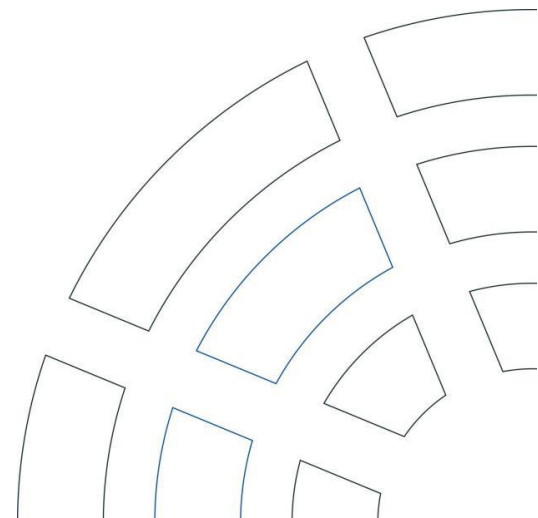# SCIENCE AND TECHNOLOGY COMMITTEE (STC)

PRELIMINARY DRAFT GENERAL REPORT

STRENGTHENING ALLIANCE S&T RESILIENCE

Preliminary Draft General Report
Nusrat GHANI (United Kingdom)
Rapporteur

023 STC 22 E – Original: English – 9 May 2022

Innovation is key to NATO's deterrence and defence. Yet more than ever, upholding a competitive pace in Research and Development (R&D) will be instrumental for NATO to dominate future warfighting domains.

NATO's innovation pipeline needs to adapt to rapidly changing security environments. Competitors invest considerable resources of their own and use illicit means to challenge the innovation achieved by NATO and like-minded countries. The innovation ecosystems have also changed and are now driven mostly by private companies and independent research institutes rather than governments.

This draft report identifies challenges to NATO's innovation pipeline. These include threats by adversaries, particularly the People's Republic of China (PRC) and Russia. The draft focuses on risks arising from economic and scientific espionage and the need to secure critical resources for the development of Emerging and Disruptive Technologies (EDTs). The preliminary draft also argues that attempts from competitors to contest norms and standards pose an additional problem, which requires urgent attention.

The rapporteur provides a short overview of efforts designed to strengthen Science and Technology (S&T) Resilience in the Alliance. The draft report concludes with several recommendations on how to make NATO's S&T endeavours more resilient. These include, among others: maintaining NATO's technological edge by increasing investment and cooperation around critical technologies; enhancing and deepening NATO's digitisation processes; and strengthening common understanding of ethical standards for these technologies.

TABLE OF CONTENTS

I-   INTRODUCTION

1.   The pace of technological innovation is increasing rapidly, affecting all sectors of society. This trend towards an ever-increasing importance of technology is prone to developing hitherto unsuspected national security issues for Allies. The heated debate around the implementation of 5G wireless networks (Gilli and Bechis, 2019), as well as examples of cyberespionage on pharmaceutical companies during the COVID-19 pandemic reflect increased awareness that the resilience of science and technology sectors is not only crucial to Allied security (Bing and Taylor, 2020) and the need for a robust holistic approach.

2.   Five trends characterise the contemporary technology environment. First, technology is key in ensuring "geopolitical, economic, and military competitiveness". Second, there is a tendency toward decoupling between democratic powers and authoritarian countries. Third, digital authoritarianism is a rising technological risk. Fourth, crises like the COVID-19 pandemic show how new vulnerabilities and dependencies can arise regarding technology. Fifth, states once again prioritise industrial policies, specifically tech-driven ones (Sahin and Barker, 2021). Against this background, many believe we are currently at a new "Sputnik moment", leading to the inevitable question: "Is NATO ahead or behind?" (Stordahl, 2022; Aronhime and Cocron, 2021).

3.   NATO's increasing focus on EDTs shows that the Alliance is willing to take on these new realities. However, the question of how successful this enterprise will be is not settled yet. In other words, will NATO only marginally adapt, or will it truly be able to innovate (Soare, 2021)? Against the backdrop of heightened geopolitical competition with contenders such as China or Russia, this question will grow in importance. After the original Sputnik moment in 1957, the space race was guided by clear goals and milestones: such performance goals are once again needed today (Aronhime and Cocron, 2021).

4.   So far, efforts and policies on both sides of the Atlantic have been diverging significantly. "Europe missed the first tech boom. It is in the United States' interest that it does not miss the second" (Lewis (a), 2021). It is safe to say that NATO needs to acquire a deeper common understanding of current technological trends within the Alliance, but also in its outreach to its partners, first and foremost the EU.

5.   This report thus attempts to tackle the question of how NATO's innovation pipeline – and S&T sectors more generally – can be made more resilient. It touches upon current key risks to Allied S&T resilience and takes a broad look at how innovation and R&D are changing and how Allies adapt to these new realities.

II-   MAINTAINING THE TECHNOLOGICAL EDGE AND THE IMPORTANCE OF S&T FOR ALLIED SECURITY

6.   Scientific innovation is driving geopolitics at an unprecedented speed. It has the power to cause, among others, "new risks to public safety and national security" (Kavanagh, 2019). The dual-use nature (military and civilian) of many crucial emerging technologies magnifies the complexity policymakers face when they must define the legal framework for their use. Assessing the impact of new technologies requires not only an understanding how they will interact with other existing and emerging technologies – for instance, how a new satellite component in space will be vulnerable to new cyber security trends – but also how they will affect society, governance or economics altogether.

7.   The current debates around Artificial Intelligence and its potential and limitations testify to the multi-layered nature of the task, ranging from discussions around human-machine interaction and ethics to its concrete implementation in a growing number of sectors. Thus, "explosive growth of technological innovation is outstripping the capacity (or willingness) of technology creators, private investors, national governments, and the existing multilateral system to understand, monitor, and effectively govern the attendant effects and consequences" (Kavanagh, 2019). To address these daunting challenges, Allies need first to gain a clear understanding of how their innovation pipelines work in the contemporary socio-political context. This requires an understanding of what might constitute "resilience" of their S&T sectors and of the concrete threats putting stress on them.

8.   Within NATO, S&T is defined as the "selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration, and validation of knowledge derived through the scientific method" (NATO STO, 2022).

9.   Resilience has been defined as the "capacity to resist and recover quickly from major infrastructure shocks" (Levy, 2021). More specifically, resilience is a state in which NATO possesses the necessary "resources, infrastructure and systems that allow Allies and their societies to continue to function in the face of the full spectrum of threats and hazards, from natural disasters to cyber-attacks, and from hybrid threats to even an armed attack" (Tarry, 2021). It is the ability to "withstand shocks and surprise – to be prepared for the unexpected" (Tarry, 2021). In an increasingly complex and unpredictable security environment, resilience is key to addressing non-traditional security threats such as those mentioned above (Tarry, 2021; Levy, 2021).

10.   Resilience falls under an Article 3 commitment by Allies to "maintain and develop their individual and collective capacity to resist armed attack" (Washington Treaty). It should be noted, though, that the notion of attack has also been subsequently broadened to non-kinetic scenarios such as in the cyber realm. It is a critical element to achieve credible deterrence and defence (NATO, 2016). This was affirmed at the Warsaw Summit in 2016 and reaffirmed most recently through the Strengthened Resilience Commitment in 2021 (NATO, 2016; NATO, 2021). Resilient societies that take a whole-of-government approach involving both the public and private sectors reduce vulnerabilities that adversaries could exploit. This in turn contributes to deterrence by denial – adversaries will not attack if they understand their objectives will not be fulfilled (Roepke and Thankey, 2019).

11.   Specifically, S&T resilience relates to the ways in which: (a) NATO's S&T capabilities can support the development of resilience in key areas, such as those outlined at the 2016 Warsaw Summit; and (b) other national capabilities can enhance resilience in critical areas relating to scientific and technological development. Essentially, S&T resilience for NATO is about protecting Allies' capability to address national security concerns through S&T. Building resilience should thus be about proactively developing solutions and domestic alternatives to these current S&T-related challenges.

III- CHALLENGES TO ALLIANCE S&T RESILIENCE

A. ECONOMIC ESPIONAGE

12.   NATO Secretary General Jens Stoltenberg identified the growing nature of the economic espionage challenge in 2019: "We have seen increased efforts by other nations to try to spy on NATO allies in different ways" (Young, 2019).

13.   The People's Republic of China (PRC) poses by far the most pressing threat to Allied security in this regard (Hannas and Tatlow, 2021). Beyond the work carried out by the Chinese intelligence agency and the Ministry of State Security, the country has increasingly resorted to so-called "non-traditional" espionage, involving spies without a formal intelligence background such as university professors, scientists, researchers, enterprise employees and even students (Wong, 2022). This has the added benefit of allowing targeted collection of valuable S&T intelligence, as the spies are "intelligence amateurs, but subject matter experts" (Mattis, 2015). In return, it enables the Chinese government to enhance their own research and development processes with an accurate sense of what information is needed to undercut foreign competitors, making the Chinese intelligence system uniquely geared towards enhancing the country's economy (Mattis, 2015; Wong, 2022).

14.   It should also be noted that several Chinese laws, including the National Intelligence Law, stipulate that Chinese individuals and organisations must, if requested, support Chinese authorities with intelligence work (Yang, 2019). Moreover, the Chinese government is using technology to strengthen control over its population at home and abroad as witnessed in Xinjiang, which Beijing has used as an incubator for increasingly intrusive policing systems (Buckley and Mozur, 2019). The PRC is honing its technological surveillance prowess in Xinjiang where it keeps approximately one million Uyghurs in mass detention. According to some reports, the authorities are testing surveillance techniques in the region before being rolled out in other parts of China (Cadell, 2018).
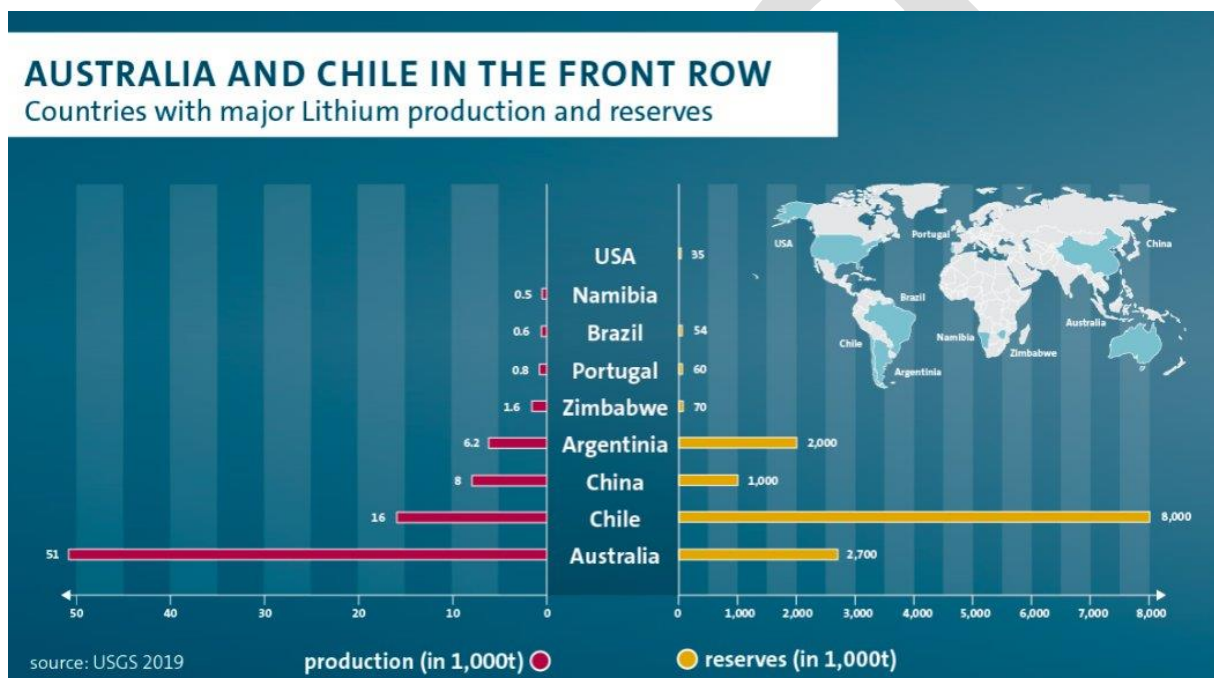
15.   Economic espionage can be facilitated by economic ties with China, especially in the area of hi-technology. The debate around the implementation of 5G broadband cellular network technology highlights the possible trade-off between using foreign, or foreign-controlled, state-of-the-art technology and shielding one's economy against outside interference. To this end, NATO stressed the importance of "the security of communications, including 5G" and acknowledged "the need to rely on secure and resilient systems" (Gilli and Bechis, 2019), to prevent backdoor access to corporate and mass communications.

16.   Near-peer competitors such as China also push their digital infrastructure and products into markets in the rest of the world. China's Belt and Road Initiative allows it to sell IT products abroad (such as basic ICT infrastructure up to advanced policing and surveillance technology), which could enable it to collect more diverse data to train its algorithms in many key sectors, geared towards the economy or national security (Pauwels, 2019). NATO should thus realise that its technological edge in data and intelligence collection can also be contested outside of its borders and seek to actively counteract or prevent such behaviour.

17.   Finally, critical R&D information can be stolen by means of cyber attacks, which has recurrently undermined research efforts undertaken by Allies. Notable examples include a data breach, attributed to China, at the US Department of Defense's subcontractor Lockheed Martin that was opened in 2007 and used for years to steal information regarding the development of the fighter jet F-35. The similarity of the F-35 to China's J-31 stealth fighter jet (Gady, 2015) shows how crucial it is to put in place effective security monitoring, including for sub-contractors working on technology with government. Even without a public-private partnership, targeting the private sector can seriously undermine national security assets, as was the case when Chinese hackers targeted the pharmaceutical company Moderna while it was developing its vaccine against the COVID-19 virus in 2020 (Bing and Taylor, 2020).

3

B. CRITICAL RESOURCES FOR THE DEVELOPMENT OF EMERGING AND DISRUPTIVE TECHNOLOGIES

18.   Due to the increasing digitisation of society and the development of EDTs, the demand for critical materials – such as component minerals for batteries or semiconductors for instance (such as aluminium, cobalt, lithium, manganese, and nickel) – will see a dramatic surge in the coming decades (Nakano, 2021). The defence sector is particularly exposed to these supply chain risks: "to produce a stealth multirole fighter Lockheed Martin F-35 Lightning II it takes 417kg of rare earths. For a missile destroyer Burke DDG-51 it takes 2,359kg and for a nuclear-powered submarine SSN-774 Virginia, as many 4,173 kg are needed" (Richiello, 2021). NATO's S&T resilience – but also its basic ability to produce state of the art weaponry, vehicles, and equipment – relies heavily on maintaining access to an affordable and secure supply of rare earth minerals.
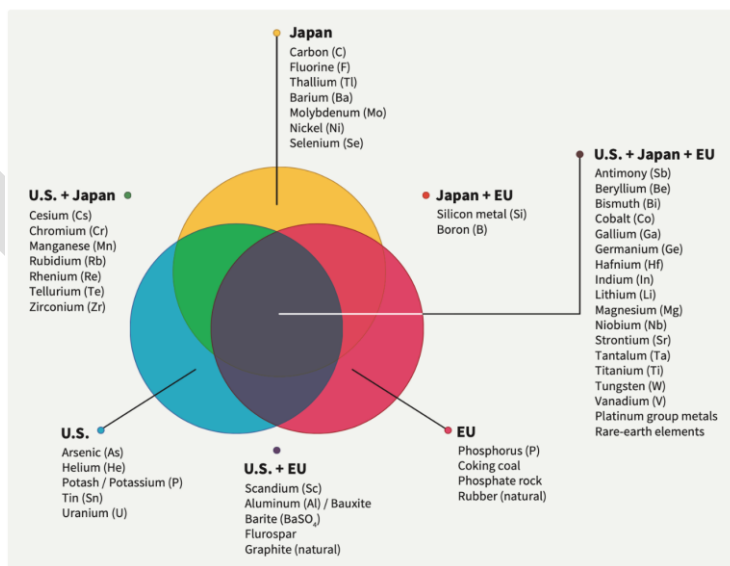

AUSTRALIA AND CHILE IN THE FRONT ROW
Countries with major Lithium production and reserves

	production (in 1,000t)	reserves (in 1,000t)
USA		35
Namibia	0.5	
Brazil	0.6	54
Portugal	0.8	60
Zimbabwe	1.6	70
Argentinia	6.2	2,000
China	8	1,000
Chile	16	8,000
Australia	51	2,700

source: USGS 2019

19.   Global supply, however, is limited and the geographical location of rare earth minerals does not necessarily favour Allied countries. "For example, about half the global supply of cobalt comes from the Democratic Republic of the Congo (DRC); over 80% of the global supply of lithium comes from Australia, Chile, and Argentina; and 60% of the global supply of manganese comes from South Africa, China, and Australia. Most notably, over 85% of the global supply of rare-earth elements comes from China" (Nakano, 2021). China controls a major part of the global supply chain for rare earths, encompassing production, extraction and refining. It thus poses a major challenge to the S&T resilience of Allied nations (Bonelli, 2021). Although less than China, Russia too constitutes a similar threat, as it disposes of 10% of the world's rare earth mineral reserves and is looking to increase its production to become self-sufficient and export some of its output, although it remains to be seen if it succeeds with this plan (Lyrchikova and Stolyarov, 2020).

4

Global Distribution of Rare Earth Elements

Source: USGS
Note: Top producers annotated

Copyright Stratfor 2019

20. Allies already pinpointed these vulnerabilities linked to rare earths back in 2010, when sanctions on rare earth trade were imposed by China on Japan as a retaliation against a territorial dispute (Nakano, 2021). Since then, the United States, the EU and Japan have developed "national and joint strategies to reduce Chinese dominance in this field" (Nakano, 2021), including the publication of several lists surveying critical raw materials for the future (European Commission, 2020). The US also published a similar list in 2018 (USGS, 2018) and initiated public-private partnerships to secure supplies. Europe, for instance, has set up projects such as the EURARE project and the European network of expertise on rare earths (ERECON) (Nakano, 2021). Allied nations should give higher priority to securing supply of rare earth minerals in their relationships with countries that mine rare earth minerals.

(Nakano, 2021)

21. Beyond competitor control, external supply shocks are also a risk that should be increasingly factored in. The COVID-19 pandemic showed how supply chains for raw materials could crumble: "the transport of cobalt produced in the Democratic Republic of the Congo was delayed in South Africa for months following the South African government's imposition of a strict lockdown in the second quarter of 2020" (Nakano, 2021). But more downstream goods that are crucial to S&T resilience can also be impacted. This is for instance the case with semiconductors, which have been recognised as crucial elements for technological sovereignty and national security (Csernatoni (a), 2021). Allies currently lack sufficient sovereignty over these critical components, which are the backbone of any ICT products: "Today, the US (Intel) competes in many parts of the advanced production processes, like chip design and fabrication. But the highest concentration of cutting-edge chips fabrication and assembly is in Asia, mostly in Taiwan (Taiwan Semiconductor Manufacturing Co – TSMC), then South Korea (Samsung Electronics), with Europe only a minor player" (Csernatoni (b), 2021).

C. CONTESTS AROUND NORMS AND STANDARDS

22. The introduction of new technologies, particularly disruptive ones, often raises important economic, societal and ethical questions. Technical standards have become critical to how technology shapes our societies (Park, 2022). Current developments in AI for national security for instance will have significant impact on international law. Russia, for instance, is contemplating the use of partly autonomous drones for its ongoing war in Ukraine (Knight, 2022). Easy solutions seem unlikely, as "the international environment is hardly conducive to discussions of how best to coordinate responses to the complex, cross-border dilemmas emerging around new technologies. In some corners, existing multilateral platforms are increasingly perceived as unsuitable for resolving these challenges" (Abendroth-Dias, 2020). Moreover, international rulemaking has a slow pace in contrast to the fast pace of innovation. In addition, the private sector is the main driver of technological change nowadays, which further separates the processes from the public debate and the needs of the public sector (Abendroth-Dias, 2020). It thus seems crucial to find better ways to co-decide what norms and ethics for science and technology should look like with a broader spectrum of actors, both internationally and across sectors.

23. Near-peer competitors, particularly the PRC, are investing considerable financial resources in developing military-related technologies and are in some areas catching up with the Allies. Regarding the development of Artificial Intelligence, for instance, China is rapidly closing the gap with the US and is surpassing EU countries (Castro & McLaughlin, 2021). The PRC is currently ranked second in the Tortoise Media's Global AI Index (Tortoise, 2022). Russia has much more limited means in this regard on the other hand and only ranks at 32 (Tortoise, 2022).

24. As countries compete for the development of new technologies, an emerging flashpoint is intellectual property (IP) policy. China has drastically increased its quantity of patent applications in fields such as AI, even surpassing the pace of countries with large innovative hubs such as the US (NSCAI, 2021). This bears the risk of hurting Allied innovators "by creating a vast reservoir of 'prior art' (the term in patent law for the worldwide scientific and technical knowledge by which an invention is evaluated to determine if it is new)", by increasing "the quantity of prior art that must be reviewed in examining a patent application" (NSCAI, 2021).

25. Furthermore, while Allied and like-minded nations firmly stand by the rule of law, near-peer competitors undercut the norms, laws and patents in S&T innovation. Russia, for instance, has announced that, as a response to the heavy sanctions against its illegal war in Ukraine, it would allow its businesses to steal technology regardless of existing patents (Knowles and Pozen, 2022).

26. Allies and like-minded states thus need to cooperate more on technology and norm and standard setting by forming coalitions. This would help to "promote the design, development, and

6

use of emerging technologies according to democratic norms and values; coordinate policies and investments to counter the malign use of these technologies by authoritarian regimes" (NSCAI, 2021). A first step was made in this direction with the organisation of a Pittsburgh EU-US Trade and Technology Council agenda in September 2021 (Csernatoni, 2021).

27.   This need is made more pressing as authoritarian countries already seek to undermine established norms borne out of the liberal international order. The trend of creating separate internets (dubbed "splinternet"), i.e. cutting networks off the open global internet, poses a threat to the free flow of information and interconnectivity of networks and systems (Park, 2022). This is not only inefficient but might also make it harder to monitor the state of human rights and promote open and free societies in the future.
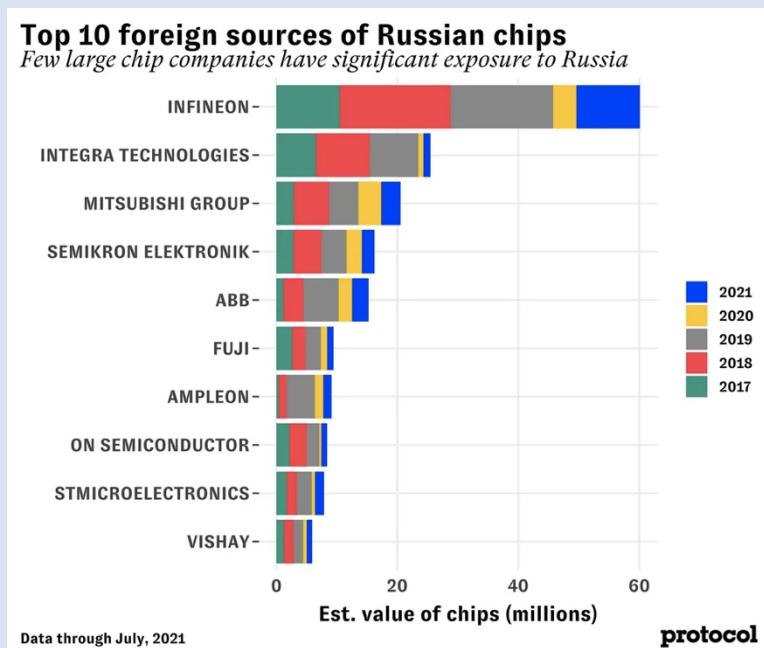

THE STATE OF S&T SECTORS FOR NATIONAL SECURITY IN RUSSIA & CHINA

Russia

Russia's S&T sector still strongly resembles the system inherited from the Soviet era. This has hampered the development of a more modern and agile innovation pipeline for the country (NATO ACT, 2021). As a result, Russia suffers from an ageing research infrastructure, outdated legal frameworks, insufficient state support and complete separation between R&D and the production side of the industry (NATO ACT, 2021). Many structural challenges are not addressed, such as a lack of funding and a continuing brain drain. These trends are bound to accelerate under the pressure of the current Western sanction regime imposed for Russia's war in Ukraine (Ivanova and Foy, 2022).

The defence industry remains the main driver of R&D in Russia, with about 30-40% of total R&D funding spent on military and defence projects. This greatly exceeds the equivalent figures in most Allied countries (2.8% in Germany, 6.4% in France). The military industry amounts to 70% of the high-tech output in the country and around half of the employed engineers (NATO ACT, 2021). This focus gives Russia some comparative advantages in certain very specific R&D sectors – such as hypersonics or narrow AI for military purposes – which it actively pursues. These innovations rest on a strong technological base built up over the last decades with products such as Russia's own positioning system GLONASS or a strong drone sector. Yet the overreliance on outdated legacy systems and the weak integration between the civilian and military R&D sectors pose long-term challenges (NATO ACT, 2021). The attempts to create "innovation hubs" modelled after the US's Silicon Valley have so far proved insufficient to overcome the lack of venture capitalism investments and maintain a steady pace of patent filings (NATO ACT, 2021).

Some of these shortcomings are most visible in the space industry, where endemic corruption has led to a chronic underfunding of research projects (Tangermann, 2022). Furthermore, due to increasingly limited access to crucial technology from the West – such as semiconductors – the Russian aerospace sector is likely to fall further behind. Due to sanctions, "Airports and seaports across the West are now closed to Russian commercial travel while imports of Korean "strategic items" as well as American computers, semiconductors, lasers, navigation and avionics – all vital components to Russia's space program – have been banned" (Tarantola, 2022). Since most semiconductor imports in Russia come from Western (or western aligned) countries (see below), the current disruptions caused by the sanctions will likely disrupt Russia's S&T sector for the short to mid-term.

Top 10 foreign sources of Russian chips
Few large chip companies have significant exposure to Russia

Legend:
- 2021 (blue)
- 2020 (yellow)
- 2019 (grey)
- 2018 (red)
- 2017 (green)

Companies (top to bottom): INFINEON, INTEGRA TECHNOLOGIES, MITSUBISHI GROUP, SEMIKRON ELEKTRONIK, ABB, FUJI, AMPLEON, ON SEMICONDUCTOR, STMICROELECTRONICS, VISHAY

X-axis: Est. value of chips (millions) — 0, 20, 40, 60

Data through July, 2021

protocol

(*Source:* Protocol, 2022)

China

China's roadmap for Science & Technology development is laid out in its 14th Five Year Plan (2021–2025). Technological innovation is one of the key ambitions of the Chinese Communist Party. China seeks to become world leader in Science and Technology by 2035 and aims to increase "research and development (R&D) spending by at least 7% annually between 2021 and 2025" (Sun and Cao, 2021). The current focus of the PRC's innovation activities is on robotics, new energy vehicles, aerospace, and agricultural machinery. The goal is self-reliance for its industrial sectors. (Sun and Cao, 2021) The "Made in China 2025" roadmap as well as the "Thousand Talents Plan" are further landmark documents setting out Beijing's S&T innovation ambitions (Wübbeke et al., 2016; Wong, 2022). The "Thousand Talents Plan" especially, with the aim to strengthen and broaden China's research base and S&T experts, has come under scrutiny in Allied countries for being linked to espionage cases (Rej, 2021).

China is in a favourable position industry-wise, in that is has been able to draw from its major influence on global overseas markets to enhance its geopolitical standing in the S&T sector. This has allowed it to catch up for some critical technology fields, partly by using unfair practices to force technology transfers. This is done for instance by tariffs, gatekeeping Western companies if they do not agree to share crucial information with the Chinese government, or through economic espionage (Wong, 2022). But China also draws resilience from a growing entrepreneurial spirit, as well as a "huge internal market of 1.4 billion people connected by well-developed transportation systems, advanced communication networks, and flexible and efficient supply chains" (Jun, 2021).

China's military and defence sectors benefit greatly from its technological innovation. Through its so-called "Military-Civil Fusion", the country aims to leverage effectively the duBoaral-use nature of new technologies by bringing the PRC's military closer to the academic and private sectors (Kahn, 2022). China wants to be a leader in AI by 2030 and to have modernised the People's Liberation Army by 2027. This entails the process of so-called "intelligentisation", meaning the implementation of concepts "of future warfare based on emerging and disruptive technologies, particularly AI and autonomous and unmanned systems" (Kahn, 2022).

Other priorities include "semiconductors and advanced computing, quantum, biotechnology, hypersonic and directed energy weapons and advanced materials and alternative energy" (Kahn, 2022). The PRC is committed to achieving these goals, as it has "increased its annual military budget by 6.8% in 2021 and is investing enormous resources into the research and development of emerging technologies" (Kahn, 2022). China is currently thus the most serious competitor to Allied nations in the S&T field. Yet it is still unclear how fruitful these investments will turn out to be in the mid- to long-term.

It seems likely that cooperation between Russia and China will deepen as a result of President Putin's war of choice against Ukraine. Increased cooperation between the two counties may also extend to the technology sector. However, whether increased cooperation in the S&T realm may pose a more serious threat to NATO's technology edge remains to be seen.

IV- EFFORTS TO STRENGTHEN S&T RESILIENCE IN THE ALLIANCE

A. A CHANGING INNOVATION LANDSCAPE

28.   The relation between industry and the defence sectors has drastically changed over the past decades. The pace, funding methods, geographical location and priorities of S&T research, innovation and development processes have evolved. It is essential for Allies to grasp fully these evolutions to adapt to these new realities and build a more resilient innovation pipeline.

29.   In the past, military R&D used to spearhead technological advances in the civil sector, generating important spin-offs for civilian use. In 1960, roughly every third dollar spent on R&D globally went into US defence projects (von Petersdorff, 2022). Silicon Valley was for a large part birthed out of the Pentagon's DARPA (Defense Advanced Research Projects Agency) money. Through contracts and direct research, the public sector, mostly through the U.S. Department of Defense, was driving innovation in the United States (Lewis (b), 2021). Major inventions that are the cornerstone of today's private tech sector, like the internet or AI, were derived from DOD-funded projects (von Petersdorff, 2022). The main R&D strategy then was to make "big bets" on certain key technologies and fund them with public money such as rockets, which led to space exploration (Lewis (b), 2021). The United Kingdom's Defence and Security Industrial Strategy aims to establish a more productive and strategic relationship between government and the defence and security industries. Total funding for defence related R&D for the 2021 to 2025 period amounts to at least £6.6 billion (UK MOD, 2021).

30.   But the drivers of research and technology have changed since the 1990s, recalibrating toward entrepreneurs and technology companies, which primarily focus on the more profitable commercial market (Lewis (b), 2021). This has obviously a profound impact on Allied military and defence innovation, as essentially the public sector has switched from the driver's seat to the passenger seat regarding innovation. This does not mean, however, that it has entirely lost the monopoly over some key strategic "bets" that are specific to defence needs, such as hypersonic missile technology or stealth technology.

31.   The bulk of technological advances is happening outside of government facilities. Some areas, like software, commercial space travel or quantum computing receive much more private than public funding (Lewis (b), 2021). Allies need to recognise those trends, harness them and adapt them to the needs of their military and defence sectors (Scharre and Riikonen, 2020). This is explained in large part by the fact that the "most dramatic changes in warfare in the coming

decades will come from huge leaps ahead in the information-centric capabilities of military systems" (Scharre and Riikonen, 2020). It is not as much about developing entirely new types of weapons systems and platforms separate from drones, tanks, and missiles but more about fine-tuning and making the existing ones smarter.

32.   Embracing the already vibrant start-up culture in Allied countries makes for a more open and diverse innovation model, which embraces disruption and incentivises fresh and plural thinking, thus making the pipeline more resilient over time (Murray, 2020).

33.   An entirely top-down state-driven approach to innovation is thus likely to yield subpar results. Even heavily government-driven economies like China recognise the pitfalls of being solely driven by political goals (Lewis (b), 2021). The public sector should not underestimate its role in driving fundamental research however, as the private sector can sometimes fall short in that regard. At the same time, it needs to find efficient ways to incentivise private companies to develop products suited for national security purposes in key areas and adapt existing technologies.

34.   Essentially, this means getting better at translating technology into dual-use cases, from the commercial to the military and vice-versa, which strengthens both sides for innovation. It also requires communicating the needs of the public sector clearly to the private sector and encouraging action regarding these needs. This requires the public sector to develop a deep understanding of the current state of the art and a deep connection with the S&T industry, in a similar fashion to what venture capital funds do (Lewis (b), 2021). Navigating public investments and the harnessing of private innovation efficiently should allow the public sector to save up on R&D costs overall. Successful public sector examples already exist, such as the US intelligence community's In-Q-Tel, or the French *Agence pour l'innovation de défense* (AID). NATO recently launched its own version of such an accelerator platform, in the form of the Defence Innovation Accelerator for the North Atlantic (DIANA).

35.   These fundamental changes in innovation culture in Allied countries need to be accompanied by a change of mindset. Adapting to the harnessing of innovation with and from the private sector also means developing a deeper culture of risk tolerance. Still today, roughly 90% of start-ups in the Silicon Valley fail (Sahin and Barker, 2021). These odds should be understood from day one by the public sector investors, while being cognisant of the fact that on the upside, working with the private sector also allows for a greater distribution of the risks among stakeholders. Young start-ups also do not function in the same way established defence industrial companies do: "If start-ups cannot close deals in a matter of weeks and months rather than quarters and years, then they would not attempt to (opportunity cost)." (Murray, 2020). This implies the need to re-evaluate the pace and logic of investments from the public sector into the private.

36.   Overall, states can envisage multi-tiered approaches to technology investments, where they simultaneously: (a) embrace the private sector's pace and methods for the adoption of new information technologies; (b) keep publicly investing in some key military-only technologies as previously (where the private sector can provide solutions only with difficulty, like optics or nuclear technology); and (c) allow themselves to place riskier "wild-card" bets, which could have revolutionary effects (Scharre and Riikonen, 2020).

37.   At the other end of the innovation pipeline lies yet another challenge that must be considered: the implementation of new technologies. An army can only profit from the development of the latest technology if it is implemented correctly, with the right doctrines and training for the personnel who supervise and use these technologies. "First adopter advantage for emerging disruptive tech could not be more prevalent in the world of geopolitics and deterrence. Indeed, the nations that win this race may be those with the most agile bureaucracy rather than those with the best technology" (Murray, 2020). The implementation of the F35 fighter jet for Norway for instance

led to a complete change in the military concepts for the Norwegian armed forces, as its functioning demands new methods (Størdal, 2022). Bureaucracy is a clear slowing factor in that regard. This is of particular importance for the implementation of very technical aspects to warfighting, like AI, which will require a tremendous effort in training so that personnel of all ranks are well suited to understand the implications and concepts regarding the use of these technologies. In 2018, the Defense Innovation Board of the US Department of Defense wrote in a report that "the Department of Defence 'does not have an innovation problem; it has an innovation adoption problem'", something any defence bureaucracy should be mindful of (Imbrie, 2019).

B. NATO's ADAPTION TO A NEW INNOVATION ECOSYSTEM

38.   Defence innovation is crucial to maintain NATO's technological edge. Since 2018, the Alliance has stepped up its efforts regarding EDTs. The Emerging and Disruptive Technologies Roadmap identified seven critical technologies: AI and machine learning; big data; autonomy; hypersonics; space technologies; quantum computing; and biotechnologies (Soare, 2021). In 2021, Allies decided to add "Energy and Propulsion" as well as "Novel Materials and Advanced Manufacturing" to this list of relevant technologies. NATO's Innovation initiatives are coordinated by the Innovation Board, which is chaired by the Deputy Secretary General. Moreover, the NATO 2030 process translates the effort to "future proof" the Alliance regarding technological competition (Soare, 2021). Under NATO 2030, Allies agreed on the establishment of a NATO Innovation Fund and DIANA, NATO's Defence Innovation Accelerator for the North Atlantic, which was launched in April 2022 (NATO (a), 2022).

39.   DIANA is a new NATO body which will be jointly funded by all Allies and will have its separate governance and funding mechanisms, which equip it with a high degree of freedom of operation and agility (Zimmermann, 2022). It will run numerous test centres and accelerators across the Alliance, as shown below.
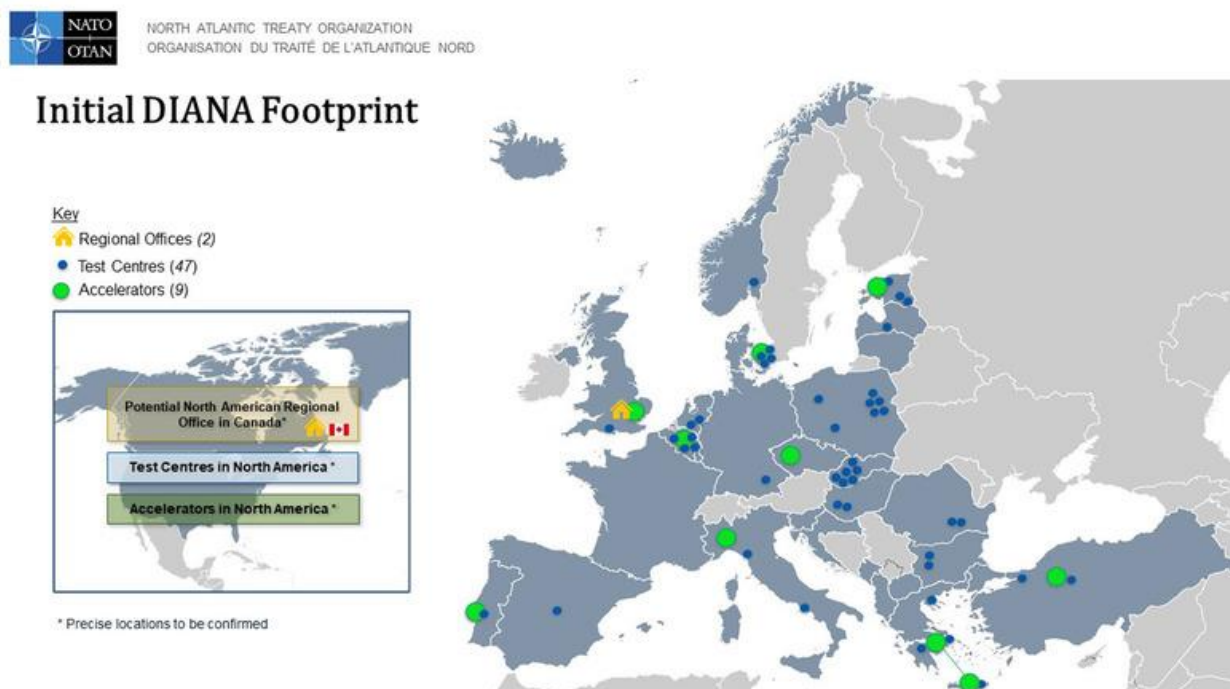
(NATO (a), 2022)

40.   DIANA closes a gap in NATO's outreach to the private sector, specifically start-ups. While both the STO and ACT also engage with the private sector, they are generally more concerned with very early stages of research and development processes (for the STO) or later stages (implementation for ACT). DIANA's strength will lie in the fact that it covers the middle ground, where start-ups and defence companies take findings from fundamental research and turn them into actual products (Zimmermann, 2022).

41.   The focus on EDTs is geared towards fostering the interoperability of military capabilities across the Atlantic, through "streamlining standardization and testing, evaluation, verification, and validation procedures" (Soare, 2021). Nascent projects like DIANA are a further step in this direction, yet the Advisory Group on Emerging and Disruptive Technologies and the NATO 2030 Reflection Group have also advocated for more possible measures in the future, such as establishing a similar NATO Advanced Technology Projects Agency or a NATO Investment Bank (Soare, 2021).

42.   Under NATO 2030, Allies also launched a EUR€1 billion NATO Innovation Fund. Backed by NATO Allies, this deep-tech venture capital fund will provide strategic investments into start-ups developing cutting-edge technological solutions, leveraging the enormous potential for commercial innovation to address critical defence and security challenges.

43.   NATO plays an important role in addressing the "fragmentation of researchers, academia, start-ups and government at the beginning" of the innovation pipeline (described in the previous sub-chapter) and its capacity to adopt quickly new technologies (Murray, 2020). In 2022, for instance, NATO launched "PROJECT X" in cooperation with Dutch universities to see how students and researchers can collaborate regarding rapid-prototyping initiatives for NATO's innovation pipeline (NATO (b), 2022).

44.   Pooling and sharing knowledge across the Alliance have a particularly positive effect on Allies with a smaller innovation sector, as they can concentrate on niche areas. Poland's biggest export partner for some critical technologies for defence is the US for instance, which would not have been possible without NATO's innovation ecosystem (Størdal, 2022). This fosters resilience, as it also helps build a more tight-knit Alliance that can focus on being less dependent on imports from competitors (Zimmermann, 2022).

45.   An area where further progress is possible is NATO-EU cooperation in the S&T realm. Both the EU and NATO have been evolving quickly in the past years regarding their understanding and policies towards EDTs. Yet there are still fundamental disconnects in which technology policy are envisioned on both sides of the Atlantic (Clüver Ashbrook and Sanger, 2021). In very general terms, European nations tend to emphasise the need to establish legal frameworks for EDTs and the companies developing these, while the United States focuses on developing the technologies. These disconnects will have to be addressed by NATO and the EU. On tech policy, the EU has concentrated on platform regulation issues, whereas the US have been mostly focused on countering China's influence in technology (Clüver Ashbrook and Sanger, 2021).

46.   While a seamless digital transatlantic integration is unlikely (Lewis (a), 2021), the inclusion of Microsoft in Europe's GAIA-X project (a European for Europeans cloud-based data storage) is an encouraging step towards more transatlantic cooperation in this regard (Clüver Ashbrook and Sanger, 2021). Projects like the EU's "Innovation Union", Horizon Europe and its earlier iteration Horizon 2020 have the capacity to enhance greatly R&D processes across the European continent. Horizon Europe allocates a budget of €95 billion to R&D over a span of seven years (Lewis (a), 2021). The European Defence Fund is another crucial European project for defence-

related R&D, with a budget of roughly €8 billion (Csernatoni (c), 2021). Enhancing Europe's technological "open strategic autonomy" – as framed in the EU's industrial strategy (Lewis (a), 2021) – is therefore not antithetical to strengthening NATO. Indeed, "technology plays a fundamental role in terms of making possible the EU's hard military power ambitions—not only to act in a tense geopolitical setting but also to defend the EU's interests in areas related to technology, security, and defence matters", such as "cybersecurity, drones, secure networks, space technologies, artificial intelligence (AI), and quantum technology" (Csernatoni (c), 2021).

47.   Allies need to deepen their common understanding of relevant technological developments and their security and economic implications. More cooperation among Allies can help protect their technology bases and improve their performance. This applies to space technology, among others. Space is a critical enabler of security and defence. According to the UK think tank "Policy Exchange", it is essential to safeguard Allies' space-industrial competitiveness as this critical industry will undergo consolidation, as fewer large-scale players will dominate this sector in the future. More particularly, NATO Allies must prevent a Huawei-type situation, i.e. a situation where critical parts of its space technology could be controlled by foreign-backed companies.

48.   NATO Allies need to respond to Beijing's aggressive build-up in global tech markets, including key space sectors, by developing viable Western alternatives to Chinese players (Sheldon, 2021). In addition, NATO could improve the sector's resilience through competition and industrial cooperation among Allies and like-minded partners. The "enhanced trilateral security partnership" between Australia, the United Kingdom and the United States (AUKUS) can generate additional momentum in this regard. Although it currently focuses on nuclear propulsion, artificial intelligence and quantum technologies, it should be expanded to include strategic space technology cooperation (Sheldon, 2021).

49.   "Innovation requires open networks, unlike the twentieth century industrial base, which was closely tied to physical infrastructure such as steel mills or coal mines" (Lewis (a), 2021). Potential future avenues for cooperation include AI ethics, foreign investment screenings and technology transfer rules (such as the Wassenaar Arrangement) (Lewis (a), 2021). First and foremost, more consultations should be sought for NATO specifically, as the EU and NATO have consulted on their respective EDTs agendas only twice (Soare, 2021).

V- PRELIMINARY CONCLUSIONS

50.   Maintaining and further developing NATO's technological edge will be pivotal to the Alliance's future. Ensuring the resilience of NATO's S&T sectors is an essential element in our ability to deter and defend ourselves.

51.   Near-peer competitors are actively trying to undermine NATO's S&T resilience. At the same time, the Alliance has to succeed in carefully making a transition to the 21st century playbook of how innovation works. This will require a successful launch of new projects like DIANA and a deeper symbiosis with key partners such as the EU.

52.   More specifically, the Allies need to:

- Maintain a focus on NATO's technological edge. A strong understanding for just how important technology will be to the Alliance is emerging. Yet this is only the first step, which must be followed by successful implementation and adoption of new technologies, as stressed throughout this report. For the organisation specifically, it will

13

have to make sure NATO's DIANA is fine-tuned, for instance, to function in strong synergy with the STO and ACT.

- Increase investment in critical technologies, particularly in cybersecurity, maritime technology and satellite technology to prevent potential adversaries gaining an edge in these areas. Allies also should deepen cooperation amongst themselves and with like-minded partner nations in this field.

- Continue enhancing and deepening NATO's digitisation processes. This does not only require more secure networks, but also more qualified personnel with STEM skills, who are able to grasp, oversee, manipulate and fix the increasingly digital assets required to operate armed forces and organisations such as NATO. Allies need to ensure they incentivise the recruitment and education of future STEM talents.

- Deepen their understanding of the implications of a further decoupling of global supply chains, economies and innovation systems, both in their positive aspects (i.e. facing less pressure from potential leverage near-peer competitors might have over Allies) and negative ones (i.e. losing an open system). This also entails identifying critical supply chains and seeing if and how NATO can protect them.

- Increase awareness of NATO militaries' dependency on foreign producers of defence-related equipment and components. Allies should also monitor and improve supply-chain security for critical components and materials. More particularly, Allies need to develop strategies to mitigate China's dominance over rare earth minerals.

- Strengthen their common understanding of ethical standards for EDTs, which can then form the basis for a common ground for international legal frameworks and strengthen interoperability through a shared vision of how military concepts should evolve.

- Enhance inter-institutional and international cooperation on EDTs, for instance through a deepened dialogue with the EU and other international partners such as Asia-Pacific democracies.

BIBLIOGRAPHY

Abendroth-Dias, Kulani, "What Does Resilience-Building to Emerging and Disruptive Technologies Actually Look Like? A Study Addressing the Public Policy Challenges and Socio-Political Implications of the Development of Artificial Intelligence for NATO Security and Defense in Continental Europe", NATO STO, 2020, https://www.sto.nato.int/publications/STO Meeting Proceedings/STO-MP-SAS-OCS-ORA-2020/MP-SAS-OCS-ORA-2020-EDT-01-2.pdf

Adger, W. Neil et al., "Urbanization, Migration, and Adaptation to Climate Change", One Earth, Vol. 3, No. 4, October 2020, https://www.sciencedirect.com/science/article/pii/S2590332220304851

Aronhime, Lawrence and Cocron, Alexander, "NATO's Innovation Challenge, NATO Review, 19 July 2021, https://www.nato.int/docu/review/articles/2021/07/19/natos-innovation-challenge/index.html

Bing, Christopher and Taylor, Marisa, "China-backed hackers 'targeted COVID-19 vaccine firm Moderna", Reuters, 30 July 2020, https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M

Bonelli, Andrea, "China's Rare-Earth Dominance Is a Security Risk for NATO and Western Supply-Chain Resilience", ICDS, 22 September 2021, https://icds.ee/en/chinas-rare-earth-dominance-is-a-security-risk-for-nato-and-western-supply-chain-resilience/

Buckley, Chris and Mozur, Paul, "How China Uses High-Tech Surveillance to Subdue Minorities", New York Times, 22 May 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Cadell, Cate, "From laboratory in far west, China's surveillance state spreads quietly", Reuters, 14 August 2018, https://www.reuters.com/article/us-china-monitoring-insight-idUSKBN1KZ0R3

Castro, Daniel and McLaughlin, Michael, "Who Is Winning the AI Race: China, the EU, or the United States? — 2021 Update", Center for Data Innovation, 25 January 2021, https://datainnovation.org/2021/01/who-is-winning-the-ai-race-china-the-eu-or-the-united-states-2021-update/.

Clüver Ashbrook, Cathryn and Sanger, David, "Technology: Transatlantic Action Plan", DGAP, 24 February 2021, https://dgap.org/en/research/publications/technology

Csernatoni, Raluca (a), "Chips geopolitics and EU's new semiconductors sovereignty agenda", Euractiv, 29 October 2021, https://www.euractiv.com/section/digital/opinion/chips-geopolitics-and-eus-new-semiconductors-sovereignty-agenda/

Csernatoni, Raluca (b), "The EU needs to reconcile its quest for technological sovereignty with a commitment to strategic openness and international cooperation", CEPA, 4 November 2021, https://cepa.org/chasing-chips-a-geopolitical-puzzle/

Csernatoni, Raluca (c), "The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty", Carnegie Endowment for International Peace, 12 August 2021, https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134

European Commission, "Critical raw materials", European Commission, https://ec.europa.eu/growth/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en

Gady, Franz-Stefan, "New Snowden Documents Reveal Chinese Behind F-35 Hack", The Diplomat, 27 January 2015, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack

Gilli, Andrea and Gilli, Mauro, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage", International Security 43 (3), 2019, https://direct.mit.edu/isec/article/43/3/141/12218/Why-China-Has-Not-Caught-Up-Yet-Military

PRELIMINARY DRAFT REPORT – 023 STC 22 E

Gilli, Andrea and Bechis, Francesco, "NATO and the 5G challenge", NATO Review, 30 September 2020, https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html

Hannas, William C. and Tatlow, Didi Kirsten, *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2021

Imbrie, Andrew, "Artificial Intelligence meets bureaucratic politics", War on the Rocks, 1 August 2019, https://warontherocks.com/2019/08/artificial-intelligence-meets-bureaucratic-politics/

Ivanova, Polina and Foy, Henry, "Russia's techies flee country they fear is 'flying into an abyss'", Financial Times, 9 March 2022, https://www.ft.com/content/a8b53d7a-08c5-484e-9dc6-cd4b2d889e3f

Jun, Zhang, "The Neglected Sources of China's Economic Resilience", Project Syndicate, 4 October 2021, https://www.project-syndicate.org/commentary/china-economic-resilience-still-strong-by-zhang-jun-2021-10

Kahn, Lauren, "What the Defense Department's 2021 China Military Power Report Tells Us about Defense Innovation", Lawfare, 15 February 2022, https://www.lawfareblog.com/what-defense-departments-2021-china-military-power-report-tells-us-about-defense-innovation

Kavanagh, Camino, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?", Carnegie Endowment for International Peace, 28 August 2019, https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736

Knight, Will, "Russia's Killer Drone in Ukraine Raises Fears about AI in Warfare", Wired, 17 March 2022, https://www.wired.com/story/ai-drones-russia-ukraine/

Knowles, Hannah and Pozen, Zina, "Russia says its businesses can steal patents from anyone in 'unfriendly' countries", The Washington Post, 9 March 2022, https://www.washingtonpost.com/business/2022/03/09/russia-allows-patent-theft/

Levy, Jaclyn, "The Best Defense: Why NATO Should Invest in Resilience", Atlantic Council, 10 June 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-best-defense-why-nato-should-invest-in-resilience/

Lewis, James Andrew (a), "Charting a New 'Digital Atlantic'", CSIS, 9 June 2021, https://www.csis.org/analysis/charting-new-digital-atlantic

Lewis, James Andrew (b), "Linking National Security and Innovation: Part 1", CSIS, 7 April 2021, https://www.csis.org/analysis/linking-national-security-and-innovation-part-1

Lyrchikova, Anastasia and Stolyarov, Gleb, "Russia has $1.5 billion plan to dent China's rare earth dominance", Reuters, 12 August 2020, https://www.reuters.com/article/russia-rareearths-idUSL8N2F73F4

Mattis, Peter, "A Guide to Chinese Intelligence Operations". War on the Rocks, 18 August 2015, https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/

Murray, Rob, "Building a resilient innovation pipeline for the Alliance", NATO Review, 1 September 2020, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html

Nakano, Jane, "The Geopolitics of Critical Minerals Supply Chains". CSIS, 11 March 2021, https://www.csis.org/analysis/geopolitics-critical-minerals-supply-chains

NATO (a), "NATO sharpens technological edge with innovation initiatives", NATO, 7 April 2022, https://www.nato.int/cps/en/natohq/news_194587.htm

NATO (b), "PROJECT X empowers young innovators to build technologies for the future", NATO, 31 January 2022, https://www.nato.int/cps/en/natohq/news_191406.htm?selectedLocale=en

NATO, 'Strengthened Resilience Commitment', NATO, 14 June 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO, "Commitment to Enhance Resilience: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016', NATO, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm

NATO ACT, 'Regional Perspectives Report on Russia. Strategic Foresight Analysis', NATO, 2021, https://www.act.nato.int/application/files/9816/1350/4281/regional-perspectives-2021-01.pdf

PRELIMINARY DRAFT REPORT – 023 STC 22 E

NATO STO, "About the STO", NATO, https://www.sto.nato.int/Pages/organization.aspx

NSCAI, "The Final Report", National Security Commission on Artificial Intelligence, 2021, https://www.nscai.gov/2021-final-report/

Park, Joshua, "Breaking the Internet: China-US Competition over Technology Standards", The Diplomat, 9 February 2022, https://thediplomat.com/2022/02/breaking-the-internet-china-us-competition-over-technology-standards/

Pauwels, Eleonore, "The Road Towards Cyber-Sovereignty Passes Through Africa", *Konrad Adenauer Stiftung*, 9 December 2019, https://www.kas.de/fr/laenderberichte/detail/-/content/the-road-towards-cyber-sovereignty-passes-through-africa

Protocol, "Where Russia gets its chips", Protocol, 3 March 2022, https://www.protocol.com/newsletters/protocol-enterprise/russia-ukraine-chips-shields-up?rebelltitem=7#rebelltitem7

Rasser, Martijn, et al., "Common Code: An Alliance Framework for Democratic Technology Policy", CNAS, 21 October 2020, https://www.cnas.org/publications/reports/common-code

Rej, Abhijnan, "US Justice Department Pushes Ahead with Counter China Plan", The Diplomat, 16 January 2021, https://thediplomat.com/2021/01/us-justice-department-pushes-ahead-with-counter-china-plan/

Richiello, Angelo, "The geopolitics of rare earths: how to counter China's dominance", Aspenia Online, 29 April 2021, https://aspeniaonline.it/the-geopolitics-of-rare-earths-how-to-counter-chinas-dominance/

Roepke, Wolf-Dieter and Thankey, Hasit, "Resilience: The First Line of Defence", NATO Review, 27 February 2019, www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

Sahin, Kaan and Barker, Tyson, "Europe's Capacity to Act in the Global Tech Race", DGAP, 22 April 2021, https://dgap.org/en/research/publications/europes-capacity-act-global-tech-race

Scharre, Paul and Riikonen, Ainikki, "Defense Technology Strategy", CNAS, 17 November 2020, https://www.cnas.org/publications/reports/defense-technology-strategy

Sheldon, John B., "Britain and the Geopolitics of Space Technology", Policy Exchange, 5 November 2021, https://policyexchange.org.uk/publication/britain-and-the-geopolitics-of-space-technology/

Soare, Simona R., "Innovation as Adaptation: NATO and Emerging Technologies" The German Marshall Fund of the United States, 11 June 2011, https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies

Størdal, John-Mikal, Director, NATO Collaboration Support Office, interview conducted 9 March 2022

Sun, Yutao &and Cao, Cong, "China's plan to become a world-leading technology force", East Asia Forum, 8 May 2021, https://www.eastasiaforum.org/2021/05/08/chinas-plan-to-become-a-world-leading-technology-force/

Tangermann, Victor, "Bumbling Russian Space Boss forced to slash huge raise he gave himself", Futurism, 4 March 2022, https://futurism.com/the-byte/dmitry-rogozin-pay-cut

Tarantola, A., "What economic sanctions mean for Russia's space program", Engadget, 2 March 2022, https://www.engadget.com/what-economic-sanctions-mean-for-russias-space-program-170003960.html

Tarry, Sarah, "How Does NATO Support Allies' Resilience and Preparedness?", NATO, 8 June 2021, https://www.nato.int/cps/en/natohq/news_184730.htm

Tortoise Media, 'The Global AI Index', Tortoise Media, https://www.tortoisemedia.com/intelligence/global-ai/

USGS, "Interior Releases 2018's Final list of Critical Minerals", USGS, 18 May 2018, https://www.usgs.gov/news/national-news-release/interior-releases-2018s-final-list-35-minerals-deemed-critical-us

United Kingdom Ministry of Defence, "Defence and Security Industrial Strategy", UK Ministry of Defence, 26 March 2021, https://www.gov.uk/government/publications/defence-and-security-industrial-strategy/defence-and-security-industrial-strategy-accessible-version

Von Petersdorff, Winand, "*Was die technologische Aufrüstung bedroht*", *Frankfurter Allgemeine Zeitung*, 21 March 2022, https://www.faz.net/aktuell/wirtschaft/digitec/usa-was-die-technologische-aufruestung-des-us-militaers-bedroht-17892378.html

Wong, Pak Nung, *Techno-Geopolitics. US-China Tech War and the Practice of Digital Statecraft*, Routledge, 2022

Wübbeke, Jost et al., "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries", Mercator Institute for China Studies, 2 December 2016, https://merics.org/sites/default/files/2020-04/Made%20in%20China%202025.pdf

Yang, Yuan, "Is Huawei compelled by Chinese law to help with espionage?", Financial Times, 5 March 2019, https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0

Young, Leslie. "NATO chief warns of threat of industrial espionage from other nations", Global News Canada, 16 July 2019, https://globalnews.ca/news/5496343/nato-industrial-espionage/

Zimmermann, Moritz, Innovation Officer, NATO Innovation Unit, interview conducted 14 April 2022