The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO

Jacopo Bellasio
Senior Analyst
Defence, Security and Infrastructure
RAND Europe

Erik Silfversten
Co-Director
Centre for Futures and Foresight Studies
RAND Europe

Abstract: Recent years have seen significant advances in a wide array of new and emerging technologies with disruptive potential, several of which have an inherent cyber dimension. These include, inter alia, artificial intelligence and machine learning, autonomous devices and systems, telecommunications and computing technologies, satellites and space assets, human-machine interfaces and quantum computing. This paper provides an overview of some of the key technology trends for the coming decade and their potential implications for the future cyber threat landscape and NATO. The paper provides an overview of challenges that could emerge from individual technologies, from complex interactions between them, as well as with broader socio-economic trends. It also discusses how technological change and development may occur at such a pace, and have such wide-ranging impact, that NATO and its member states could struggle to achieve its mission and objectives. It concludes by putting forward a set of considerations for preparing for, responding to, and mitigating these challenges.

Keywords: *Cyber security, future threats, emerging threats, disruptive technologies*

1. INTRODUCTION

What cyber threats could emerge over the next decade from new and emerging technologies? How could NATO prepare for and manage them? Recent decades have seen a revolution in Information and Communication Technologies (ICTs) and related technology areas. The development, proliferation, widespread use and embedding of ICTs in contemporary societies have resulted in unprecedented change affecting all aspects of human activity, including military and foreign affairs.

In defence, this has been evident in cyber security and network defence, but has also contributed to the growth of hybrid threats[1] and wider threats in the information environment. In this context, NATO and its member states are facing growing challenges from state and non-state actors in cyberspace, with threats to the Alliance's integrity and military operations and to the day-to-day functioning of its institutions (NATO, 2020a).

In parallel with these developments, we have seen significant advances in a wide array of new and emerging technologies that could have disruptive implications to the nature, scope and potential impact of cyber threats to NATO. The pace of technological change is expected to continue in the next decade and may have profound effects on defence and security matters (Kepe et al., 2018). The rapid pace of change, the complexity and the uncertainty of these developments require an understanding of their implications to ensure NATO's ability to ensure resilience and manoeuvrability in the cyber domain.

This paper discusses a selection of new and emerging technologies with potentially disruptive effects, particularly concerning cyber threats that may stem from their maturation and use over the next decade. It concludes by presenting cross-cutting implications to the future cyber threat landscape before offering thoughts for possible actions to be implemented by NATO and its member states. Given the breadth of technologies considered, this paper is meant to provide an introductory overview of new and emerging technologies, particularly for a non-specialist decision-maker audience. The chapter focuses on implications for the future cyber threat landscape, so it does not discuss effects on defence capabilities or on ways in which threats could be mitigated.

2. NEW AND EMERGING TECHNOLOGIES OF RELEVANCE FOR THE FUTURE CYBER THREAT LANDSCAPE

Deep uncertainty characterises the future geostrategic context and how the technology and cyber threat landscapes will develop. The latter issues

[1] Threats comprising of a mix of coercive and subversive activities and tactics, leveraging both conventional and non-conventional methods below the threshold of war to achieve a range of diplomatic, military, economic, and political objectives.

put cyber security and defence professionals, as well as the institutions and communities they protect, at a structural disadvantage, favouring attackers over defenders. Gaining an improved awareness of how the cyber threat landscape may evolve in the next decade could help decision-makers anticipate threats and coordinate timely and effective responses to future challenges. This paper aims to contribute to such efforts by looking at how technological developments may affect the cyber threat landscape over the next decade.

To identify the most relevant new and emerging technologies that could affect that landscape, the authors reviewed the science and technology (S&T) horizon-scanning database of RAND Europe's Centre for Futures and Foresight Studies (CFFS). The CFFS continuously and systematically captures publicly available reports of the latest S&T developments across a wide range of disciplines and fields. At present, the database comprises over 3,000 technology items relevant to security and defence identified from sources in English, Russian and Mandarin. The horizon-scanning approach underpinning the database combines bibliometric and scientometric approaches with expert engagement activities and assessments.

Overall, the following new and emerging technology clusters were deemed most relevant from a NATO perspective in terms of expected effect on the cyber threat landscape: artificial intelligence and machine learning; autonomous devices and systems; telecommunications and computing technologies; satellites and space assets; human-machine interfaces; and quantum computing. While other technology clusters and clustering approaches could have been selected, the authors selected these technologies based on a combined assessment of their likelihood to achieve significant advances over the next decade, and of their potential impact on the cyber threat landscape should these advances materialise.

A. Artificial Intelligence and Machine Learning

Multiple definitions of artificial intelligence (AI) exist. This paper takes AI to refer to a capability within computer systems to perform tasks that would otherwise require human intelligence to be conducted. AI systems can be classified according to a variety of parameters, including their levels of autonomy and sophistication (McCarthy, 2007; Joshi, 2019; Wong et al., 2020). AI systems can also be underpinned by machine learning (ML), which is the science of creating intelligent computer programs that can automatically improve their performance through experience (i.e., 'learning').

AI and ML have already enabled the development of a wide range of applications to make systems more efficient and scalable and for the delivery of tasks that can exceed the capabilities of humans. From an adversarial perspective, AI/ML could be leveraged for nefarious purposes to automate cyber attacks. While the use of AI/ML for such purposes has not yet been observed in the wild, companies have already launched 'red teaming as service' platforms offering automated attack services which combine a confidence engine with

target temptation analysis to detect system and network vulnerabilities, highlighting assets with the highest perceived adversarial value (Randori, 2019). Data collection and AI/ML advances could also be used in the future to analyse large, complex data sets collected and analysed in real-time from the operational environment with predictive aims or to support decision making at the strategic, operational and tactical levels. In this context, holding AI dominance or a competitive advantage could result in AI/ML acting as a critical force multiplier for military capabilities (Waltzman et al., 2020; Williams, 2020).

Concerns have, however, been raised over the current limitations of security evaluations for AI systems and methods, stemming from the lack of a common language to discuss the vulnerability of such systems and more broadly from oversight in terms of assessing the security of AI incorporated in broader applications and systems (Hartmann & Steup, 2020). The proliferation of AI systems has also given rise to the development of so-called adversarial AI, a set of tactics designed to cause ML models to behave in ways desired by adversaries. Adversarial AI has been highlighted as a significant area of concern, particularly for those AI systems designed with humans 'out-of-the-loop' and in those systems where erratic AI behaviour and readings could degrade human situational awareness (Danks, 2020). Defence applications leveraging AI to support decision making on the battlefield or in the context of broader missions and operations could be subject to similar attacks, with an impact on NATO.

AI/ML have also been used to generate so-called 'deep fakes', synthetic media where individuals' likeness are simulated or replaced with those of others (Cauduro, 2018). Deep fakes may be used by hostile actors for propaganda, offensive or covert purposes. For example, highly realistic deep fakes could be used to support influence operations and broader hybrid tactics. Similarly, AI-powered bots on social media could become increasingly difficult to distinguish from human users, making their harnessing for propaganda and influence operations purposes more effective. Recent advances in AI include software that can deploy deep fakes live, for instance in the context of online video conferencing, or algorithms that can alter audio-visual media to change speakers' speech by editing, adding or deleting content (Cole, 2019; Myers, 2019). Such capabilities could be used to influence the trajectory of public discourse, undermine social cohesion and polarise political debates within and between NATO member countries, or to drive a wedge between NATO and local populations in an area of NATO operations (NATO, 2020b).

B. Autonomous Devices and Systems

Autonomous devices and systems are platforms and devices that can achieve their goals independently and require little or external control and supervision. They combine intelligent software which, thanks to AI-enabled autonomy, conducts or assists with decision-making via hardware devices which interact with the system's surroundings and the physical world to collect data and undertake tasks (Scharre, 2018; Vallor and Bekey, 2017).

Autonomous systems can vary in size, hardware and level of autonomy. The level of autonomy is typically classified according to the expected 'meaningful human control', which is a metric reflecting the extent to which humans are required to intervene in a system's interactions with the real world (Scharre, 2018; Fong, 2019; Leikas et al., 2019).

A wide array of autonomous systems with direct relevance to security and defence have been developed in recent years, including autonomous unmanned vehicles, unmanned weapons systems and smart medical devices. Further advances in this field are expected to stem from developments in swarming technologies[2] and of more sophisticated autonomous systems, including for autonomous weapons. These advances are expected to reduce reliance on humans for decision-making or operational control, thus opening vulnerabilities for the possible disruption and manipulation of autonomous systems.

From a cyber threat perspective, the proliferation of autonomous systems and devices is expected to increase the attack surface available to adversaries and malicious actors (Bogan & Feeney, 2020). For example, autonomous weapons systems that include a tether, enabling the remote control of a system from a supplying country wishing to ensure compliance of the use of its systems with international humanitarian law, could result in the embedding of back doors and kill switches limiting the value of autonomous system assets and potentially making them vulnerable to disruption or manipulation by other third parties (Kajander et al., 2020). Similarly, the use of autonomous vehicles for logistics could be targeted by adversaries leveraging cyber vulnerabilities or adversarial AI to disrupt the logistics and supply chains of a military operation (Danks, 2020; Bogan & Feeney, 2020).

C. Computing, Data Storage, Sensors and Telecommunications Technologies

Computing power and data storage technologies are fundamental enablers of ICT systems. Along with sensors, these technologies allow the capture, manipulation and storage of data. Advances in these fields have led to the development of sophisticated capabilities able to record, store and manipulate expanding datasets at increasing speed. Over the next few years, advances for computing technologies are expected to lead to increasing miniaturisation and greater power, enabling a variety of new solutions such as miniaturised supercomputers, semiconductors and microprocessors like 'smart dust' (Shaikh et al., 2016; Beijing Innovation Centre for Future Chips, 2018). With regard to data storage, in addition to the development of high-density low-energy consumption data storage solutions, it is expected that the future will see a continuation of the growing use and reliance of cloud storage technologies, enabling ubiquitous, on-demand access to data through remote servers (Hess et al., 2019).

These trends and their effects are expected to be further reinforced by advances

[2] The development of advanced collective behaviour mechanisms that enable two or more autonomous systems to operate collectively.

in the fields of sensors. Sensors are used on IT-enabled systems to acquire data to contribute to the performing of different tasks, including decision-making and the tracking and monitoring of a variety of different phenomena. Advances in sensors are expected to result in improved performance and accuracy, further miniaturisation[3] and improved ability to record or generate new types of data. From a defence standpoint, modern platforms and systems have already witnessed the embedding of an increasing number and type of networked sensors which monitor and support their performance. In the coming decade, sensors could also see a growing integration at the level of individual soldiers or systems to improve communications, situational awareness and enable more robust decision-making at different levels through data fusion and analysis (Kepe et al., 2018).

These trends are expected to be further reinforced thanks to advances in telecommunications infrastructure. Telecommunications technologies comprise all the physical and digital infrastructure that enables information to flow across the internet and between devices and systems. The global telecommunication infrastructure is expected to continue evolving rapidly and already encompasses a wide range of technologies including Wi-Fi, optical fibre, light-fidelity and fifth-generation mobile networks (5G) (Deloitte, 2017; ENISA, 2019). Advances in telecommunications technologies in the next years are expected to increase bandwidth, decrease latency and increase spectral efficiency, leading to greater connectivity and a more digitalised world.

The coming decade is likely to see a continuation of the shift from offline to online, with more devices, systems and services becoming digital and connected, including in critical infrastructure sectors (Bogan & Feeney, 2020). This will extend to military platforms and activities, providing for a greater impact of cyber threats beyond the cyber domain to traditional military domains of operations and the day-to-day functioning of military institutions (Kepe et al., 2018). Sensors, computing, data storage and telecommunications technology are therefore expected to play a key enabling role for trends and challenges discussed in Section Three of this chapter.

D. Satellites and Space Assets

Satellites and space assets comprise all those technologies that facilitate access to and maintain superiority within orbital and sub-orbital environments in support of ground-based operations. Under this umbrella fall a wide variety of systems and instruments including expendable and reusable launch vehicles, High Altitude Pseudo Satellites (HAPS) and novel satellites. Space assets and technologies also comprise space-based systems supporting ground operations (e.g., for sensing, navigation, or communication) and counterspace and anti-satellite systems (e.g. anti-satellite missiles and jamming technologies) (Black, 2018; Kepe et al., 2018; ESA, 2018; Unal, 2019).

[3] I.e. a trend to manufacture ever smaller mechanical, optical and electronic products and devices.

Future advances in this field are expected to result in progressively reduced technological and financial barriers, encouraging greater activities in space. For instance, commercial space launches and the broader commercial use of space are expected to continue growing after having witnessed significant growth in the last decade (Space Policy Online, 2020). This, in turn, could result in an increasingly congested operating environment where it may be difficult to monitor and distinguish threats from non-threats. Broader advances in space technologies are also expected to enable them to perform a wider array of functions and further expand the contribution and critical enabling that space technologies can offer to ground operations. Low-orbiting small satellites may improve situational awareness, for example by transmitting high-resolution, real-time video directly into the cockpit of military aircraft (Space News, 2019). HAPS could be used to better monitor crises and adversarial activities, as well as to develop more accurate and reliable navigation capabilities (ESA, 2020).

From a NATO perspective, space-based assets already provide critical enabling functions to most military engagements and operations occurring across the land, air, cyber and maritime domains. In turn, satellites and most space assets are characterised by a complex supply-chain and by a significant degree of dependence on cyber-based enabling capabilities. Advances in space technologies and their further embedding in NATO's daily operations could result in cyber threats and vulnerabilities associated with these technologies disproportionately affecting NATO missions and operations (Unal, 2019). As the space domain becomes accessible to actors other than a small cohort of technologically advanced states, the volume and significance of cyber threats against space systems are expected to increase. In this context, threat actors could leverage jamming, spoofing and hacking attacks on communications networks, hijacking of satellites' control systems and mission packages or conduct, as well as cyber attacks on-ground infrastructure and their associated cyber assets (e.g., data centres) (Unal, 2019; Livingstone & Lewis, 2016).

E. Human-Machine Interfaces

The coming decade is likely to see not only an increase in technology use and reliance but also a growing integration of human and machine. As technological systems continue to grow in scale and complexity, humans are likely to expand their role as users of technology to become purveyors, operators and exploiters of these systems (Yanakiev, 2020). Brain-computer interfaces (BCI) and human-machine interfaces (HMI) enable the connection of the human nervous system to electromechanical systems, leveraging advances in neural engineering, nanotechnology and computational neurosciences (Ienca & Haselager, 2016). BCI and HMI are still emerging research areas, but promising technologies and applications have already been illustrated by industry, including brain-controlled computer systems, robotic limbs, neuro-prostheses, brain-stimulators, cognitive orthotics and hearing and visual implants (Chai et al., 2017).

BCI, HMI and wider human-machine teaming have also attracted significant interest from the defence sector with several areas under investigation, including brain-controlled weapons systems, drone swarms and training and exercise applications (Chai et al., 2017; Tucker 2018). HMI has also been particularly explored in relation to manned and unmanned aircraft where it is perceived to be able to facilitate improved information handling and enhance the human operator's effectiveness (Lim et al., 2018). For example, the US Defense Advanced Research Projects Agency (DARPA) is developing an HMI system aimed at reducing pilot workload, augmenting mission performance and improving aircraft safety. It is known as the Aircrew Labour In-Cockpit Automation System (ALIAS). The coming decade is likely to see further integration of humans and machines across society, including in defence, and may prove to offer hitherto unattainable performance in data processing, analysis and decision-making support.

The implications for NATO may, therefore, be wide-ranging and considerable. The shift from humans simply being users of technology towards being part of a complex and connected technological system will both bring opportunities for capability improvement and new vulnerabilities and risks. The future adoption of HMI within NATO and its member countries will require significant efforts in developing appropriate technology and processes across the doctrine, organisation, training, materiel, leadership, personnel, facilities and interoperability (DOTMLPF-I)[4] spectrum, including the relevant knowledge, skills and abilities needed for human-machine integration. The closer integration of humans and technological systems may also lead to significant cyber vulnerabilities that could be exploited by adversaries by, for example, compromising the integrity of information from an HMI to the human operator, such as a pilot, thereby increasing the risk of operator error or failure. Through HMI, humans will comprise a significant part of the system and their behaviour may thus affect the level of system security that can be achieved. The human aspect of cyber security is an emerging area of knowledge and research and substantial efforts are likely to be required to achieve cyber-secure HMI in the future.

F. Quantum Computing

Quantum technologies can be defined as technologies that seek to exploit the properties of quantum science to achieve functions or levels of performance that may otherwise be unattainable or explainable. The properties of quantum science, where subatomic particles (qubits) can exist in two states simultaneously, enable a wide range of novel technologies and applications that go beyond current capabilities. Prominent emerging quantum technology areas include quantum computing, which can enable parallel, faster and less energy-consuming data processing (Innovate UK, 2019), quantum communications, quantum cryptography (Pirandola et al., 2019), quantum sensors (UK Government Office for Science, 2016) and quantum clocks (European Commission Joint Research Centre, 2016).

[4] DOTMLPF-I is a way of describing the essential elements of military capability development (NATO, 2016).

Quantum advances may result in transformational and fundamental shifts in several S&T areas, making their time of realisation and effect inherently difficult to predict. Fully realised quantum computers may be able to overcome the performance limitations of current computing approaches by enabling the parallel processing of data with hugely improvedl speed, precision and detail, potentially revolutionising the future information environment. Within the cyber domain, advances in quantum cryptography could compromise current encryption approaches, posing fundamental challenges to the integrity and security of all NATO data and communications. Further advances in quantum sensing and timing may also create new types of information or insights, contributing to advances in situational awareness and shedding light on previously opaque complexity that can be exploited by NATO and adversaries alike. As with many emerging technologies, quantum technologies may have a 'first mover' advantage that offers potentially significant advantages to the first adopter.

3. DISCUSSION—CROSS-CUTTING THREATS AND IMPLICATIONS

Technological developments and trends of the types discussed in this paper are expected to have profound effects on all levels of society in the coming decade, including on NATO, its member states and its missions and operations. The research cited in this paper also suggests that these technologies will have a significant effect on the cyber threat landscape and, perhaps more concerningly, that the pace and impact of technological change may be so profound that the ability of NATO and its member states to cope with them is surpassed. If the Alliance is unable to keep pace with technology, it may find itself at a disadvantage compared to its adversaries or subject to technological vulnerabilities that could be exploited by adversaries.

In this context, successfully leveraging new and emerging technologies in a timely manner will be key to ensuring NATO's ability to maintain a technological edge in critical areas, including in cyberspace. While we have previously discussed cyber threats that may stem from developments in specific technology areas, these technologies will not operate in silos in the future but rather build on and interact with one another in ways that will result in additional, broader trends and challenges. From a cyber threat perspective, an array of cross-cutting trends and implications should be highlighted and considered by NATO in the coming decade.

A. Complex Synergies and Effects

The most significant impact on the cyber threat landscape will not stem from any individual technology but rather from the complex interaction and combination of different new and existing technologies and broader interplay with the socio-technological environment. The degree of penetration and pervasiveness that new and emerging technologies will achieve over the next decade is expected to span across defence, security, critical infrastructure

and the overall day-to-day functioning of societies. This is likely to significantly increase the volume and impact of threats, vulnerabilities and disruptions associated with digital technologies and societal systems that depend on ICTs. Beyond the volume of potential threats, the coming decade is also likely to further compound the competitive advantage for attackers as malicious actors and adversaries will be less constrained in leveraging emerging technology for offensive purposes due, for example, to their reduced regulation, lower ethical or moral standards, or fewer requirements for testing and validation. This is particularly prominent in the cyber domain, where adversary activities are perceived as low-risk due to attribution challenges, difficulties in cross-border cooperation, differing national laws, lack of adequate legislation and diverging normative views of responsible behaviour in cyberspace (Rid & Buchanan, 2015).

The wide penetration and pervasiveness of emerging technologies may also result in cascading effects which could be difficult to predict or mitigate in increasingly complex and non-linear systems. The exploitation of system vulnerabilities or system failures may result in much broader impacts due to previously unforeseen linkages and embedded co-dependencies, potentially even spanning geographical areas and national boundaries. Continuous technology evolution and varying rates of technology development and adoption will also present significant challenges for NATO in monitoring and understanding the interaction of different technologies, particularly in increasingly complex supply chains. Advances in fields such as telecommunications and computing technologies and sensors are expected to achieve maturity over a shorter time frame, partly due to lower barriers to implementation. Conversely, other potentially disruptive technologies such as quantum computing and more advanced forms of AI and autonomous systems are characterised by greater uncertainty as regards their epoch, making it difficult to anticipate and articulate their expected impact over the next decade (Kepe et al., 2018; Bellasio et al., 2020). The complexity of technology adoption and the challenges associated with mapping and monitoring the threats and vulnerabilities associated with them could, therefore, significantly undermine NATO's ability to protect critical digital and physical infrastructure and retain information superiority.

Much of the innovation and envisioned advances are expected to occur in the private sector through non-defence companies that may be reluctant to support military programmes. For example, cultural and interest divides between the US Department of Defence and the US technology sector have resulted in strained collaborations and the cancellation of several R&D programmes including in AI and facial recognition programmes (Zegart & Childs, 2018). In contrast, China's military-civil fusion policy seeks to foster innovation in several emerging technology areas through an array of policies and other government-controlled mechanisms (US-China Economic and Security Review Commission, 2019). Much innovation in emerging technologies is also taking place in non-NATO countries: China, for example, is emerging as a leader in quantum science (Kania & Costello,

2018) and Japan, South Korea and Taiwan are leaders in areas such as sensors and controls for autonomous vehicles and flexible electronics (Alliance for Manufacturing Foresight, 2019).

This adds further layers of complexity to the challenge and could put NATO and its member states at a disadvantage, limiting access to technological innovation and putting the Alliance and its institutions in a reactive position. This is particularly concerning as an increasing number of services and key enabling technologies are developed and supplied by a limited number of companies and service providers outside NATO's influence or control, which could jeopardise or undermine the security of NATO's supply chains. This could, for example, result in embedded vulnerabilities or unknown systemic weakness that could be used to gain access to critical mission systems or cause significant cascading or systemic disruptions.

B. Hybrid or Sub-Threshold Activities

Several new and emerging technologies have and will continue to facilitate the adoption of hybrid tactics and the undertaking of activities below the threshold of war with increased difficulty in attributing and understanding adversaries' activities and their impact (Thiele, 2020). Advances expected in AI, telecommunications and computing technologies and autonomous systems could facilitate improved ways of delivering known methods, such as deep fakes or the creation of mis- or disinformation, or the creation of entirely novel attacks and approaches. This could include the proliferation of real-time video deep fakes at scale (Seymour, 2018) or advanced voice manipulation (Vincent, 2020) which adversaries could use to manipulate messages from policymakers and military commanders.

Such activities could include, for example, election meddling, influence operations and economic coercion. Such advances present serious risks to the information environment and could undermine NATO, its member states and their institutions by reducing the social cohesion and resilience critical to maintaining socio-economic stability and prosperity. A significant growth in sub-threshold and hybrid activities in the next decade may undermine the integrity and verifiability of data and information. This would make it increasingly difficult to understand where information comes from, where it is going, how and why it was created and who created it, such as, for example, the emergence of competing 'facts' without clear origin that cannot be easily verified or challenged. This could emphasise current trends of misinformation and associated issues, but it could also lead to more consequential systemic effects where the general population loses faith in technology, data or government institutions. These developments may threaten the very foundations of society and will likely require increasingly agile and creative responses from NATO and its member states for their successful mitigation.

C. Exacerbation of Current Trends and Grey Swan Scenarios

The technologies highlighted in this paper may contribute to the exacerbation of current trends in the cyber threat landscape and herald so-called grey swan scenarios.[5] The increasing availability of powerful, easy-to-use and inexpensive technologies is likely to further stimulate the conduct of malicious activities by a wide array of state and non-state actors. The democratisation and 'servitisation'[6] of technology have enabled consumer access to a wide range of technologies that were previously accessible only by governments. This includes enabling technologies like additive manufacturing and large-scale distributed computing, to more niche technological services such as on-demand development of bespoke software-defined radio applications that could be used for disrupting the electromagnetic environment. While most of these activities are likely to entail low-tech tactics, this trend could result in an even greater volume of malicious activities than currently witnessed.

The development of new, complex technological solutions and capabilities may also enable state-sponsored actors to conduct advanced, covert or persistent attacks and activities which could undermine or jeopardise NATO's missions and day-to-day operations by, for example, exploiting unknown vulnerabilities in the NATO supply chain to gain access to sensitive information. Sophisticated and persistent attacks are likely to be less frequent, making these threats more challenging for NATO to identify, detect, prepare for and manage due to limited exposure to and knowledge of the tactics, techniques and procedures (TTP) employed. The proliferation of connected and embedded systems, particularly through a drive towards the Internet of Things (IoT) and the digitalisation of legacy infrastructure may also increase NATO's attack surface and the likelihood of vulnerabilities that could be exploited by malicious actors.

Technological advances are also expected to contribute to an increased ability to record, store, process and analyse data, which will be further compounded by greater connectivity coverage and speeds. The proliferation of new and existing sensors across a growing number of systems and devices will improve data collection capabilities and contribute to the creation and collection of new data types. In the coming decade, these could lead to a near-ubiquitous ability to access and manipulate data, for instance through cloud storage and miniaturised processors. This would provide greater opportunities for the conduct of malicious activities, including through hitherto unseen TTPs, facilitating the exfiltration of sensitive data and making it increasingly difficult to operate without being monitored (Bogan & Feeney, 2020). Increased connectivity, through both an increasing number of connected devices and the adoption of new technologies such as 5G, is

[5] A grey swan scenario refers to an event that could have significant cascading impact that is seen as unlikely, but not impossible.

[6] A trend whereby vendors not only sell products and devices but also offer services. For example, this can result in vendors of certain technologies providing access to enabling or maintenance services for their products, leading to increasingly complex business models, supply chains, liability and ownership arrangements.

also expected to result in an increased volume and speed of activities being conducted, including by adversaries. The proliferation of data may further challenge the ability to identify, detect and attribute malicious activities in Alliance ICT systems and present novel challenges such as difficulties in maintaining privacy and anonymity in datasets. For example, an increasingly rich data environment may enable adversaries to better hide information using steganography techniques to bypass security controls or to exfiltrate sensitive data, also making it more difficult to understand how attacks were perpetrated and who may have been behind them (Cabaj et al., 2018).

With respect to data analysis capabilities, advances in computing power accompanied by developments in AI/ML are expected to contribute to a growing ability to process and analyse data, allowing inferences and results currently beyond the reach of human and current data science capabilities. This trend, perhaps amplified by HMI, could lead to an ability to infer and extrapolate sensitive information from different data types not considered sensitive or threatening when taken in isolation. For example, research has already shown that present-day capabilities allow for the de-anonymisation of incomplete datasets with data on demographic attributes (Rocher et al., 2019).

These advances are expected to contribute to the development of new forms of malicious activities and could hold particularly true in light of the growing potential for the automation and large-scale running of existing malicious activities. Finally, the democratisation of computing power, particularly through the growth of on-demand, scalable and inexpensive cloud data services such as Amazon Web Services and Microsoft Azure, may enable a wider range of actors, including non-state groups, to attain advanced analytical capabilities.

4. SUMMARY AND CONCLUSION

While advances in new and emerging technologies are not expected to be the sole drivers and factors affecting the future cyber threat landscape, their impact should not be underestimated or overlooked. Certainly, the multifaceted and uncertain nature of the future technology landscape, as discussed in section two, and the complex trends and effects expected to stem from it, as presented in section three, will require the adoption of flexible, innovative and forward-looking responses and approaches. No single solution will enable NATO and its member states to respond to the wide array of advances occurring in the technology landscape or to effectively manage new threats in the cyber domain. Bearing this in mind, a number of measures could be considered for adoption by NATO to prepare for future challenges emerging in the cyber threat landscape.

A. Ensuring an Absorptive Capacity for Innovation and Transformation
NATO and its member states need to ensure that the Alliance can prepare for, respond to and exploit advances in the technological and cyber landscapes.

The absorptive capacity – in other words, the ability for NATO to recognise and harness the value of emerging technologies – relies on a complex system with many interacting factors. Previous RAND research has identified several factors that enable innovation and transformation in defence, including organisational culture, input factors such as knowledge, talent and capital, and enabling resources such as infrastructure, networks and connections (Freeman et al., 2015).

NATO should, therefore, consider how best to adapt its organisational culture, civilian and military structures, organisations and agencies to recognise and absorb innovation in the cyber domain in the coming decade. While a range of relevant bodies is already in place including the NATO Science and Technology Organisation, the Emerging Security Challenges Division, the Joint Intelligence and Security Division, the NATO Communications and Information Agency and the Cyber Operations Centre, these considerations may require further adjustments depending on which technology area, or combination thereof, is ultimately pursued. Adjustments could entail placing a specific focus on: (i) whether current procurement processes are fit for purpose; (ii) whether NATO is in a position to contribute to the development and definition of legal and regulatory standards for the use of different technologies; and (iii) the requirements for and availability of adequate testing and assurance mechanisms for the use of emerging technologies in a military context.

B. Enabling the Identification of Emerging Technology Requirements and Cooperation with Industry

Beyond the absorptive capacity for innovation and transformation, NATO must also be in a position to identify emerging technologies of interest, their implications to NATO and what the Alliance's requirements in relation to those technologies may be. As previously noted, being an early adopter or creating a technological edge over adversaries and competitors will be pivotal to enable NATO and its member states to hold a strategic advantage and superiority in the cyber domain. Some of the technologies presented in this paper will also act as enablers, expanding and deepening the impact of other existing and developing technologies.

In this context, NATO should seek to be in a position to gather intelligence continuously and systematically on emerging science and technology developments and their potential implications for NATO through approaches such as strategic foresight analysis, horizon scanning, scenario planning and analytical gaming. This will enable the Alliance to improve its posture and agility with early warning signs of technologies that may be exploited by adversaries in the future. Activities in this regard are ongoing through Allied Command Transformation Strategic Foresight Analysis (e.g., ACT, 2017), the NATO Science and Technology Organisation and NATO education and training institutions such as the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Defence College (e.g., Gilli, 2020). The work of other NATO Centres of Excellence could also facilitate the identification and

monitoring of relevant technologies of interest across different areas.

A fundamental part of ensuring this will be close consultation and cooperation with industry. Many of these emerging technologies will be primarily developed in the private sector and often by companies that traditionally have not worked within the defence sector. NATO must therefore be able to clearly communicate its innovation and transformation needs and explain why it may be worthwhile for non-traditional defence suppliers to support defence needs and engage with the Alliance. It is also essential that NATO encourages and enables its member states to leverage the expertise and knowledge found in the private sector to understand the state-of-the-art in the different emerging technology areas and what opportunities or risks they may bring. This entails enabling and maintaining partnerships that go beyond customer-supplier relationships and should involve structures for innovation where inventors, investors and industry can partner with NATO across a wide range of emerging technology areas to better meet the cyber challenges of the coming decade. In this regard, the NATO Industry Cyber Partnership has already laid the foundation for engagement between NATO and industry in the cyber domain that goes beyond information sharing for improved situational awareness to building trust and access between NATO and the private sector, including for capability development purposes (NICP, 2018). NATO Smart Defence could also act as an example on which to build the blueprint for identifying requirements and cooperatively generating future capabilities, bringing together not just Alliance members, but industry representatives and stakeholders more broadly (NATO, 2017).

C. Strengthening Trust and Interoperability Across the Alliance

The coming decade will be of pivotal importance to NATO as a period characterised by a continuously evolving technology landscape with potentially disruptive effects in the cyber domain and beyond. In an era of uncertainty, constrained resources and political tension, cooperation and trust will be fundamental enablers of an agile, technology-driven and digital NATO. Only through joint efforts will NATO truly be able to harness the potential of the emerging technologies discussed in this chapter and successfully mitigate the risks and threats they may pose in the future. The need for trust therefore extends to both trust in technology and trust in the Alliance and its member states.

Similar to how the effects of emerging technologies should not be treated in isolation, NATO's response to emerging technologies must be one of joint efforts and interoperability. Technical, legal, financial and organisational barriers to the implementation of emerging technologies are more likely to be overcome through joint capability and force development efforts, which will, by extension, also help build trust and facilitate interoperability. Several of the emerging technology areas discussed in this paper would place significant data, infrastructure and interoperability requirements on NATO, which may be particularly difficult to overcome given the current state of data heterogeneity and sometimes incompatible digital infrastructure across the

Alliance. Several emerging technologies would also require interoperability in relation to shared vocabularies of technical terms, norms, standards and organisational practices, as well as human interoperability and joint training and exercising. For example, AI has been highlighted as a potential area of concern where a lack of interoperability and common definitions paired with technological mismatches could erode Alliance cohesion (Dufour, 2018).

Joint efforts are, therefore, likely to help overcome these challenges and barriers to NATO harnessing emerging technologies in the next decade. While the 30-member Alliance may be at a competitive disadvantage compared to single state or non-state adversaries in relation to interoperability barriers, NATO's collective strength may also serve as an enabler for technological superiority. Joint planning, requirement setting, and development may enable individual member states to pursue specialisation in aspects of particular emergent technology areas, thereby allowing other countries to pursue other specialisations and, by extension, increasing the overall capability within the Alliance.

5. REFERENCES

Allied Command Transformation. (2017) Strategic Foresight Analysis 2017. Available from: https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf [Accessed 20th October 2020].

Alliance for Manufacturing Foresight. (2019) 'Reclaiming America's Leadership in Advanced Manufacturing'. Available from http://mforesight.org/download-reports/ [Accessed 24th September 2020].

Beijing Innovation Centre for Future Chips. (2018) White Paper on AI Chip Technologies. Available from: https://www.080910t.com/downloads/AI%20Chip%202018%20EN.pdf [Accessed 21st August 2020].

Bellasio, J., Silfversten, E., Leverett, E., Quimbre, F., Knack, A. & Favaro, M. (2020) *The future of cybercrime in light of technology developments.* Prepared for the European Commission Structural Reform Support Service (Ref: SRSS/C2018/092).

Black, J. (2018) 'Our reliance on space tech means we should prepare for the worst'. *Defensenews.com*. Available from https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/ [Accessed 21st August 2020].

Bogan, J. & Feeney, A. (2020) *Future cities: Trends and implications.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875528/Dstl_Future_Cities_Trends____Implications_OFFICIAL.pdf [Accessed 23rd September 2020].

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A. & Zander, S. (2018) The new threats of information hiding: The road ahead. *IT Professional*, 20 (3), 31-39. Available from: https://arxiv.org/ftp/arxiv/papers/1801/1801.00694.pdf [Accessed 20th October 2020].

Cauduro, A. (2018) Live Deep Fakes – you can now change your face to someone else's in real time video applications. *Medium*. Available from: https://medium.com/huia/live-deep-fakes-you-can-now-change-your-face-to-someone-elses-in-real-time-video-applications-a4727e06612f [Accessed

12th August 2020].

Chai, R., Naik, G.R., Ling, S.H. & Nguyen, H.T. (2017) Hybrid brain–computer interface for biomedical cyber-physical system application using wireless embedded EEG systems. *Biomedical engineering online*. 16 (1), 5. [Accessed 20th August 2020] Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5234249/

Cole, S. 2020 *This Open-Source Program Deepfakes You During Zoom Meetings, in Real Time*. Available from: https://www.vice.com/en_us/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time [Accessed 23rd September 2020].

Danks, D. 2020 *How Adversarial Attacks Could Destabilize Military AI Systems.* Available from: https://spectrum.ieee.org/automaton/artificial-intelligence/embedded-ai/adversarial-attacks-and-ai-systems [Accessed 23rd September 2020].

DARPA. (2020) *Aircrew Labor In-Cockpit Automation System (ALIAS).* Available from https://www.darpa.mil/program/aircrew-labor-in-cockpit-automation-system [Accessed 24th September 2020].

Deloitte. (2017) *Communications infrastructure upgrade: The need for deep fiber.* Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5GReady-the-need-for-deep-fiber-pov.pdf [Accessed 20th August 2020].

Dufour, M. 2018 Will artificial intelligence challenge NATO interoperability? *NDC Policy Brief.* Available from: http://www.ndc.nato.int/news/news.php?icode=1239# [Accessed 23rd September 2020].

ENISA. (2019) *ENISA threat landscape for 5G network.* Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [Accessed 18th August 2020].

European Commission. (2019) *A definition of Artificial Intelligence: main capabilities and scientific disciplines.* Available from: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [Accessed 20th August 2020].

European Commission Joint Research Centre. (2016) *Quantum Technologies: Implications for European Policy*. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC101632/lbna28103enn.pdf [Accessed 20th August 2020].

ESA. (2018) *Could High-Altitude Pseudo-Satellites Transform the Space Industry?* Available from: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Could_High-Altitude_Pseudo-Satellites_Transform_the_Space_Industry [Accessed 20th August 2020].

ESA. 2020 *Services enabled by High Altitude Pseudo Satellites (HAPS) complemented by satellites.* Available from: https://business.esa.int/projects/services-enabled-haps [Accessed 23rd September 2020].

Fong, T. (2018) *Autonomous systems: NASA capability overview.* Available from: https://www.nasa.gov/sites/default/files/atoms/files/nac_tie_aug2018_tfong_tagged.pdf [Accessed 20th August 2020].

Freeman, J., Hellgren, T., Mastroeni, M., Persi Paoli, G., Cox, K. & J. Black. (2015) *Innovation Models: Enabling new defence solutions and enhanced benefits from science and technology.* Available from: https://www.rand.org/pubs/research_reports/RR840.html [Accessed 21st August 2020].

Gilli, A. (2020) *NATO and 5G: what strategic lessons? NDC Policy Brief.* 13(July 2020).

Available from https://www.ndc.nato.int/research/research.php?icode=0 [Accessed 18th August 2020].

GSMA. (2019) *Mobile Telecommunications Security Threat Landscape.* Available from https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf [Accessed 18th August 2020].

Hartmann, K. & Steup, C. 2020 Hacking the AI – The Next Generation of Hijacked Systems. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. & G. Visky (eds.) *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade.*

Hess, J., Kiser, A., Bouhafa, E.M. & Williams, S. (2019) The Combat Cloud: Enabling Multidomain Command and Control across the Range of Military Operations. *Wright Flying Papers, Air Command and Staff College.* February 2019. Available from: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/wf_0065_hess_combat_cloud.pdf [Accessed 14th August 2020].

Ienca, M. (2015) Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. *Bioethica Forum*. 8 (2), 51-3. Available from: https://edoc.unibas.ch/39747/ [Accessed 20th August].

Innovate UK. (2019) *Innovate UK: Global Expert Mission Quantum Technologies in the USA.* Available from: https://admin.ktn-uk.co.uk/app/uploads/2020/03/0183_KTN_USA-QuantumTechnologiesReport_v4.pdf [Accessed 21st August 2020].

Joshi, N. 2019) 7 Types of Artificial Intelligence. *Forbes*. 19 June 2019. Available from: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#6eb1f3ad233e [Accessed 21st August 2020].

Kajander, A., Kasper, A. & Tsybulenko, E. (2020) Making the Cyber Mercenary – Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. & G. Visky (eds.) *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade.*

Katano, Y., Muroi, T., Kinoshita, N. & Ishii, N. (2017) Prototype holographic data storage drive with wavefront compensation for playback of 8K video data. *IEEE Transactions on Consumer Electronics.* 63(3). Available from: https://ieeexplore.ieee.org/document/8103372 [Accessed 18th August 2020].

Kepe, M., Black, J., Melling, J., & Plumridge, J. (2018) *Exploring Europe's capability requirements for 2035 and beyond Insights from the 2018 update of the long-term strand of the Capability Development Plan*. Available from: https://www.eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf [Accessed 12th August 2020].

Kersting, K. (2018) Machine learning and artificial intelligence: two fellow travelers on the quest for intelligent behaviour in machines. *Specialty Grand Challenge 1.* Available from: https://ml-research.github.io/papers/kerstingg2018aiml_frontiers.pdf [Accessed 12th August 2020].

Leikas, J.; Koivisto, R.; & Gotcheva, N. (2019) Ethical Framework for Designing Autonomous Intelligent Systems. *J. Open Innov. Technol. Mark. Complex.* 5 (1), 18. Available from: https://doi.org/10.3390/joitmc5010018 [Accessed 21st August 2020].

Lim, Y., Ramasamy, S., Gardi, A., Kistan, T. & Sabatini, R. (2018) Cognitive human-machine interfaces and interactions for unmanned aircraft. *Journal of Intelligent & Robotic Systems*. 91 (3-4), 755-774.

Livingstone, D. & P. Lewis. (2016) *Space, the Final Frontier for Cybersecurity?* Available from: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf [Accessed 23 September 2020].

McCarthy, J. (2007) *What Is Artificial Intelligence? Technical report.* Stanford University. Available from: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf [Accessed 12th August 2020].

Myers, A. (2019) *Stanford engineers make editing video as easy as editing text.* Available from: https://news.stanford.edu/2019/06/05/edit-video-editing-text/ [Accessed 23 September 2020].

NATO. (2016) *Joint Analysis Handbook* Available from http://www.jallc.nato.int/products/docs/Joint_Analysis_Handbook_4th_edition.pdf [Accessed 24th September 2020].

NATO. (2018) *Smart Defence*. Available from: https://www.nato.int/cps/en/natohq/topics_84268.htm [Accessed 23 September 2020].

NATO. (2020a) *Cyber defence*. Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 13th August 2020].

NATO. (2020b) *NATO's approach to countering disinformation: a focus on COVID-19*. Available from: https://www.nato.int/cps/en/natohq/177273.htm [Accessed 23 September 2020].

NATO CCD COE. (2020) *Exercises*. Available from: https://ccdcoe.org/exercises/ [Accessed 23 September 2020].

NICP. (2018) *Our objectives and principles*. Available from: https://nicp.nato.int/objectives-and-principles/index.html [Accessed 23 September 2020].

Pirandola, S., Andersen, U. L., Banchi, Berta, L., M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J.S., Tomamichel, M., Usenko, V.C., Vallone, G., Villoresi, P., and Wallden, P. (2019). *Advances in Quantum Cryptography. Quantum Physics*. Available from: https://arxiv.org/abs/1906.01645 [Accessed 12th August 2020].

Randori. (2020) *Randori Recon: Shining Light on Your Most Tempting Targets.* Available from: https://www.randori.com/randori-recon-shining-light-on-your-most-tempting-targets/ [Accessed 23 September 2020].

Rid, T & Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*. 38 (1-2), 4-37.

Rocher, L., Hendricks, J.M., & Montjoye, Y. M. (2019) Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications.* 10 (3069).

Scharre, P. (2018) *Army of None: Autonomous Weapons and the Future of War*. London, UK: W.W. Norton & Company.

Seymour, M. (2018) *A.I. at SIGGRAPH: Part 2. Pinscreen at Real Time Live.* Fxguide. Available from https://www.fxguide.com/fxfeatured/a-i-at-siggraph-part-2-pinscreen-at-real-time-live/ [Accessed 24th September 2020].

Shaik, M., Shaik, N., & Ullah, W. (2016) The Wireless Sensor Networks: Smart Dust. *International Research Journal of Engineering and Technology.* 3 (6). Available from: https://www.irjet.net/archives/V3/i6/IRJET-V3I6172.pdf [Accessed 20th August 2020].

Shea, J. (2018) Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy? *MCU Journal*. 9 (2), 133-150. Available from: https://doi.

org/10.21140/mcuj.2018090208 [Accessed 10 August 2020].

Space News. (2019) *U.K. deepens space ties with U.S., announces investments in small satellites, responsive launch*. Available from: https://spacenews.com/u-k-deepens-space-ties-with-u-s-announces-investments-in-small-satellites-responsive-launch/ [Accessed 23 September 2020].

Space Policy Online. (2020) *Commercial Space Activities*. Available from: https://spacepolicyonline.com/topics/commercial-space-activities/ [Accessed 23 September 2020].

Thiele, R. (2020) *Artificial Intelligence – A Key Enabler of Hybrid Warfare. Hybrid CoE Working Paper 6*. Available from https://www.hybridcoe.fi/wp-content/uploads/2020/03/WP-6_2020_rgb.pdf [Accessed 24th September 2020].

Tucker, P. (2018) It's now possible to telepathically communicate with a drone swarm. *Defense One*. Available from https://www.defenseone.com/technology/2018/09/its-now-possible-telepathically-communicate-drone-swarm/151068/ [Accessed 21st August 2020].

UK Government Office for Science. (2016) *The Quantum Age: technological opportunities.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf [Accessed 21st August 2020].

Unal, B. (2019) *Cybersecurity of NATO's Space-based Strategic Assets. Chatham House*. Available from: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf [Accessed 21st August 2020].

U.S.-China Economic and Security Review Commission. (2019) *2019 Annual Report to Congress*. Available from https://www.uscc.gov/annual-report/2019-annual-report-congress [Accessed 24th September 2020].

Vallor, S., & Bekey, G. A. (2017) Artificial Intelligence and the Ethics of Self-learning Robots. In Lin, P., Abney, K., & Jenkins, R. (eds.) *Robot Ethics 2.0.* Oxford University Press, pp. 338-353.

Vincent, J. (2020) This is what a deepfake voice clone used in a failed fraud attempt sounds like. *The Verge*. Available from https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos [Accessed 24th September 2020].

Waltzman, R., Ablon, L., Curriden, C., Hartnett, G. S., Holliday, M. A., Ma, L., Nichiporuk, B., Scobell, A. & Tarraf, D. C. (2020) *Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning*. Available from: https://www.rand.org/pubs/research_reports/RRA200-1.html [Accessed 21st August 2020].

Williams, L.C. (2020) *JADC2 Tops Pentagon's Artificial Intelligence Efforts.* FCW, 9 July 2020. Available from: https://fcw.com/articles/2020/07/09/williams-jaic-ai.aspx [Accessed 13th August 2020].

Wong, Y.H., Yurchak, J.M., Button, R.W., Frank, A., Laird, B., Osoba, O.A., Steeb, R., Harris, B.N. & Bae, S.J. (2020) *Deterrence in the Age of Thinking Machines.* Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf [Accessed 12th August 2020].

Xiao, L., Jianying, H., Mingjie, Z., Tiangui, D., Hui L. & Yuhong, R. (2019) Optical holographic data storage — The time for new development. *Opto-Electronic Engineering*. 46(3). Available from http://www.oejournal.org/J/OEE/Article/Details/A190315000012 [Accessed 20th August 2020].

Yanakiev, Y. (2020) Introduction to NATO STO Task Group Hfm-259: Human Systems