avoidance, swarming, weapon selection, battle-damage assessment and effects coordination). In cyberspace and info-space, networks and information systems will be configured, maintained and protected by AI-enabled autonomous agents. AI will also enhance training due to a real-time adaption to human behaviour and the generation of customised training environments or scenarios (STO, 2020).

22. According to the STO report (2020), **autonomy** is defined as “the ability of a system to respond to uncertain situations by independently composing and selecting among different courses of action in order to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation” (STO, 2020). Because AI-empowered machines will increasingly be involved in the decision-making processes, autonomy and human-machine interaction are a matter of degree (Klare, 2019). Whether or not nations will develop fully autonomous systems, semi-autonomous systems are likely to have an impact on operations in the short- and medium-term (STO, 2020).

23. Robotics and Autonomous Systems (RAS) are becoming key enablers in warfare. Progress in autonomy is likely to impact on the future force structure, as unmanned air, sea, or ground vehicles (UxV) and autonomous software agents increase the importance of human-machine interaction. Counter-UxV capabilities will enable new counter-measure possibilities. Unmanned aerial vehicles (UAVs) can conduct ISR and targeting operations against front lines, supply lines and logistics bases (Shashank, 2022). In fact, even the smallest commercial drones can be weaponised and cause devastating harm. Low-tech drones, which can be used as flying IEDs, will be challenging to defend against by regular armed forces. Swarming technologies will enable new sensing and improve the protection of critical assets. The increasing use of dispersed and low-observable vehicles like micro-UAVs in evolving operational areas such as space and urban environments will substantially improve ISR and Situational Awareness (SA). In the area of information warfare, autonomous software agents will increasingly conduct cyber missions (STO, 2020).

24. The world’s economies, militaries and societies increasingly rely on **space**-based systems and technologies, such as satellites used for communication, earth observation or navigation. In fact, the number of satellites is expected to quintuple by 2030, with 1,100 expected to be launched per year in 2025 alone (almost four times the number launched in 2018) (Ryan-Mosley, 2019). NATO’s near-peer competitors invest heavily in the development of their space capacities and are also working on counter-space capabilities (Brunner, 2021).

25. NATO has identified five core space capabilities: position, navigation, time (PNT) & velocity; integrated tactical warning and threat assessment; environmental monitoring; communications; and ISR, which are necessary for the Alliance to successfully undertake military operations. Small satellites (smallsats)[4] are exemplary in space-technologies relevant for military capabilities. They operate primarily in low-Earth (LEO) and medium-Earth (MEO) orbits and perform military missions that used to be conducted by large spacecraft. In the context of NATO, smallsats could

[3] Unmanned aerial vehicles (UAV, UCAV if combat capable), unmanned underwater (UUV) and unmanned surface vehicles (USV) – and unmanned ground vehicles (UGV).

[4] Smallsats are spacecraft which are less than 500 kg in mass.

support NATO's strategic information dominance, ensure reliable, secure communication and enhance situational awareness (STO, 2020).

26. Advanced **hypersonic weapons** operate within the atmosphere at speeds higher than Mach 5 (6,125 kph) (JAPCC, 2017). They are ultra-fast and manoeuvrable weapon systems, which can be used for fast, long-range strikes at high-value targets. Due to their speed and manoeuvrability, hypersonic systems introduce an increased degree of unpredictability and pose substantial countermeasure and interception challenges (Brimelow, 2018; Davenport, 2018). Several nations, including China and Russia, have already reported the successful development and testing of hypersonic weapons (Reuters, 2021). Therefore, there is a critical need to develop countermeasures, which currently include interceptors, electronic countermeasures and directed energy systems (DES).

27. Hypersonic missile technologies may also develop beyond delivering warheads and encompass hypersonic intelligence and reconnaissance aircraft by the 2030s. Hypersonic UAVs could be more flexible for long-range ISR than reconnaissance satellites and also include a possible option for weapon delivery (Swartz, 2016).

28. Advances in **quantum technology** will support substantial technological progress in the following: cryptography; computation; precision navigation and timing (PNT); sensing and imaging; communications; and materials. Yet, the practical application of the new quantum effects still requires profound research (STO, 2020).

29. Quantum technologies may enable NATO military capabilities across the four main streams of activity relevant for security and defence. In the field of **communication and cryptography**, combined with **unbreakable** cryptography, cryptographic technologies such as blockchain will pose substantial challenges to the current C4ISR system. Breakthroughs in **computing** will allow for very sophisticated techniques to code encryption and decryption. **PNT** will substantially improve through new sensitive precision instruments, which will facilitate military operations in particularly challenging environments (e.g. long-duration submerged under-ice autonomous operations). Quantum **sensor** technologies promise to be more resistant to jamming and will feed into the development of counter-stealth and covert radars, or of magnetic, acoustic and gravity sensors with greatly increased ASW capabilities (STO, 2020).

30. Advances in materials, information systems and human sciences push the boundaries of physiological, cognitive and social human performance. **Biotechnology** refers to the use of cellular and biomolecular processes aimed at the development of new technologies. **Human enhancement technologies** are bio-medical inventions which improve, modify and/or add to the traits or abilities a person is born with (Sienna, 2022).

31. Wearable biomedical systems, as well as virtual and mixed reality, stand out as exemplars for BHET's (Biotechnology & Human Enhancement Technologies) impact on operation planning and conduct. Bio-markers and bio-sensors will allow for substantially improved medical countermeasures and care. Optimised performance of individuals and groups (in cognitive, physical or resilience domains), along with personalised and virtualised training possibilities, will enhance overall military capabilities (STO, 2020).

32. Advancements in nanotechnology and synthetic biology drive the manufacturing of artificial **novel materials'** unique characteristics, such as graphene[5]. **Additive manufacturing**, or 3D printing, uses computer models and a range of metals, polymers and resins to build three-dimensional solid objects of nearly infinite shapes (STO, 2020). These novel materials are projected to improve robustness and operational life as well as reducing weight/size of equipment and leading to novel devices and uses, such as biological and chemical warfare detectors. Additive manufacturing is expected to improve product development as it allows for rapid prototyping. It will also enable on-demand and on-site production and repair of deployed military equipment (STO, 2020).

III- TECHNOLOGICAL ASPECTS OF FUTURE WARFARE

33. **EDTs will make military capabilities increasingly intelligent, interconnected, distributed and digital in nature**. According to the NATO Chief Scientist, Dr Bryan Wells, future military capabilities will increasingly depend on:

– ***Intelligent*** *technologies* which will exploit AI and new analytic capabilities;
– ***Interconnected*** *technologies* which will exploit virtual and physical domains;
– ***Distributed*** *technologies* which will employ decentralised and large-scale sensing, storage, and computation*;* and
– ***Digital*** *technologies* which will blend human, physical, and information domains (Wells, 2022).

34. **As a result, we will see greater Intelligent Autonomous Action, the increased importance of Cognitive Dominance, Expanded Warfare Domains and a greater emphasis on Precision Warfare:**

➢ *Intelligent Autonomous Action*: Intelligent and autonomous systems are supplanting and exceeding the capabilities of human forces; they will be engaged in significantly more sophisticated decision-making and self-directed activity. This will result in competition between battle networks, with each seeking a combination of effects that will lead to a decisive victory.

➢ *Cognitive Dominance*: Quantum technologies will increase C4ISR data collection, processing and exploitation capabilities through significantly increased sensor capabilities, secure communications and computing, particularly in Space. This increased reliance on seamless and ubiquitous connectivity will increase the operational importance of targeting such networks (military or civilian) through disinformation, cyber- or physical attacks. Such attacks may be implemented long before the conflict is initiated.

➢ *Expanded Domains*: The need to think, plan and operate in a widely dispersed, interconnected and multi-domain manner will become even more critical to mission success. The increased exploitation of new domains will inevitably lead to the search for domain superiority. In concert with Big Data and Quantum, AI will expand our ability to exploit the biological domain, contributing to new personalised drugs and living sensors. These technologies will enable

[5] Graphene is a new carbon-based substance that has a unique set of mechanical, physical, chemical and electrical characteristics that no other material has. It is chemically stable, non-toxic, light and simple to produce from readily available raw components.

more effective human-enhancement technologies across the cognitive, social, and physiological domains.

- *Precision Warfare*: Increased digitisation across C4ISR capabilities is dramatically increasing the development of precision strike capabilities. Swarming and the use of lower-cost precision weaponry will continue to put large high-value capabilities at risk. Directed energy precision weapons will become more widespread and effective as power and energy storage issues are addressed.

IV- PREPARING NATO FOR FUTURE WARFARE - TECHNOLOGICAL ASPECTS

A. THE NATO WARFARE CAPSTONE CONCEPT

35. **Allied Command Transformation** (ACT) plays an important role in conceptualising future warfare and in defining the future military context. ACT identifies future challenges to and opportunities for the Alliance in order to innovate and maintain a warfighting edge. ACT puts a strong emphasis on ensuring maximum interoperability of NATO forces, thereby also making an important contribution to NATO defence planning and capability development. ACT also applies innovation to leverage ideas, procedures and technologies to the benefit of NATO's warfare development.

36. To help NATO to prepare and adapt to this evolving security environment, Allied Command Transformation (ACT) has developed the NATO Warfighting Capstone Concept (NWCC). The NWCC was affirmed by several NATO bodies, including Allied Heads of State and Government at the 2021 Brussels Summit. NWCC is a follow-up and a part of the NATO 2030 project: it represents an important milestone for the adaptation of the Alliance. The NWCC gives guidance for developing future military capabilities, focusing on five Warfare Development Imperatives (WDIs) (Ellison, 2021). These are, according to Ellison:

– Cognitive superiority: knowing ourselves and potential adversaries better;
– Layered resilience: strengthening cross-instrument connections and actions;
– Influence and power projection: challenging other actors' attempts to shape the environment;
– Cross-domain command: creatively acting across domains and connecting beyond the military instrument;
– Integrated multi-domain defence: protecting the joint force from multi-domain threats.

37. The ACT also includes an **Innovation Hub,** which supports projects relevant to NATO. It facilitates a community of experts and innovators collaborating to address NATO challenges and "design solutions" (IH, 2022). ACT's most relevant contribution is based on its extensive network of civilian, military and government personnel as well as academics and scientists (NATO, 2021f). While the states support the network through assigning personnel, the network contributes through providing knowledge and "soft- and hard assets" (Størdal, 2022). On one hand, states get exposed to a diversity of perspectives and approaches (soft assets). On the other hand, they gain access to testing facilities and environments (hard assets), as well as project results. Sharing costs and pooling knowledge has allowed NATO member states to have some of the most modern armed forces and to be world leading in niche areas (Størdal, 2022).

B. MAINTAINING AND ADVANCING NATO'S TECHNOLOGICAL EDGE: THE COLLABORATIVE PROGRAMME OF WORK

38. Recognising the importance of EDTs for future capability development, Allies agreed in 2019 on an **Emerging and Disruptive Technology Implementation Roadmap.** The roadmap structures NATO's work across key technology areas and enables Allies to consider their implications for deterrence, defence and capability development. In 2021, NATO endorsed a **Coherent Implementation Strategy on EDTs**. The strategy focusses on strengthening the development of dual-use technologies and on creating a forum for Allies to exchange best practices (NATO, 2021).

39. The **Science and Technology Organization** (STO) is the main body that promotes and leverages the S&T investments of Allied member states and NATO to conduct and advance scientific research, technology development and innovation. The Collaborative Programme of Work (CPoW), which features an extensive network of scientists from NATO member and partner nations and is supported by the Collaboration Support Office (CSO), represents the STO's main contribution to developing modern interoperable capabilities. At the beginning of 2022, the total number of ongoing activities in the STO CPoW was 283. The work of the CPoW is taking place in six technical panels, which cover a wide range of research activities and a group specialising in modelling and simulation (STO, 2022c). S&T work in the STO is also undertaken by the STO Centre for Maritime Research and Experimentation (CMRE).

40. The **Applied Vehicle Technology** (AVT) panel "strives to improve the performance, reliability, affordability, and safety of vehicles through advancement of appropriate technologies" (STO, 2022). Focusing on developing technologies for vehicles operating in all domains the AVT community exploits joint expertise in the fields of: (1) Mechanical Systems, Structures and Materials; (2) Propulsion and Power Systems; and (3) Performance, Stability and Control, Fluid Physics.

41. The **Human Factors and Medicine** (HFM) panel focuses on efforts to optimise health, human protection, well-being and performance of soldiers in different operational environments. This involves understanding and ensuring physical, physiological, psychological and cognitive compatibility among military personnel, technological systems, missions and environments. For example, unmanned surveillance technologies are soon unlikely to replace the need for human military presence in extreme environments. HFM explore and test new concepts to prevent and treat "freezing" (traditionally known as "frostbite") and "non-freezing" (body cooling or "hypothermia") injuries.

42. The **Information Systems Technology** (IST) panel works on the development of techniques and technologies to improve C3I systems, with a special focus on AI, Interoperability and Cyber Security and to provide timely, affordable, dependable, secure and relevant information to war fighters, planners and strategists. The IST Programme of Work is organised under three Focus Groups: Information and Knowledge Management, Architecture and Intelligence Information Systems and Communications & Networks.

43. The **System Analysis and Studies** (SAS) panel conducts studies and analysis for better decisions in strategy, capability development and operations within NATO as well as in NATO member and partner nations. The SAS panel's work centres on the exploitation of new technologies, new forms of organisation and new concepts of operation.

44. The **Sensors and Electronics Technology** (SET) panel promotes co-operative research, the exchange of information and the advancement of science and technology among the NATO Nations in the field of sensors and electronics for defence and security. The SET Panel addresses the development and enhancement of both passive and active sensors, as well as electronic technology

capabilities, multi-sensor integration and fusion as they pertain to Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), Remote Sensing, Electronic Warfare (EW), Communications, and Navigation. The SET Panel is organised into three Focus Groups: RadioFrequency Technology (RFT); Optical Technology (OT); and Multi-Sensors & Electronics (MSE).

45. The **Systems, Concepts and Integration** (SCI) panel fosters the development of knowledge regarding "advanced system concepts, integration, engineering techniques and technologies across the spectrum of platforms and operating environments to assure cost-effective mission area capabilities". For instance, Unmanned Air Systems (UASs) are already being widely used in many conflict areas in the world. Autonomy and autonomous systems will be the key player in the upcoming decades. The SCI panel also helps to share and disseminate the experience and the lessons learned from flight testing of UAVs among different NATO nations.

46. Finally, the **NATO Modelling and Simulation Group** (NMSG) promotes cooperation among Alliance bodies, NATO, and partner nations to maximize the effective utilisation of modelling and simulation (M&S). This includes (M&S) standardisation, education and associated science and technology.

47. The work of the **Centre for Maritime Research and Experimentation** (CMRE), a world-class scientific research and experimentation facility located in La Spezia (Italy), focuses on scientific research and technology development in the maritime domain. CMRE is a 100% customer-funded defence research facility that delivers innovative and field-tested defence-related S&T solutions; NATO ACT is the largest customer, followed by individual nations and other organisations, such as the European Commission.

48. More generally, the STO primarily cooperates with larger companies and focuses on technologies on 1–4 of the Technology Readiness Level[6]. The concentration on lower TRLs is the indispensable first step on the path to the development and delivery of future military capabilities. It necessitates constant investments over a longer period of time before it produces mature technologies that can be fielded. In addition to in-depth research, the STO organises events such as symposia, workshops and experts' meetings, as well as educational activities such as lecture series and technical courses (STO, 2022b).

49. Moreover, as the STO plays a crucial role in the coordination of Allied efforts in the S&T realm. It also helps to increase mutual awareness, avoid duplication and promote synergies. It is important to note that cooperation in S&T can be considered a strong trust-building measure among states. Thus, the STO also works closely with enhanced opportunity partners (Australia and Japan) and invitees (Finland and Sweden) and receives strong engagement from South Korea and Singapore (Wells, 2022; Størdal, 2022).

[6] Originally developed by NASA, Technology Readiness Levels (TRL) are a type of measurement system used to assess the maturity level of a particular technology. A technology in TRL 1 refers to the start of scientific research where basic principles are observed and reported. TLR 9 refers to the actual system proven through successful mission operations. Emerging technologies are usually in the range of TRL 1 through 5.

C. Recent Initiatives

50. Recognising the need to maintain its technological edge, the Alliance has begun to put innovation higher on its agenda. In 2021, 17 Allies[7] launched a multinational **Innovation Fund** worth EUR 1 billion enabling NATO to retain its technological edge. It will not only enable investments in dual-use technologies but also facilitate cooperation with deep-tech innovators (NATO, 2021g). Additionally, NATO adapted the structure of its International Staff by creating new units dedicated to innovation and to data policy (Rühle & Roberts, 2021).

51. In a joint effort between the private sector, NGOs and academia, Allies launched the civil-military **Defence Innovation Accelerator of the North Atlantic** (DIANA). DIANA will become operational in 2023. It will provide the necessary knowledge for the development of technologies to improve[8] and support[9] EDTs (FINABEL, 2021). DIANA is being developed as a means for Allies, if they choose, to pick the science and mature it to testable military capabilities. DIANA will primarily work with start-ups and smaller companies and support the process of technologies along the development path (technologies at TRL 4 and above). DIANA and the NATO Innovation Fund will concentrate on the development of technologies with higher TRLs (compared to that covered by the STO); hence their work will be complementary to the STO’s portfolio. At the 2022 Madrid NATO Summit, the Allies approved the charter for DIANA and disclosed its initial footprint of Test Centres and Accelerator sites. Nine accelerator sites and more than 63 test centres across Europe and North America will foster the creation and adaptation of dual-use emerging technologies to defence threats and critical security (NATO, 2022c).

V- CONCLUSIONS

52. While NATO is the most successful Alliance in the world, it needs to adapt to a continually changing international environment. Geostrategic competition over technological primacy is growing as the pace of technology development accelerates while technology supply chains become increasingly complex. Countries like China and others are making great strides towards developing a world-class S&T community which risks disrupting the global strategic balance. Maintaining its technological edge is crucial for the Alliance to keep a credible defence and deterrence posture. At the 2022 Madrid Summit, Heads of State and Government agreed to enhance the Alliance’s technological edge to maintain NATO’s interoperability and military edge.

53. Having recognised the importance of innovation for the development of future capabilities, both NATO and Allied member states have established organisations focusing on the development and fielding of emerging technology. To leverage the investment into different areas of research and avoid duplication amongst themselves, Allies should examine if there is a need for greater cooperation, ideally via the existing NATO network and the STO. This is important to maintain and further increase interoperability, particularly as the military capabilities and technological prowess of 30 member states differ greatly.

[7] Belgium, the Czech Republic, Estonia, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia and the United Kingdom.

[8] Artificial intelligence (AI), quantum-enable technologies and big-data processing.

[9] Data and computing, autonomy, biotechnology and human enhancements, hypersonic technologies, and space.

54. Strengthening the Alliance’s deterrence and defence posture will increase the demand for cutting-edge military capabilities and their accelerated delivery. While the investment in emerging and disruptive technologies must grow, the pace of adoption of novel technologies must increase at the same time.

55. In addition, 21 nations are members of both NATO and the European Union. Considering that resources are limited, NATO, the European Union and their member states should evaluate how NATO can improve cooperation in the technology field with the EU, but also with the European Defence Agency and the European Defence Fund. Member states cannot afford to continue duplicating their S&T efforts the way they do it now.

56. There is a need to link technological innovation and the acquisition processes more effectively. In this context, NATO should examine whether there are opportunities to link the NATO Defence Planning Process with the research produced in the STO and with DIANA. A decision for a weapon system or platform can have a profound longer-term effect on capabilities, force structure, interoperability and defence budgets, among other issues. Allies need to leverage the development of future capabilities with the need to have capable forces with high readiness.

57. There is also a need to strengthen NATO as the transatlantic forum between Allies’ and likeminded nations’ innovation ecosystems, including by strengthening cooperation with the private sector, academia and other relevant actors. Moreover, stakeholders in Allied and partner countries need to develop a common understanding of research security as a critical underpinning for maintaining military advantage into the future. They need to protect their knowledge base and innovation ecosystems from strategic competitors and potential adversaries exploiting the Allies’ and partners’ research results and undermining the Alliance’s world-class defence research collaboration.

58. The further development of research produced by the STO and DIANA into mature products and their subsequent deployment is instrumental for generating future military capabilities. As the STO generally concentrates on promoting technology up to TRL 4 (with the exception of the CMRE which can also focus on higher TRL levels) it could pass the completed scientific research or product to DIANA, which could mature it to potential military equipment. As DIANA will become operational in 2023, NATO should evaluate if the way research and development is conducted in the NATO network is efficient or if established structures and procedures could be streamlined.

59. Moreover, NATO should evaluate if and how cooperation between the STO and other NATO bodies involved in capability development could be improved to accelerate the development of future military capabilities. NATO should also evaluate if and how the STO’s coordination role for the S&T planning domain in the NATO Defence Planning Process (NDPP) can be strengthened. In addition, as the pace of technological progress is fast, NATO should review the structure of the CPoW, which is in place since the late 1990s.

60. NATO Allies should explore preliminary rules of the road, standards and norms governing the global deployment of EDTs in military systems. This applies particularly to the areas of AI, automation/robotics as well as biotechnology as technological advances will create both benefits and risks. “A race in autonomy poses a particular danger because the consequences of investing machines with increased intelligence and decision-making authority are largely unknown and could prove catastrophic” (Klare, 2019). This is also the case for biotechnology where technological progress could allow for the production of dangerous pathogens. NATO member and partner states, and the international community more generally, therefore, need to address the legal, moral and ethical questions that arise with the progress in these technologies.

61. Human-machine interactions are becoming ever more important, among others because the speed with which machines can analyse data is increasing dramatically. Moreover, scientific research will generate a better understanding of the human mind, which will allow breakthroughs in cognitive warfare as a result. However, this development also requires bridging the technical and human domains; the challenges are organisational and strategic and involve choosing the right people to implement and execute them (Regnault, 2019).

62. NATO Allies should increase funding for Allied EDT research and development for the seven EDTs identified in NATO's "Coherent Implementation Strategy on Emerging and Disruptive Technologies." The NATO Innovation Fund, which is designed to invest in early-stage start-ups, is a step in the right direction. However, the size of the fund is relatively limited. The Allies should also agree on spending a certain percentage of funds on S&T. The revision of the Defence Investment Pledge planned for 2024 should incorporate a concrete target for defence R&D expenditure of Allied nations.

63. The commercial sector is now driving technology advances: private corporations are developing the hard- and software needed for advanced military capabilities. However, the adaptation of commercial applications for military purposes requires the consideration of specific constraints to ensure that these applications operate securely and reliably in contested operational environments and academia / start-ups may still be reluctant to get involved with NATO.

64. Building an efficient innovation pipeline is a longer-term project, which, in addition to sufficient and sustained funding, structures and secure processes, also requires personnel development. NATO member states should encourage the young generation to become more engaged in science, technology, engineering and mathematics (STEM).

65. It is more important than ever that NATO Nations and partners use technology to get ahead of adversaries by developing new concepts of warfare and strengthening interoperability at the same time. President Putin's war against Ukraine has been a wake-up call and Allied nations are increasing their investments in defence. However, NATO Allies need to spend the extra money available for defence in the smartest way possible.

BIBLIOGRAPHY

Bodnar, Jozsef and Collins, Sue, "NATO Joint Military Operations in an Urban Environment //A Capstone Concept", NATO Joint Warfare Centre: The Three Swords Magazine, 2019, https://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/NATOUrbanization_2035.pdf

Braw, Elisabeth, "Modern warfare is catching companies in its crossfire", *Financial Times*, 14 February 2022, https://www.ft.com/content/f6a726e2-0d50-4214-a32b-630dd747bf6e?segmentId=114a04fe-353d-37db-f705-204c9a0a157b

Brimelow, Ben, "China and Russia are 'aggressively pursuing' hypersonic weapons – and the US doesn't have any defenses", Business Insider, 20 March 2018, https://www.businessinsider.com/us-china-russia-hypersonicweapons-2018-3?r=US&IR=T

Brown, Larisa, "Enemy hackers target Nato with constant cyberattacks", *The Times*, 28 May 2021, https://www.thetimes.co.uk/article/enemy-hackers-target-nato-with-constant-cyberattacks-dj263x2lh

Brunner, Karl-Heinz, "Space and Security – NATO's Role", NATO Parliamentary Assembly, 1 December 2021, https://www.nato-pa.int/document/025-stc-21-e-space-and-security-natos-role-report-brunner

Coats, Daniel R., "Statement for the record worldwide threat assessment of the US intelligence community", DNI, 6 March 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf

Coats, Daniel R., "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community", DNI, 29 January 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Cohen, Raphael S. et al, "The Future of Warfare in 2030. The Changing Global Environment and Its Implications for the U.S. Air Force. Project Overview and Conclusions", RAND Corporation, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2849z1/RAND_RR2849z1.pdf

Crosbie, Thomas, "Joint Doctrine / Getting the Joint Functions Right", National Defense University Press, 2019, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_108-112_Crosbie.pdf?ver=2019-07-25-162025-397

Darbyshire, Eoghan and Weir, Doug, "How does war contribute to climate change?", Conflict and Environment Observatory, 14 June 2021, https://ceobs.org/how-does-war-contribute-to-climate-change/

Davenport, Christian, "Why the Pentagon fears the U.S. is losing the hypersonic arms race with Russia and China", *The Washington Post*, 8 June 2018, https://www.washingtonpost.com/business/economy/why-the-pentagon-fears-the-us-is-losing-the-hypersonic-arms-race-with-russia-and-china/2018/06/08/7c2c3b4c-57a7-11e8-b656-a5f8c2a9295d_story.html

Ellison, Davis, "Mastering the Fundamentals – Developing the Alliance for the future Battlefield", NATO Joint Warfare Centre: The Three Swords Magazine, 2021, https://www.jwc.nato.int/application/files/9116/3280/7847/issue37_03.pdf

FINABEL, "Defence Innovation Accelerator for the North Atlantic (DIANA)", FINABEL, 17 August 2012, https://finabel.org/defence-innovation-accelerator-for-the-north-atlantic-diana/

GMACCC and Christopher-King, Wendell, "Climate Change: Implication for Defence", GMACC, June 2014, https://www.gmaccc.org/gmaccc-publications/climate-change-implications-for-defence

GAO (US Government Accountability Office), “Weapon systems cybersecurity. Guidance Would Help DOD Programs Better Communicate Requirements to Contractors”, US Government Accountability Office, 4 March 2021, https://www.gao.gov/assets/gao-21-179.pdf

Goddard, William, “Cyber Security Statistics 2020”, IT Chronicles, 27 May 2021, https://itchronicles.com/information-security/cyber-security-statistics-2020/

ICRC, “Urban Services during Protracted Armed Conflict. A Call for a Better Approach to Assisting Affected People”, ICRC, https://www.icrc.org/en/publication/4249-urban-services-during-protracted-armed-conflict

IH, “Partnering with the Innovation Hub - ACT”, https://www.innovationhub-act.org/partnering-innovation-hub

JAPCC, “Hypersonic Vehicles. Game Changers for Future Warfare?, Spring/Summer 2017, https://www.japcc.org/articles/hypersonic-vehicles/

Klare, Michael T., “Autonomous Weapons Systems and the Laws of War”, Arms Control Association, March 2019, https://www.armscontrol.org/act/2019-03/features/autonomous-weapons-systems-laws-war

Labott, Elise, “’We are the First in the World to Introduce this New Warfare’: Ukraine’s Digital Battle against Russia”, Politico, 8 March 2022, https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880

Lavikainen, Jyri, “Strengthening Russia’s Nuclear Forces in the Arctic: The Case of the Kinzhal Missile”, CSIS, 14 September 2021, https://www.csis.org/analysis/strengthening-russias-nuclear-forces-arctic-case-kinzhal-missile

MacDonald, Geri, “NATO’s first operational UAS flying unit is providing increased security and persistent regional deterrence for the Alliance”, Northrop Grumman Corporation, 18 February 2021, https://news.northropgrumman.com/news/releases/nato-alliance-ground-surveillance-force-achieves-initial-operating-capability

Michel-Kleisbauer, Philippe, *“*Urban Warfare*”,* NATO PA: STC, 20 November 2020, https://www.nato-pa.int/download-file?filename=/sites/default/files/2020-12/040%20STCTTTS%2020%20E%20rev%202%20fin%20-%20REPORT%20-%20URBAN%20WARFARE_0.pdf

Migdon, Brooke, “Experts say the first wars over climate are already starting to happen”, The Hill, 3 November 2021, https://thehill.com/changing-america/sustainability/climate-change/579902-experts-say-the-first-wars-over-climate-are

NATO 2019. “NATO: Ready for the Future, Adapting the Alliance (2018–2019)”, NATO, 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf

NATO 2021, “Emerging and disruptive technologies”, NATO, 7 April 2022, https://www.nato.int/cps/en/natohq/topics_184303.htm

NATO 2021a, “NATO Defence Planning Process”, NATO, 31 March 2022, https://www.nato.int/cps/en/natohq/topics_49202.htm

NATO 2021b, “Brussels Summit Communiqué”, PR NATO, 8 April 2022, https://www.nato.int/cps/en/natohq/news_185000.htm

NATO 2021c, “NATO and Luxembourg boost Alliance Space Situational Awareness”. NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/news_185365.htm

NATO 2021d, “Summary of the NATO Artificial Intelligence Strategy”, NATO, 22 October 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm

NATO 2021e, “Environment, climate change and security”, NATO, 3 December 2021, https://www.nato.int/cps/en/natohq/topics_91048.htm

NATO 2021f, “NATO Science and Technology Organization” NATO, 13 April 2022, https://www.nato.int/cps/en/natohq/topics_88745.htm

NATO 2021g, “NATO Climate Change and Security Action Plan”, NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185174.htm

NATO 2022a, “NATO’s overarching Space Policy”, NATO, 17 January 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm

NATO 2022b, “NATO launches Innovation Fund”, NATO, 30 June 2022, https://www.nato.int/cps/en/natohq/news_197494.htm

NATO 2022c, “Emerging and disruptive technologies”, NATO, 17 July 2022, https://www.nato.int/cps/en/natohq/topics_184303.htm?

NATO 2022d, NATO Strategic Concept, NATO, 29 June 2022, https://www.nato.int/strategic-concept/

NATO ACT, “Activities”, https://www.act.nato.int/activities

NATO ACT 2017, “Strategic Foresight Analysis, 2017 Report”, Norfolk Virginia USA: HQ SACT Strategic Plans and Policy, https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf

NATO ACT 2018, “Framework for Future Alliance Operations, 2018 Report”, Norfolk Virginia USA: HQ SACT Strategic Plans and Policy, https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf

NATO ACT 2020, “2020 Factsheet. Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR)”, https://www.act.nato.int/application/files/5515/8257/4725/2020_mcdc-muaar.pdf

NATO ACT 2021, “NWCC NATO Warfighting Capstone Concept” NATO ACT, https://www.act.nato.int/nwcc

NATO NSO, “NATO Standard. AJP-3. Allied Joint Doctrine for the Conduct of Operations. Edition C Version 1”, NATO Standardization Office, February 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

NATO STO, “Science & Technology Trends 2020-2040. Exploring the S&T Edge”, Brussels: NATO Science & Technology Organization, March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO STO 2022a, “Organization”, https://www.sto.nato.int/Pages/organization.aspx

NATO STO 2022b, “Technical Activities of the STO”, https://www.sto.nato.int/Pages/activitieslisting.aspx

NATO STO 2022c, “The Collaboration Support Office – CSO”, https://www.sto.nato.int/Pages/collaboration-support-office.aspx

Reuters, “Russia test-fires new hypersonic Tsirkon missiles from frigate, submarine”, Reuters, 31 December 2021, https://www.reuters.com/business/aerospace-defense/russia-test-fires-new-hypersonic-tsirkon-missiles-frigate-submarine-2021-12-31/

Regnault, Heather “Emerging Technologies and the Future of Warfare”, The Cipher Brief, 7 November 2019, https://www.thecipherbrief.com/column_article/emerging-technologies-and-the-future-of-warfare

Rühle, Michael and Roberts Claire, “Enlarging NATO’s toolbox to counter hybrid threats”, NATO Review, 19 March 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

Ryan-Mosley, Tate, Winick, Erin and Kakaes, Konstantin, “The number of satellites orbiting Earth could quintuple in the next decade”, Technology Review, 26 June 2019, https://www.technologyreview.com/s/613746/satellite-constellations-orbiting-earth-quintuple/

Shashank, Joshi, “The technology of seeing and shooting your enemies”, *The Economist*, 29 January 2022, https://www.economist.com/technology-quarterly/2022/01/29/the-technology-of-seeing-and-shooting-your-enemies

Sienna, “What is Human Enhancement?” Sienna/ Uppsala University, https://www.sienna-project.eu/enhancement/facts/

Simonite, Tom, “AI Could Revolutionize War as Much as Nukes”, WIRED, 19 July 2017, https://www.wired.com/story/ai-could-revolutionize-war-as-much-as-nukes/

Sprenger, Sebastian, “NATO’s new fleet of surveillance drones is deemed mission-ready”, Defence News, 15 February 2021, https://www.defensenews.com/global/europe/2021/02/15/natos-new-fleet-of-surveillance-drones-is-deemed-mission-ready/

Størdal, John-Mikal, CSO Interview conducted in Brussels, Belgium, 9 March 2022

Swartz, Philip, “Hypersonic missiles could be operational in 2020s, general says”, Defence News, 26 February 2016, https://www.defensenews.com/air/2016/02/26/hypersonic-missiles-could-be-operational-in-2020s-general-says/

Uchill, Joe, “Disinformation as a service crosses borders with ease”, Axios, 3 October 2019, https://www.axios.com/disinformation-misinformation-service-online-1da509b2-d535-4ab0-bd51-3ae2fc344e31.html

UN, “Report of the UN Economist Network for the UN 75th Anniversary Shaping the Trends of Our Time”, UN, September 2020, https://www.un.org/development/desa/publications/wp-content/uploads/sites/10/2020/09/20-124-UNEN-75Report-1.pdf

Wells, Bryan, NATO Chief Scientist, presentation to STC Committee Officers, Brussels, Belgium, 16 March 2022

Zimmermann, Moritz, Innovation Officer, NATO Innovation Unit, Interview, 14 April 2022