NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

ECONOMICS AND SECURITY COMMITTEE (ESC)

PRELIMINARY DRAFT

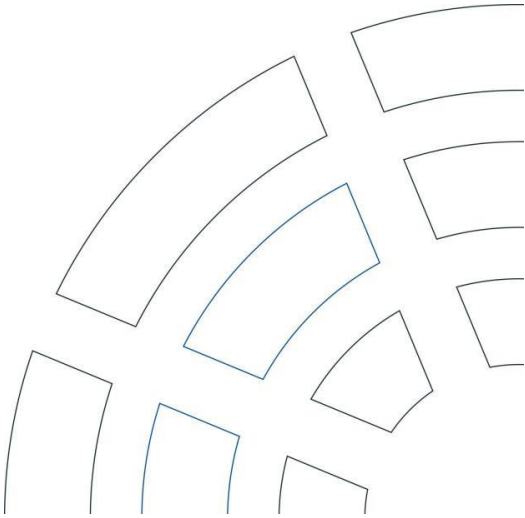
CRITICAL DUAL-USE TECHNOLOGIES: COMMERCIAL, REGULATORY, SOCIETAL, AND NATIONAL SECURITY CHALLENGES

Preliminary Draft General Report

Harriett Baldwin (United Kingdom)
Rapporteur

051 ESC 24 E – Original: English – 14 March 2024

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This working document only represents the views of the Rapporteur until it has been adopted by the Economics and Security Committee. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.



EXECUTIVE SUMMARY

The defence industry long functioned as a critical engine of technological innovation and often "spun off" technologies it developed into the commercial realm. Today the reverse is increasingly the case. Militaries increasingly depend on technologies developed initially for commercial markets and then spun into the defence sector. Commercially developed emerging technologies hold enormous potential for armed forces even when not originally developed for them. These technologies not only bolster the lethality of defence platforms but can also increase the efficiency of defence spending. When the private sector initially funds technology development for commercial markets, it covers a significant part of the initial development costs. Scale economies from commercial sales also drive down unit costs. Those countries that develop, commercialise, and integrate these technologies into products national militaries need stand to derive compelling economic, and strategic advantages.

China possesses considerable economic and technological capacities that have generated mounting concern. Beijing has a demonstrated the ability to leverage its commercial power and technological prowess to achieve its strategic objectives. Reducing its reliance on Western technology represents one of Beijing's most fundamental ambitions. Beijing, however, confronts considerable barriers to achieving its goals, and Western capacities to outpace China on the technology front remain considerable. China seeks shortcuts and uses espionage and intellectual property theft to keep pace with the West. Allied governments and partners have had to redouble efforts to restrict Chinese access to a range of sensitive technologies. For its part, Russia is currently engaged in widespread export control evasion and sanctions circumvention and continues to acquire restricted Western technologies needed to run its war on Ukraine and develop its energy sector.

NATO allies and partners need to impose tighter export controls, more funding for enforcement of restrictions, enhanced counter espionage efforts, and, in some cases, secondary sanctions to maintain strategic technology-capability advantages over competitor nations. Allies are working both to strengthen technology export controls and address a range of critical supply chain vulnerabilities that leave members vulnerable to economic coercion. But they also need to maintain their technological lead. NATO's DIANA program demonstrates that the Alliance sees technology innovation as fundamental to security and a focused supplement to national technological development. Artificial intelligence will become a critical agent for speeding the pace of technological advance, and this is precisely why NATO allies must sustain coherent and well-funded innovation programs in partnership with the private sector and universities to put all allies into a better position to exploit the commercial and strategic advantages technology confers.

TABLE OF CONTENTS

I- MANAGING THE PARADOX OF A TECHNOLOGICAL COLD WAR IN A GLOBALLY INTEGRATED ECONOMY

1. The global economy is undergoing fundamental change because of exponential development of technologies such as artificial intelligence (AI), quantum computing and extraordinarily advanced communication systems linked to ever denser satellite grids. Military planners have been compelled to incorporate these very same technologies into national arsenals and, by extension, into the tactics and strategies that these technologies facilitate. As these very same technologies become available to strategic competitors and even to malicious non-state actors, it has become equally important to plan how to best defend against them.

2. The explosion of digital electronics has also precipitated something of a military-industrial paradigm change. Whereas defence industries had traditionally functioned as a great engine of technological innovation and tended to "spin off" non-lethal technologies into the commercial realm, today the reverse is increasingly the case. High technology firms engaged in commercial product development are producing technologies that are subsequently discovered to have compelling and even game-changing military applications because of their potential as powerful force multipliers. Militaries thus increasingly rely on technologies originally conceived for purely commercial purposes that rapidly spin into the military realm once their military applications become evident.

3. Dual use technologies hold great potential for armed forces. They can increase the efficiency and cost effectiveness of defence spending. Implicit savings to defence budgets become possible simply because much of the research and development costs have already been covered during the initial commercial development phase. This, in turn, slashes development costs and shortens development timelines for the military applications while delivering new and powerful capabilities quickly to forces in the field. Moreover, because these technologies are developed for commercial markets, scale economies help drive down unit costs. In an era of tight national budgets and mounting strategic threat, these new commercial-defence market links promise to restructure some of the central patterns of defence systems development and procurement (Kissinger, 2023). The commercial market has been the primary driver of a technology revolution which has produced an array of innovations with important military applications. Drones, for example, were originally developed as children's toys. Their military use became apparent when an Israeli inventor placed a camera on one. As the war in Ukraine has so clearly demonstrated, drones now play a central role in battlefield management, intelligence gathering and as a key offensive and defensive military platform. Mobile phones developed for commercial markets have helped transform military communications. Ongoing commercial developments in areas like quantum computing, artificial intelligence and novel materials are all seen as having direct implications for future military systems.

4. The stakes in the emerging race to develop, commercialise and integrate these technologies into national militaries are thus extraordinarily high. The 2022 National Defense Strategy (NDS) of the United States stated that the U.S. Department of Defense (DoD) cannot ignore that market forces are driving new capabilities that could prove useful, particularly considering mounting strategic competition with China at the high end of the capability spectrum. "To gain and maintain operational advantage over competitors, the DOD requires an order of magnitude increase in its adoption of commercial technologies. To this end, DOD must act as a fast follower." The DoD's Defense Innovation Unit is accordingly working to identify emerging technologies developed in the commercial sector for potential use to the military (Vergun, 2023).

5. National military establishments have long been a factor in technological advance and continue to play a significant role in this regard even as technology developed for commercial markets is of increasing importance to military planners. The U.S. Department of Defense recently identified thirteen technologies for priority development. Interestingly, most of those technologies are also

driving foundational change in commercial markets: biotechnology, quantum science, future generation wireless technology, advanced materials, trusted AI and autonomy, integrated network systems-of-systems, microelectronics, space technology, renewable energy generation and storage, advanced computing and software, and human-machine interfaces. It has also identified three priority areas of technology development that are primarily defence-related: directed energy weapons, hypersonics, and integrated sensing and cyber defence (The Under Secretary of Defense for Research and Engineering website). Not surprisingly, NATO's own list of emerging and disruptive technologies largely overlaps those of the DoD and includes artificial intelligence, data, autonomy, quantum-enabled technologies, biotechnology, hypersonic technologies, space, novel materials and manufacturing, and energy and propulsion (Ricart, 2023).

6. Space represents another area where the commercial-state roles seems to be switching. Over decades, the US space programme nurtured a network of companies that developed technologies needed by that program. This need for advanced computing and smaller electronics for space flight contributed to significant advances in a range of fields from computers to advanced materials. Satellites, which were essentially built by governments for military surveillance and reconnaissance, ultimately enabled global telecommunications and GPS technologies. Today, private firms are no longer simply operating as contractors to nation states but are themselves becoming key protagonists in space. As a result, developments in the commercial market are spinning into the military realm (Bockel, 2018). Even though the 1967 Outer Space Treaty bans the stationing of weapons of mass destruction (WMD) in outer space, prohibits military activities on celestial bodies, and details legally binding rules governing the peaceful exploration and use of space. Space represents a domain where commercial technologies have direct military applications. NATO Secretary General Stoltenberg noted that "What happens in space is of great importance for what we can do on the Earth: communications, navigation, cell phones, military communications, transmission of data and a lot of activities on the Earth, at sea and on land, is dependent on capabilities in space, not least satellites. So, this is important for our civilian societies, but also, of course, for military capabilities." (Brunner, 2021). It is noteworthy in this regard that a commercial satellite system, Starlink, has played a pivotal role in Ukrainian battlefield communications and, among other things, helped guide Ukraine's drone strikes on Russian tanks and positions. Analysts would suggest that those countries that master these technologies and their commercial and military applications will dominate the international system both in military and economic terms for the coming decades while those failing to do so will find themselves increasingly marginalised and even threatened (Lee, 2023).

II- DIVERGENT MODELS OF TECHNLOGY DEVELOPMENT

7. Every country innovates in unique ways, and the state's role varies simply because the lines between state and market differ even among free market democracies. It is often presumed, for example, that the United States represents the apotheosis of laissez faire capitalism; yet many of the cutting-edge US-generated technologies that dominate today's global market, are, to varying extents, also the product of US government support for basic and applied research, for example, through grants underwriting university research and DoD funding to develop advanced military systems. The same is certainly the case for Europe although the relationship between universities, market players and the state can differ by country.

8. A key challenge allies confront today is how best to exercise regulatory and trade controls over sensitive dual use technologies. Governments need to incentivise private sector actors not only to accept technology transfer restrictions but also to effectively enforce these export boundaries. On the face of it, this implies greater costs to the private sector. But efforts to restrict access to these technologies can also benefit commercial operators. For example, reducing technology theft is in the

direct interest both of the owners of intellectual property and of governments focused on ensuring national security. However, states and companies can come to loggerheads on these matters and there is ample room to improve government-market cooperation to ensure that strategic competitors are denied easy access to militarily relevant technologies.

9. Despite the challenges Allies confront in this burgeoning technological race, they also enjoy important advantages. The United States, for example, has some of the world's leading universities conducting innovative research funded both by the government and the private sector. These universities have forged unique ties with the commercial sector, and it is no coincidence that three vital US technological hubs – the greater San Francisco Bay area in California; Boston, Massachusetts; and Austin, Texas are also home to leading global universities. Those schools are infused with a spirit of liberal inquiry that no authoritarian country can recreate simply because the very notion of free thought is antithetical to their core ideology. This phenomenon is apparent across a range of allied countries' universities, including the University of Leuven, the University of Erlangen Nuremberg, Imperial College London, Cambridge University, University College London, the Technical University of Munich, and the University of Manchester, all of which a study by Reuters listed as among the ten top rated patent-producing universities in Europe (Ewalt, 2019).

10. The digital revolution in the West has not been a top-down affair but rather a decentralised process that states have nonetheless facilitated. The approach has generally combined competition and cooperation across a broad range of institutions and actors. The openness, the rule of law and the intellectual property protections legal systems provide have allowed this process to flourish in the West and conferred important advantages to Allied societies in the arena of technology development. It should hardly be surprising that Western societies have made many of the great advances across an array of cutting-edge technologies, although China has begun to make important inroads.

11. Europe is also an extraordinarily important generator of technology. Again, the model differs somewhat by country and, of course, different countries on the continent have different comparative advantages just as different regions of the United States take the lead on different kinds of technological advance. State-market balances also differ by country. Economic and political history, the nature and targeted end use of the technology, the dynamics of international competition, and the existing and historic industrial base all condition the role played by the state in developing technology. The European Union, which fosters cross inter-state coordination among its members and helps ensure the kind of market depth that a Europe of nation states alone could not generate, supplements the role of national states. The EU also provides a degree of strategic funding and direction to the process through programs like the Digital Europe Programme which funds research for supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring the wide use of digital technologies across the economy and society. In February 2023, the United Kingdom created a new Department for Science, Innovation & Technology to address the opportunities and challenges brought by rapid technological change. It recognises that technology is a national asset that is fundamental to the country's economic future and its security, and notes that it must work with allies and partners to ensure global technology standards are shaped by the democratic community of nations (UK Department for Science, Innovation & Technology, 2023).

12. The template differs for less developed countries without important technology development capacities. These countries generally need to import rather than develop sophisticated weapons or the technologies that make weapons more accurate and impactful on the battlefield and enhance communications and intelligence capabilities. When export controls or sanctions limit access to this technology, countries that do not subscribe to international intellectual property rules like Russia and China have resorted to theft to acquire these key technologies. In addition, where there are international bodies like the International Telecommunications Union, the United Nation's specialised agency for information and communication technologies, it is vital that NATO member states aim to get their nominees elected to key positions.

13. China, far more than Russia, is an increasingly important technology incubator and so the long-term challenge it poses in this field is more substantial that that posed by Russia. In any case, however they acquire the technology, authoritarian countries are now deploying it within their military and security arsenals not only to enhance military capabilities but also to reap economic benefits through foreign sales. They are also unearthing ways to use these systems to erode basic human and political rights in their own societies. Finally, authoritarian technology leaders like China are now selling these technologies to like-minded regimes sharing their anti-democratic ambitions (Kelley, 2023). This poses a growing military, political, and commercial challenge to allied democracies.

III- THE CHINA CHALLENGE

14. The greatest current challenge to the West on the geostrategic-technology front is China. This is not simply because it rejects the democratic principles and the rules-based order that animates governance in democratic societies, but also because it is technologically advanced, commercially consequential and has the size, market scale, scientific community, population, and commercial and shipping infrastructure to exercise enormous commercial power. Moreover, it has shown itself willing to leverage its commercial power for geostrategic ends and is quickly integrating technology into its military systems in a way that is altering the global balance of power.

15. In many respects, technology lies at the centre of the today's growing rivalry between China and the democratic community of nations. The two sides approach technological development in very different ways. Allied nations, for example, see technology development as a process fundamentally linked to the core freedoms liberal governance foster. They recognise that the marketplace of ideas as well as commercial markets themselves are fundamental to this process.

16. The Chinese perception is quite different. Beijing fully understands the significant role technology will play in future security calculations, but it looks at security through a highly authoritarian lens. Technology will not only be a critical difference maker in export markets and on the battlefield. It will also provide the ruling Communist Party powerful means to exercise ever greater social and political controls over its own society. The Chinese state's use of surveillance technologies exemplifies this relationship, and China not only deploys these technologies domestically but also exports them where it recognises the authoritarian impulse in other countries promises both commercial and diplomatic rewards. In this sense, technology stands at the front and centre of China's anti-democratic international campaign, the goals of which Russian and Iranian rulers share. Finally, while China wants to develop these technologies autonomously and often claims that this is its intention, it is currently not able to do so despite the great strides its own scientists have made. Beijing often relies on the technologies developed elsewhere and then seeks to acquire these through investment, mergers, technology sharing arrangements, and, when all else fails, espionage and outright theft. Its ambition, however, is to develop its own capacity to incubate and commercialise world leading technologies.

17. China has the capacity to muster enormous resources and the full weight of the state behind targeted technology projects. It has managed to make great strides in doing so, even though one element of this grand project involves the illicit acquisition of Western developed technologies. China, for example, established an early lead in 5G communications networks, in part, through these means. Concerns about its intentions have now led many democracies to deny Chinese firms a role in building out national 5G networks. China's long-term ambition is to take the lead across myriad technology sectors including AI, and it can tap into deep foreign exchange reserves to help underwrite these ambitions. A 2017 study by the Breugel research institute noted that even then, China was outperforming the European Union in terms of expenditure on research and development as a share of its GDP, and producing roughly the same number of scientific publications, and more

PhDs in natural sciences and engineering than the United States. China is also assuming an ever more powerful role in industries that intensively use scientific and technological knowledge. In 2017, it ranked second behind the US in terms of the share of total value added by high-tech manufacturing. In knowledge-intensive business, financial and information service industries, China had surpassed Japan to move into third place behind the US and the EU (Veugelers, 2017). These trends have only accelerated.

18. Although the West continues to produce an important share of innovative technologies, many with both commercial and military applications, the past forty years has seen new countries emerge as technology powers. The so-called Asian Tigers were among the first countries to move quickly up the production scale, graduating from mass producers of Western developed products to innovators of critical technologies that rivalled achievements of the older industrial powers. China itself quickly transformed its economic and technological capacities after opening the national economy to foreign investment and trade. According to the Australian Strategic Policy Institute's (ASPI) Critical Technology Tracker, China has established a lead in thirty-seven out of forty-four technologies ASPI is monitoring. ASPI's widely cited findings, which its experts presented to this Committee in Sydney in November 2023, focused on "high impact" research in critical and emerging technology fields. The study compared the number of research papers published in top-tier journals and then widely cited by subsequent research. It warns that China could be on the cusp of establishing a monopoly in eight of these technologies, including nanoscale materials and manufacturing, hydrogen and ammonia for power generation, and synthetic biology. It has made notable progress in advanced aircraft engines including those used in hypersonics (ASPI, 2023). ASPI's study notes that China and the United States are far ahead of other countries in these emerging technologies although India, the United Kingdom, South Korea, Germany, Australia, Italy and Japan are also important players (Hurst, 2023).

19. Artificial intelligence constitutes an increasingly important arena of trade and geostrategic friction between Western governments and China. AI is spawning a paradigmatic shift in technology development, global markets and the defence industry, and a race is underway to develop, commercialise and control/regulate the technology. China sees AI as a central element of national economic development and a linchpin of techno-authoritarian control systems which it deploys domestically and can market abroad along with its unique brand of authoritarian ideology. Beijing has used its Belt and Road network to train potential consumers of Chinese-generated AI products for security and logistical use. But authoritarian governments can also deploy these technologies for more nefarious purposes including political repression. China sells these technologies to build out partnerships with authoritarian elites in countries seeking to enhance their capacity to exercise social and political controls at the expense of civil society autonomy. From Beijing's perspective, there are both commercial and geopolitical advantages to moving down this commercial-technological pathway.

20. The West has also been compelled to focus on developing regulatory approaches given the potential dangers AI poses, including privacy violations, autonomous weapons deployment, disinformation, bias and discrimination, societal surveillance, and even theoretical extinction risks, among others (Roose, 2023). One could argue that this has put the West at something of a commercial disadvantage to China, which is willing to commercialise this powerful technology with no strings attached. By contrast, Brussels tends to regulate first and is quite insistent on the need to work out prudent regulatory frameworks as part of a comprehensive approach to building out the AI market. For its part, the Biden Administration recently issued an executive order to develop plans for regulation with international implications. The White House has promised to engage international allies and partners "in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges." The Federal Government is now committed to establishing responsible AI safety and security principles with other countries including competitors, "to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms." (The White House, 2023). The United Kingdom

is working with the United States on shared approaches to this regulatory challenge, including a global AI summit at Bletchley Park in 2023. The concern is, however, that as the West begins to lay out workable and responsible regulatory frameworks, China is already deploying and making this technology available to developing countries and has shown a general disregard for safety considerations. China would likely not abide by US and EU regulatory codes, and it uses this ostensibly *laissez faire* approach in its marketing to third countries (Kelley and Drexel, 2023).

21. Of course, there is a difference between advancing technologies and developing commercially and militarily viable end products. Here China has a less impressive track record then its Western competitors. According to a 2011 Center for American Progress, China's "import/assimilate/re-innovate model" had not fostered a climate of genuine innovation. Indeed, many of the Chinese institutions of higher education receiving governmental R&D engage in high rates of academic dishonesty which often goes unpunished. This has led to elevated levels of waste, fraud, and abuse in Chinese R&D spending (Gordon et al., 2011). Moreover, China's investment record is not impressive, and the country is currently undergoing a crisis, driven, in part, by poor and often politically driven or highly speculative investment. Slowing economic growth might well function as a check on Beijing's soaring technology ambitions particularly as fiscally pressed local governments play an oversized role in allocating funding for research throughout the country. Sixty percent of innovation funding comes from government sources in China, and weakening fiscal conditions could erode the financial base for China's technology ambitions (Boullenois et al., 2023)

22. But the alliance cannot simply discount these ambitions. China is too important a technology player to adopt a position of complacency. Indeed, Beijing is pushing hard on this front despite its current fiscal challenges. "Scientific and technological innovation has become the main battlefield of the international strategic game," Chinese President Xi Jinping stated in May 2021 (Boullenois et al., 2023). China's R&D spending has risen steadily over the past decade, and the government hopes to repatriate its best scientists and innovators through financial incentives. The appointment of five leading scientists to the Politburo in October 2022 encapsulates the degree to which China's leadership is prioritizing this effort and sees a national technological push as key to breaking through what it characterises as a Western technological "chokehold" (Jie, 2023).

IV- RESTRICTING SEMI-CONDUCTOR ACCESS

23. The semiconductor market has become a particularly crucial technology given its capacity to confer both commercial and military leverage to those countries that develop and commercialise the design and the manufacture of these chips. With China's announced intention to dominate the market and its willingness to pour resources into that project, the semi-conductor market has become particularly contested and increasingly shaped by national legislation aiming to protect this valuable intellectual property, secure relevant supply chains, and establish or repatriate a higher share of production capacity. The ambitions for these projects are both commercial and security driven.

24. As announced in the government's Made in China 2025 program, Beijing's goal is to achieve self-reliance in semi-conductor production. It aspires eventually to terminate trade in semi-conductors with Western producers and rely only on those made in China itself. But again, China lags in this sector and relies on imported chips to support its domestic industry. Although Beijing is not explicit in suggesting that espionage is crucial to its long-term strategy, in fact, it is. This points both to China's enduring weaknesses in this field and the need for Western companies and governments to protect their intellectual property more assiduously. Denying access to critical microchip manufacturing technologies is now central to the Western response.

25. The United States remains a leader in the design of microchips, and in some of the machinery that manufactures these essential industrial inputs. But the manufacturing of many of the most advanced chips has been largely offshored. Today roughly 70% of total manufacturing capacity lies in South Korea (25%), Taiwan (22%) and China (22%). Japan (14%) is the fourth largest producer, the United States is fifth at 8%, while Europe and the Middle East account for 6% of the market. This represents a significant departure from the situation in 1990 when the United States accounted for 37% of chip manufacturing, Europe 44%, and Japan 19%. The United States, however, has now awakened to the supply chain vulnerabilities of relying too heavily on Asian production and is intent on reclaiming its leadership role. The CHIPS and Science Act of August 2022, for example, appropriated USD 280 billion to galvanise domestic chip research and production (Zandt, 2023).

26. As it seeks to rebuild its manufacturing position, the United States government is also working to restrict Chinese access to US technologies used to manufacture sophisticated micro-processors. It has enacted a ban on the export to China of sophisticated printers needed to produce more advanced microchips unless it extends exceptional licenses. The decision also prevents the export of machines manufactured in the Netherlands and Japan that employ US licensed deep ultraviolet technology. The Dutch company ASML is a particularly important player in this market and had been exporting highly advanced lithography machines to China which had allowed China to manufacture chips with extraordinarily tiny transistor dimensions. The rule has also impacted sales by US firms like Applied Materials and Lam Research. China is years behind in its capacity to manufacture advanced chips with its own tools and has relied on machinery made in the US, the Netherlands and Japan to do so. Although allied governments largely agree with the aims of US policy, these restrictions on sales, services, and parts have provoked a degree of friction with the private sector producers that see China as a key market for these products (Swanson et al., 2023).

27. On 7 October 2022, the United States enacted new export controls designed to restrict China's access to US developed AI technology and limit its capacity to exploit that technology to expand its own capabilities on that front. Among the measures the US adopted was a decision to deny Chinese access to the highly advanced computer chip hardware needed to run AI programs. In March 2023, the Netherlands and Japan adopted similar restrictions. Like China, the United States, the European allies, and partner democracies in Asia recognise that AI represents a force multiplier that will shape future military and economic dynamics (Allen, 2023). Imposing restrictions on Chinese access to Western developed AI technology aims to make it more difficult for China to directly purchase these advanced chips or the equipment needed to develop these programs, and it will likely slow although certainly not entirely impede China's strategy to reinforce this strategic sector.

28. China has retaliated against the United States by preventing US semiconductor firms from merging with Chinese firms. It has also banned the sale of US made Micron memory chips to the Chinese critical infrastructure sector. Finally, it made the export of gallium and germanium, two critical inputs to the semiconductor sector, subject to strict export licensing requirements. Both minerals can be found elsewhere in the world, but the decision by the Chinese governments points to its willingness to leverage its powerful position in mining critical minerals needed for a range of digital technologies to counter Western strategic-economic ambitions. China is the world's leading player in extracting and processing rare earth minerals used across a range of leading technological sectors, and this decision has demonstrated its own willingness to deploy its market advantages in the mineral sector to advance its ambitions in the micro-processor sector.

29. Rare earth minerals that China mines are generally available elsewhere. The problem is that China has established a formidable lead in mining these commodities, and in signing access agreements where these minerals are found. Still, China must wield its powerful position with care because if it were seen as an unreliable supplier – and it is increasingly the case – this will inspire competitors to jump into the mining market and generate new supplies that undermine China's leverage. There are signs that such a response is underway, and the United States, the EU and the members of the G7 now see this as a de-risking imperative. Private companies are also making their

own de-risking decisions apart from the strategic policy decisions of their governments. Dell Inc., for example, has decided to end its reliance on Chinese manufactured chips in 2024 to reduce its exposure to future supply shocks (Allen, 2023).

30. Beijing also works diligently to undermine a unified Western approach to de-risking the chip trade. While the United States and the Netherlands, for example, have adopted a tough line on restricting Chinese access to sophisticated microchip manufacturing machinery needed to build chips to run an advanced AI sector, other Western governments have been more accommodating, and the Chinese offer very attractive financial terms for those willing to work with its firms in these sectors. Beijing is thus not facing an entirely united front on these matters. China is also working to counter restrictions that might hinder its broad effort to achieve a dominant position in AI by finding workarounds to import currently banned chips and equipment. It employs an extensive and sophisticated network of shell companies and smugglers for this purpose, and this, in turn, poses serious enforcement challenges to under-resourced Western export control agencies.

31. China also has a history of stealing technology and doing so is one of the highest priorities of its espionage agencies. This challenges Western firms and governments alike to enhance their own security and counter-intelligence capacities. China has long made technology sharing a prerequisite for foreign firms either operating in China or seeking to purchase shares of Chinese firms and this gives that country access to myriad Western developed technologies. Beijing also sees Western universities as vehicles for acquiring advanced technologies. Western universities, in turn, have become increasingly dependent on the fees paid by Chinese students. Beijing also employs Chinese citizens working for Western companies and at research facilities to steal proprietary technologies. Western governments have now begun to block Chinese nationals from working at certain advanced scientific and engineering departments to stymie this Chinese effort (Baazil and Koc, 2023).

V- THE RUSSIA CHALLENGE

32. Although Russia has a large defence sector and dedicates a significant share of its budget to underwrite its military, defence production and now its war on Ukraine, it is not in itself an impressive generator of cutting-edge technology. Russian military platforms often rely on imported dual use technologies. This represents a real vulnerability to the Russian military machine, and allied governments and partners want to restrict Russian access to these critical components and technologies. As a result of the war, both the United States and the EU have tightened technology export controls to limit Russia's access to technologies that might enhance its military capabilities.

33. Among the sanctions launched by the United States Department of the Treasury's Office of Foreign Assets (OFAC) was a set of export restrictions targeting technology needed by Russian military manufacturers. This policy aligned with commitments made by G7 leaders in May 2023. OFAC has also targeted individuals and entities that enable Russia's ability to procure high tech and dual use goods in violation of these rules. It has accused several companies in allied countries and in Russia as operating in contravention of the rules (Cross et al., 2023). In addition to sweeping restrictions on the Russian defence sector, the US government also imposed restrictions on sensitive US technologies produced in foreign countries using US-origin software, technology, or equipment. This included semiconductors, telecommunication, encryption security, lasers, sensors, navigation, avionics, and maritime technologies (The White House, 2022).

34. Since the start of Russia's war on Ukraine, however, the Kremlin has managed to exploit a range of loopholes to evade sanctions. It has, for example, tapped into a network of suppliers willing to move restricted products and technologies to Russia. Kyrgyz and Kazakh companies, for example, have exported restricted dual use technology including microchips to Russian suppliers who, in turn,

pass it on to the Russian military despite Western efforts to prevent this commerce moving through Central Asia. Both countries are members of the Russian-led Eurasian Economic Union and have routinely supplied Moscow with components from US firms like Texas Instruments and Analog Devices. Ukraine has found Western manufactured microchips used in thermal imaging guns in Russian military equipment recovered in Ukraine. Russian firms have also employed Kazakh companies to import restricted dual use electronics. US officials have raised this problem with both governments and have not taken off the table the possibility of imposing secondary sanctions.

35. Despite a range of sanctions and restrictions to which it is subject, Russia continues to access global markets surreptitiously to purchase telecom equipment, surveillance technologies, and sophisticated microchips for advanced computing, precision weaponry, and drones. It has done so through a host of intermediaries, shell companies and third countries including China but, in some instances, allied countries as well. A recent New York Times article reports that Russian trade officials routinely shared tips on which ports would transfer goods, who would trade in rubles and which port facilities would service Russian-flagged ships. “If one supplier stopped selling, they found another. If a shipping route was cut off, new ones took up the slack.” This has helped Russia stay one step ahead of sanctioning countries while ensuring a degree of access to technologies that it is incapable either of producing or acquiring through legal means. These kinds of revelations raise questions both about the permeability of Western sanctions and technology export controls and about the wilful obliviousness of some Western companies regarding the destination of their products (Mozur et al., 2023).

VI- EXPORT CONTROLS AND SANCTIONS

36. Efforts to restrict access to Western generated technology and weaponry is critical to any effort to maintain strategic technology-capability advantages over competitor nations. But as the nature of military technology development has changed, governments have had to reassess export control strategies aiming to limit access to critical military systems. Indeed, during the Cold War, export controls focused largely on military hardware while most commercial products, with some notable exceptions, essentially flew under the radar and were far less restricted. Now allied governments need to assess the capacity of commercial technologies to contribute to competitor nation military capabilities and lay out strategies to limit access to these technologies when necessary.

37. Indeed, the changing paradigm of military equipment development demands new export control strategies. Governments must exercise more stringent controls over dual use technology exports, but this can be technically and politically daunting. Restrictions can impinge on the export potential of commercially important technologies in areas like digital communications, artificial intelligence, biometrics, quantum computing and aerospace technologies. Controlling the secondary export of commercial technology, moreover, poses all manner of regulatory and enforcement challenges. Whereas the goal once was to limit narrowly defined military capabilities of rival countries, today strictly defined military capabilities are not the only focus for those regulating technology trade. Concerns about threats to critical commercial supply chains and technology driven human rights abuses are also informing deliberations on these matters. The United States Export Control Reform Act of 2018 (ECRA), for example, notes that “the protection of human rights and the promotion of democracy” represent a fundamental US foreign policy interest (Kelley, 2023).

38. For control regimes to be effective, it is essential to build coalitions among like-minded states so that restrictions are sufficiently comprehensive to effectively impede access of these technologies to rivals. This requirement shapes the choices available to policy makers as building broadly supported control regimes requires consideration of the interests of allies and partners and demands shared risk assessments. One could argue that these controls are only as strong as the weakest link

in the coalition, and this creates daunting diplomatic as well as regulatory challenges. It also can require the applications of sanctions or secondary sanctions on countries and companies that wilfully or negligently violate agreed restrictions. Differing legal standards, however, can make the application of secondary measures particularly challenging across a broad coalition of countries.

39. The multilateral Wassenaar Arrangement has long facilitated exchanges and coordination of export controls on dual use technologies as they related to non-proliferation objectives and military exports. But that Arrangement is both limited and flawed since Russia participates in the process. Moscow can thus block export controls within this process. This compels members to work outside of the framework to block exports to Russia. The United States and Europe must then patch together coalitions of the willing to control sales of dual use technologies. International coordination of these policies has taken place within NATO itself but also in other fora albeit in a more ad hoc fashion.

40. The recently created AUKUS partnership, which has significantly deepened defence cooperation among the United States, Australia, and the United Kingdom, has had to confront this challenge directly. Indeed, one of the preconditions for deepening military-technology cooperation among these three states for the purpose of developing and procuring a new generation of nuclear-powered submarines has been to shore up controls on the export of dual use technologies to ensure that these technologies do not end up in the hands of rival states. A recently proposed Australian law, for example, would tighten restrictions on how industries and universities share defence-related technology with foreigners, while exempting both the United Kingdom and the United States from these controls. The legislation outlines criminal offences, restricts sharing defence technology to foreign persons both in and beyond Australia while permitting license-free sharing among AUKUS partners (Harris, 2023). Australia has thus opened its technology sharing potential with like-minded partners while imposing new restrictions on technology sharing with rival countries and others. It has thus sought to balance between openness and security.

41. States must engage the private sector in weighing these trade-offs. If there is no buy-in from commercial actors, resistance to these controls can make effective action difficult and the matter can be unhelpfully politicised or subject to diplomatic controversy. Indeed, commercial actors must be engaged, incentivised, and monitored to ensure success in limiting access to critical technologies while finding new ways to share this technology with allies and partners. Market operators have critical knowledge that Ministries of Defence and Trade need to tap into to ensure that any limits on technology trade are effective and properly targeted. The goal is to minimise costs and maximise impact. The US government, for example, manages the domestic dialogue with industry through the Emerging Technology Technical Advisory Committee (TAC). The TAC meets four times yearly to identify potential dual use technologies. It generates advice to the US Department of Commerce on specific export controls for emerging technologies and collaborates with the State Department to manage the diplomatic angle with allies and partners.

42. Engaging with industry reduces the likelihood that government restrictions will result in supply chain shocks that complicate efforts to move technology to market. Governments need to be transparent about why particular restrictions are essential both to convince national actors and to assure the international community that security is not being used as a prop to justify protectionism. Export restrictions, by definition, reduce the scale of potential markets and can upset the metrics employed by investors. Here it may make sense for states to devise vehicles to help underwrite research and development costs to compensate for reduced market depth. This could, for example, constitute legitimate use of funds allocated for defence research and development even when these technologies are primarily commercially oriented.

43. Universities are critical engines of technology development. Many closely work with both the private sector and state bodies which fund both basic and applied research. They also educate specialised workers needed by industry to develop commercial and defence applications for these technologies. Indeed, university researchers in the United States and Europe are increasingly

positioned both to patent their findings and participate in the commercialisation of technologies developed at research universities. It is also worth noting that competitor countries' intelligence agencies increasingly target universities for intellectual property theft. This is another challenge that policy makers need to address in partnership with universities that depend on the income generated by tuition paid by Chinese students and findings made by Chinese researchers.

44. A related challenge involves the sheer proliferation of technology capacity. In the early Cold War, technical innovation was largely if not exclusively concentrated in the democratic world. Russia generated much of its own technology through the defence sector when China was only beginning to industrialise and much of the developing world was a consumer rather than a generator of advanced technologies. The technology landscape has evolved significantly since then.

45. The ever-broader diffusion of innovative capacities and the technology and applications that capacity produces obviously reduces the leverage of any single country like the United States or a group of countries like those in NATO over the international market. In practical terms, this makes it ever more difficult to establish broadly respected market standards, rules, and norms on technology transfer. Indeed, this arena has become a highly contested space. Obviously, the degree to which an ideologically compact group of countries plays a key role in technology development and commercialisation and shares a common vision regarding industry standards and rules, including the nature and degree of any security driven export controls they deem necessary, will help determine the capacity of those countries to shape the market. If unity proves elusive or if countries beyond that coalition develop and manufacture these technologies, this leverage begins to wane. This suggests that the conduct of diplomacy on these matters is one key to any successful effort to establish international governance that both facilitate commercialisation and reduce security risks.

46. In a recent EU strategy document, the Commission admitted that it needs to do more to address critical supply chain vulnerabilities. Failure to move on these fronts will leave Europe vulnerable to coercion and a range of economic risks. National security and resilience, the document suggests, are now intertwined and some of what were once viewed as benign economic linkages are now understood to pose security risks. It suggests that "Working together with our allies, partners, and the business sector to articulate and execute a vision of economic security will serve as a force multiplier" (European Commission, 2023). The Commission recognises that it needs a strategy for economic security that identifies de-risking as an essential security tool, understands technological advance as key to economic dynamism and argues that innovative technologies are blurring the boundaries between civil and military sectors. It says that Europe must promote its competitiveness, protect itself from economic security risks and partner with the broadest possible range of countries that share these concerns and interests in greater economic security. The Commission is also calling for greater supply chain resilience, physical and cyber security measures to defend critical infrastructure, and to address the weaponisation of economic dependencies. It argues that Europe needs to establish policies to better cope with foreign subsidies, 5G/6G security, foreign direct investment screening, export controls and the development of tools to counter economic coercion. It also needs to expand the EU toolkit to deal with exports and outward investment of key enabling technologies with military applications including quantum technologies, advanced semi-conductors, and artificial intelligence.

47. For its part, the United States has established tough export rules to restrict access to sensitive technologies, but for both the United States and Europe there is a disconnect between the aspirations as expressed in legislation and rules, on the one hand, and practice, on the other. The gap is a product of leaky enforcement. In 2022, for example the United States government announced rules forbidding US companies from selling and servicing equipment to manufacture chips below the 14-nanometer level used in supercomputers and in computers developing artificial intelligence. Following the Russian attack on Ukraine, NATO allies and partners formally halted the sale of machine tools to Russia. But Western machine tools have continued to operate in Russian missile factories as well in China's telecommunication and semi-conductor manufacturing facilities.

The problem is not so much the lack of tough rules, but more one of weak enforcement (Miller and Schneider, 2023). China and Russia have found myriad ways to import prohibited technologies, and both have developed workarounds to circumnavigate current control regimes to acquire all manner of restricted Western dual use technologies. Beijing has long employed the direct purchase of technology firms to acquire US and European innovations used in Chinese military systems. It has also exploited bankruptcy proceedings and acquisitions by foreign venture capital firms to acquire companies producing sensitive and military useful technologies (Bennett and Bender, 2018). Efforts are underway to close these loopholes.

48. Understaffing of enforcement officials in government and industry needed to uphold restrictions poses another problem. In the United States, the Bureau of Industry and Security (BIS) at the Department of Commerce enforces export controls on semiconductors bound for China, and all other US-controlled dual use exports. But BIS has only six hundred employees to play an oversight role covering trillions of dollars of exports, and its budget stands at USD 200 million. This is a herculean task for such a small number of officials (Allen, 2023). Staff shortages limit the US government's capacity to enforce export restrictions and it must carefully harness its investigative and prosecutorial assets to maximise their impact. Indeed, financing export control enforcement poses challenges throughout the alliance. Governments now need to bolster spending to plug leakages of vital and protected technologies to competitor countries under sanction or other restrictions.

49. Other countries have significantly less personnel to cope with challenge, and it is difficult to accumulate enough evidence to prosecute rule breakers. The capacity of officials to track financial transactions related to this illegal trade is even lower. Enforcement efforts tend to focus on shadowy and elusive intermediaries rather than Western producers. If Western companies face few adverse consequences for indirectly selling sensitive technologies through intermediaries to competitor countries on sanctions or restrictions lists, then they will have incentives to ignore glaringly obvious cases of sanctions violations. This can lead to an "export and forget" mentality that erodes respect for both the letter and spirit of these laws and regulations (Ribakova, 2023).

50. Resales of restricted technologies pose another set of challenges. Western firms frequently sell into countries where technology restrictions do not apply or are less rigorous. Many routinely fail to track the movement of the technology to the actual end user. Importers of these products can find ways to sell on to Russia and China, and there are obvious premiums in doing so. A shadow network trafficking in diverted technology has emerged with obvious support from Beijing and Moscow. Enforcement of the rules established by allied governments has proven inadequate.

51. Governments are beginning to address this problem in a more comprehensive fashion. The EU is developing innovative approaches to monitoring and controlling the way European companies invest in production facilities overseas, and it is closing loopholes and regulatory lacunae that made reexport of restricted technologies to Russia and China possible. But there has been resistance in member states which maintain important trading relations with China. The US has taken a direct interest in this discussion and, for example, directly negotiated with the Netherlands to agree restrictions on the sale of Dutch made chip printing technologies to the Chinese (Bounds, 2023).

52. The EU's dual use regime recognises the challenge of ensuring that third countries do not reexport restricted technologies and has now established a licensing requirement to control sensitive technology exports. The European Council has recently added various digital surveillance technologies to its existing control list. The decision to do so is driven by concerns that these technologies simply reinforce dictatorships intent on suppressing basic human rights. It urges companies to exercise due diligence to ensure that exported technologies are not used for such purposes. The EU has accordingly enacted tight controls on the export of facial recognition technologies to China and Belarus, among others.

53. The various EU sanctions packages targeting Russia have included the prohibition of direct and indirect export to Russia of a range of dual use products that are listed in Annex I of the EU dual use regulation. The relevant Council regulation states that "it shall be prohibited to sell, supply, transfer or export, directly or indirectly, dual use goods and technology, whether or not originating in the Union, to any natural or legal person, entity or body in Russia or for use in Russia." (European Council, 2022)

54. In its 11th package of sanctions on Russia, the EU expressly takes on the problem of sanctions circumvention with a series of countermeasures that according to European Commission President Ursula von der Leyen aim to "prevent Russia from getting its hands on sanctioned goods." David O'Sullivan, the EU's international special envoy for the implementation of EU sanctions has been charged with developing policies to make such deviations more difficult (Schreck et al., 2023). The current EU list of restricted items includes cutting-edge technology (e.g. quantum computers and advanced semiconductors, electronic components and software), certain types of machinery and transportation equipment, specific goods and technology needed for oil refining, energy industry equipment, technology and services, aviation and space industry goods and technology (e.g. aircraft, aircraft engines, spare parts or any kind of equipment for planes and helicopters, jet fuel), maritime navigation goods and radio communication technology, a number of dual use goods such as drones and software for drones or encryption devices, civilian firearms, their parts and other army materials, chemicals, lithium batteries and thermostats, and goods which could enhance Russian industrial capacities (European Council, 2024). The EU is cooperating with the United States, the United Kingdom and other NATO countries on these sanction measures.

55. The United States and the EU have deepened their dialogue on dual use technology and cyber-surveillance export controls. These issues are on the agenda of the Trade and Technology Council (TTC) which coordinates export control regulations based, in part, on shared intelligence and joint identification of security threats. This is not always easy given the distinctive regulatory mechanisms employed on each side of the Atlantic and the sometimes-differing security and economic calculations each makes. Differing regulatory frameworks as well as the complicated task of balancing national security interests with economic considerations have militated against rapid across the board agreement on these matters. (Du Bois and Reyes, 2023).

VII- THE NATO APPROACH TO TECHNOLOGY AND ITS COMMERCIAL DEVELOPMENT

56. As suggested above, NATO has always identified technology development as a critical force multiplier, an agent of interoperability and a source of efficiency. It encourages the development and integration of critical emerging technologies into the planning cycles and force structures of allied nations and has established institutional links to the scientific and defence industrial communities to ensure a continuous dialogue on these matters. NATO itself has several bodies promoting technology development: the Science and Technology Organization, the NATO-Industry Forum, and the NATO Industrial Advisory Group. It also has a command dedicated to defence innovation – Allied Command Transformation (ACT) in Norfolk, Virginia.

57. Considering ever accelerating technological change and the emergence of new threats which will require technological responses, NATO governments have recognised the need to ensure that NATO and member states more closely monitor advances in the commercial realm that could make a difference on the battlefield. At a February 2021 Defence Ministerial, the NATO Secretary General proposed launching a Defence Innovation Initiative to promote interoperability, strengthen NATO standards across a range of systems and boost transatlantic cooperation on defence innovation.

58. Then at the 2021 Brussels Summit, leaders launched the Defence Innovation Accelerator for the North Atlantic (DIANA). DIANA is now coordinating financial support for a range of innovation projects with the private sector. It is, in effect, a technical financing hub that joins up public and private investment funds from small and medium firms, including start-ups developing advanced technologies with potential use for allied militaries. DIANA has regional offices in London, Halifax, Canada as well as a regional hub in Tallinn, Estonia. In addition, DIANA will establish a network of more than ten affiliated accelerator sites and ninety test centres in innovation clusters across the Alliance. This network will be dynamic, and the expectation is that it will continue to grow. DIANA aims to deepen transatlantic cooperation on vital technologies, promote interoperability among allied forces through this cooperation, and tap into civilian innovation which is generating militarily significant technologies by engaging directly with academia and the private sector (Mundell, 2023). Technologies developed through DIANA may also receive funding from the NATO Innovation Fund, a EUR 1 billion venture capital fund established by a group of NATO Allies at the 2022 Madrid Summit. The fund will support small companies producing dual use technologies of potential application to defence and security, including those engaged with DIANA (NATO, 26 September 2023).

59. This ambitious endeavour seeks to deepen interoperability and reduce the costs of innovation. DIANA will be particularly useful for smaller Allied countries which do not enjoy scale economies in research and development (NATO, 14 June 2021). In November 2023, DIANA selected the first group of forty-four companies (out of 1,300 applicants) tasked to develop technology to enhance energy resilience, undersea sensing and surveillance, and secure information sharing. DIANA also issued a call for mentors to support and advise the chosen innovators and entrepreneurs. Each company will receive EUR 100,000 to help address one of the three specific challenges. The grant can cover salaries, rent and equipment (NATO, 4 December 2023).

60. NATO has also established an Artificial Intelligence Strategy both because of this powerful technology's capacity to alter fundamentally the global defence and security environment and the likelihood that it will be a highly consequential force multiplier for NATO, but also for its strategic competitors. Indeed, AI will recast the way NATO undertakes its core missions of collective defence, crisis management and cooperative security. Allied governments want to ensure that they deploy AI in a responsible fashion and ensure that its use complies with national and international law, builds in human responsibility to decision making, is safe, dependable, and governable, and does not reinforce bias. At the same, Allies must quickly incorporate AI into the capability development process while enhancing interoperability and denying malicious state and non-state actors' access to these critical technologies (NATO, 22 October 2021). In the same manner, NATO has also developed a Quantum Strategy. These technologies are particularly important for sensing, imaging, precise positioning, navigation, and timing, improving the detection of submarines, and upgrading and securing data communications with quantum resistant cryptography. Many of these technologies are already in commercial use. NATO is accordingly cooperating with industry to develop a transatlantic quantum technologies ecosystem, while also preparing NATO to defend itself against the malicious use of these technologies (NATO, 17 January 2024).

61. Finally, NATO has acknowledged that supply chain vulnerabilities constitute a strategic concern that it must address. The Strategic Concept adopted in June 2022, for example, noted that China aspires to control key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains. It uses its economic leverage to create strategic dependencies and enhance its influence. That document calls for a robust, integrated, and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to security, as a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty. The Strategic Concept states that NATO will identify and mitigate strategic vulnerabilities and dependencies, including those pertaining to critical infrastructure, supply chains and health systems. It accordingly promises to bolster NATO's capacity to prepare for, resist,

respond to, and quickly recover from strategic shocks and disruptions, while ensuring the continuity of the Alliance's activities (NATO, 29 June 2022).

VIII- CONCLUSION

62. NATO allies require a more comprehensive framework for regulating trade in sensitive technologies with competitor nations. It is not at all evident that the status quo is altering the risk calculations of those directly or indirectly trading restricted dual use technologies. Governments need better enforcement tools and resources, including secondary sanctions on countries facilitating this trade. Allies should accordingly strengthen their enforcement capacities as trade controls are useless if violators feel they can act with impunity. The producers of restricted dual use technologies in the private sector need incentives to ensure that end users are not those countries on restricted lists. Governments should also engage financial institutions in these efforts as following the money can effectively expose law breakers.

63. Governments need better assessments of risks posed by technology leakages precipitated by technology trade, targeted investments in Western firms made by competitors, and espionage. Dual use technologies pose a particularly daunting challenge in this regard as their military potential as well as their capacity to facilitate human rights violations is not always evident. Allied governments need forward looking criteria to make these assessments, and the reflection process should engage government, the military, universities, and the private sector.

64. In the face of China's concerted effort to develop microprocessor and AI industries superior to those of its Western competitors, recognising that it seeks to deploy these technologies to create an international order antithetical to democracy and noting its willingness to engage in technology theft to achieve these ends, allied governments and companies need to exercise enormous vigilance to protect these technologies and limit access to them. This requires a multifaceted approach, including tough export control policies, fully funded enforcement agencies, counter-espionage efforts, and a willingness to collaborate across industries and borders.

65. Secondary sanctions on countries violating technology export restrictions and sanctions seem increasingly necessary. As governments close regulatory loopholes to make current sanctions regimes and technology transfer restrictions efficient and impactful, they will need more stringent penalties to incentivise actors violating those restrictions. Companies need incentives to ensure compliance with these rules and should not close their eyes to those actors engaged in outlawed reexporting. It is particularly important that governments prevent commercial operators from sending restricted Western machine tools and the parts needed to maintain these to Russia, China and other strategic competitors that intend to use this equipment to build weapons. Russia, for example, is more than likely to then deploy these weapons against Ukraine and use them to threaten allied nations (Miller and Schneider, 2023).

66. Allied governments should continuously work to coordinate export controls on emerging dual use technologies and to protect strategic intellectual property so that these innovations are not incorporated into the manufacturing process of rival states like Russia and China. This effort should be global in nature and placed high on the agenda of US-EU trade and security discussions, and the Trade and Technology Council, but also in AUKUS, the EU-Asia Dialogue, the G7 and the Quadrilateral Security Dialogue which engages the United States, Japan, India, and Australia.

67. Researchers have tabled proposals to make sure that technology exports restrictions are enforced. One idea is to require tamperproof geolocation devices in sophisticated machine tools to track if and how they are reexported to countries on prohibited lists. These tools could also be

structured to disable machines that illegally end up in Russia, China or in other proscribed countries. Software tracking systems can serve the same ends. Most importantly, the governments of the countries producing this equipment need to deepen their collaboration on these kinds of measures so that there is a united front and no lowest common denominators leaking restricted technologies to strategic competitors. Governments need to ensure that their national companies are assuming their responsibilities as well, and penalties need to be sufficiently high to dissuade those looking for quick profits at the expense of national security. The banking sector is already subject to these kinds of restrictions. It is now time to make sure that technology producing firms are as well. Getting serious about machinery export controls today is one of the most cost-effective ways to meaningfully limit the capacity of adversaries to develop high end capabilities tapping into the most sophisticated technologies. Facing a revanchist Russia and adversarial China, governments need to deepen their collaboration and properly fund these vital defensive efforts (Miller and Scheider, 2023).

68. One persistent challenge lies in balancing security considerations against the need to maintain open trading regimes. It is important that technology generating societies, the prosperity of which increasingly hinges on the capacity to commercialise technology advances, do not effectively kill the golden goose through overly stringent controls and outright protectionism. Governments must strike reasonable balances between economic and security considerations. Here too, structured dialogue among allies and partners and with the private sector and research communities are essential. Systematic cost-benefit analysis of technology control policies is thus essential in this regard.

69. Allied governments need to consider investment's role in technology proliferation. China uses inward and outward investment to acquire dual use technologies. More coordination among allied and partner countries in developing and enforcing relevant investment rules are needed. Russia and China are using shell companies to gain access to restricted technologies. Coping with this challenge requires vigilant monitoring, international coordination and secondary sanctions against firms and countries facilitating these practices (Mozur et al., 2023).

70. Although Western technological advantages are the product of liberal free markets and the spirit of free inquiry, state support has nonetheless also been critical to underwriting technological development. Many of today's critical technologies, including the internet itself, are spin offs from technologies originally designed for and with the support of national military budgets and state support for basic research at leading universities. Military requirements and procurement programs will continue to be an important catalyst for technology development even as the paradigm has shifted from commercial technology "spinning off" from defence related projects to a process in which commercial technologies "spin in" to the defence sector.

71. Money matters in this regard, and it is important that a significant share of Allied defence budgets continue to allocate funding to support technological advances with military applications. This is precisely why allies first agreed at the 2014 Wales summit to meet the 2% of GDP guideline for defence spending and the 20% of annual defence expenditure guideline on major new equipment expenditure, including investment in research and development (NATO, 27 September 2023). These percentages now represent the floor of what allies need to spend on defence and related technology and equipment investment, and it is a matter of urgency that they do so. NATO's DIANA initiative is important in this regard as it will help identify companies generating promising technologies and link those firms up with potential funding sources. This is a welcome development and will broaden the community of commercial players engaging directly with NATO to produce technologies that will help reinforce deterrence over the coming decades.

72. Engaging those institutions that serve as incubators of emerging technologies including research universities and specialised laboratories conducting basic and applied research is essential. These institutions have a special perspective on the pathway of technological advance and how it might be weaponised. Understanding this early on can serve policy makers seeking to ensure that that such technology does not end up in the hands of dangerous rivals, intent on

undermining international security. Allied governments should tighten rules to restrict students from strategic competitors from studying in programs developing militarily sensitive technologies.

73. The gestation period for military technology development is typically long, and it can take decades to go from the conceptional phase to the deployment of new platforms and systems. These timelines, however, are quickening, in part, because of the information revolution. AI itself will become a critical agent for speeding the pace of technological advance, and this is precisely why NATO allies need coherent and well-funded technology development programs to put all allies into a better position to exploit the advance of technology to bolster national and collective security.

BIBLIOGRAPHY

Allen, Gregory C., “China Is Striking Back in the Tech War with the U.S.”, Time, 20 July 2023 https://time.com/6295902/china-tech-war-u-s/)

ASPI, “Who is Leading the Critical Technology Race?”, Critical Technology Tracker, 22 September 2023, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-09/All%20technologies%20by%20top%205%20countries%20and%20tech%20monopoly%20risk_0.pdf?VersionId=t4zjD8euvaT9P.WHc6wFMbDC81Cm8uMj

Bennett, Cory And Bryan Bender, “How China acquires ‘the crown jewels’ of US technology”, Politico, 22 May 2018, https://www.politico.eu/article/china-investment-uber-apple-us-tech-how-china-acquires-the-crown-jewels/

Boullenois, Camille, Agatha Kratz, and Laura Gormley, “Spread Thin: China’s Science and Technology Spending in an Economic Slowdown”, Rhodium Group, December 15, 2023, https://rhg.com/research/spread-thin-chinas-science-and-technology-spending-in-an-economic-slowdown

Bounds, Andy, “Brussels seeks new controls to limit China acquiring high-tech”, Financial Times, 14 March 2023, https://www.ft.com/content/af9671d8-39fa-4de2-9428-cbcaca838d58

Baazil, Diederik and Cagan Koc, “Dutch seek to Bar Chinese Students from Tech Courses in Chip War”, Bloomberg, 12 Junne 2023, https://www.bloomberg.com/news/articles/2023-06-12/dutch-seek-to-bar-chinese-students-from-tech-courses-in-chip-war?embedded-checkout=true

Bockel, Jean-Marie, The Future of the Space Industry, NATO PA Report [173 ESC 18 E fin], 17 November 2018, https://www.nato-pa.int/document/2018-future-space-industry-bockel-report-173-esc-18-e-fin

Brunner, Karl-Heinz, “Space and Security – NATO’s Role”, NATO PA Science and Technology Special Report, 10 October 2021, https://www.nato-pa.int/document/025-stc-21-e-space-and-security-natos-role-report-brunner

Cross, Jonathan, Christopher Boyd, Brittany Crosby-Banyai and Kelly Adams, “With Wide-Ranging New Sanctions, United States Treasury Department Targets Russian Technology Supply Chains, Military-Linked Elites And Industrial Base, And More”, Herbert Smith Freehills, Mondaq.com., 20 September 2023, https://www.mondaq.com/uk/export-controls--trade--investment-sanctions/1368104/with-wide-ranging-new-sanctions-united-states-treasury-department-targets-russian-technology-supply-chains-military-linked-elites-and-industrial-base-and-more

Du Bois, Rudi and Alexandre Tapia Reyes, “Dual-use and cyber-surveillance: EU policies and current practices”, European Parliament, November 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754439/EXPO_BRI(2023)754439_EN.pdf

European Commission, “European Economic Security Strategy: Joint Communication To The European Parliament, The European Council And The Council” Join(2023) 20 Final, 20 June 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023JC0020

European Council, Council Regulation (EU) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine states, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0328

European Council, “EU sanctions against Russia explained”, 15 March 2024, https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

Ewalt, David M., “Europe’s Most Innovative Universities 2019”, Reuters, https://www.reuters.com/article/idUSKCN1S60O9/

EY India “How India is emerging as the World's Technology Hub”, 27 January 2023, https://www.ey.com/en_in/india-at-100/how-india-is-emerging-as-the-world-s-technology-and-services-hub

Gordon, Kate, Susan Lyon, and Ed Paisley, “Rising to the Challenge: A progressive U.S. Approach to China’s innovation and competitiveness policies,” Center for American Progress, https://www.americanprogress.org/article/rising-to-the-challenge-2/
Harris, Bryant “Congress lays groundwork for AUKUS export control reform”, Defense News, March 22, 2023, https://www.defensenews.com/congress/2023/03/22/congress-lays-groundwork-for-aukus-export-control-reform/
Hurst, Daniel, “China leading US in technology race in all but a few fields, think tank finds”, The Guardian, 2 March, 2023, https://www.theguardian.com/world/2023/mar/02/china-leading-us-in-technology-race-in-all-but-a-few-fields-thinktank-finds
IT Services India, “Top technology trends for 2023 and 2024”, 12 September 2023, https://www.linkedin.com/pulse/top-technology-trends-2023-2024-it-services-india/
Jie, Yu, “China’s new scientists”, Chatham House, 24 July 2023, https://www.chathamhouse.org/2023/07/chinas-new-scientists/breaking-chinas-technological-chokepoints
Kelley, Hannah, “Dual-Use Technology and U.S. Export Controls: Findings from the CNAS Technology Policy Lab”, CNAS, 15 June 2023, https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls
Kelley, Hannah, and Bill Drexel, “How China is beating the U.S. at AI”, CNAS, 30 November 2023, https://www.cnas.org/publications/podcast/how-china-is-beating-the-u-s-at-ai
Kissinger, Bernice, “The importance of dual-use technologies for the warfighter”, Defence Connect, 11 August 2023, https://www.defenceconnect.com.au/industry/12547-opinion-the-importance-of-dual-use-technologies-for-the-warfighter
Law, Marcus, “Magnificent Seven’ Tech Companies Driving Forward With AI”, Technology, 20 February 2024, https://technologymagazine.com/articles/magnificent-seven-tech-companies-driving-forward-with-ai
Lee, Caitlin, “Winning the Tech Cold War”, The RAND Blog August 17, 2023, https://www.rand.org/blog/2023/08/winning-the-tech-cold-war.html
Miller, Chris and Jordan Schneider, “How to Stop Our High-Tech Equipment From Arming Russia and China”, The New York Times, 29 December 2023, https://www.nytimes.com/2023/12/29/opinion/chips-semiconductor-china-russia-military.html
Mozur, Paul, Aaron Krolik and Adam Satariano, “Chinese Traders and Moroccan Ports: How Russia Flouts Global Tech Bans, The New York Times, 19 December 2023, https://www.nytimes.com/2023/12/19/technology/russia-flouts-global-tech-bans.html
Mundell, Ian, “The Ecosystem: Civilian start-ups are embracing NATO’s new interest in dual use technology”, Science Business, 8 November 2023, https://sciencebusiness.net/news/start-ups/ecosystem-civilian-start-ups-are-embracing-natos-new-interest-dual-use-technology
NATO, “Brussels Summit Communiqué,” 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm
NATO, Defence Innovation Accelerator for the North Atlantic (DIANA), 26 September 2023, https://www.nato.int/cps/en/natohq/topics_216199.htm
NATO, “DIANA announces first cohort of innovators, launches call for mentors”, 4 December 2023, https://www.nato.int/cps/en/natohq/news_220930.htm?selectedLocale=en
NATO, “Funding NATO”, 27 September 2023, https://www.nato.int/cps/en/natohq/topics_67655.htm
NATO, “NATO releases first ever quantum strategy”, 17 January 2024, https://www.nato.int/cps/en/natohq/news_221601.htm?selectedLocale=en
NATO, “2022 Strategic Concept,” 29 June 2022.
NATO, “Summary of the NATO Artificial Intelligence Strategy”, 22 October 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm?selectedLocale=en
Needham, Kirsty, “Australia plans to boost AUKUS tech-sharing, restrict 'foreign' access”, Reuters, 14 November 2023, https://www.reuters.com/world/australia-plans-boost-aukus-tech-sharing-restrict-foreign-access-2023-11-14/
Ribakova, Elina, “Economic sanctions risk losing their bite as a US policy weapon: More effective enforcement and stepped-up compliance on the part of the private sector are needed”,

Financial Times, 7 November 2023, https://www.ft.com/content/b54201be-f307-4171-bb99-b356537b1898

Ricart, Raquel Jorge "NATO Defense Innovation and Deep Tech: Measuring Willingness and Effectiveness", Carnegie Europe, 29 August 2023, https://carnegieeurope.eu/2023/08/29/nato-defense-innovation-and-deep-tech-measuring-willingness-and-effectiveness-pub-90314#:~:text=NATO%20defines%20nine%20technology%20priorities,manufacturing%2C%20and%20energy%20and%20propulsion

Roose, Kevin, "A.I. Poses 'Risk of Extinction,' Industry Leaders Warn", The New York Times, 30 May 2023, https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html

Schreck, Carl et al., "Kyrgyz, Kazakh Companies Send Western Tech To Firms Linked To Kremlin War Machine, Radio Free Europe, 22 June 2023, https://www.rferl.org/a/kyrgyz-kazakh-firms-investigation-western-tech-russia-war-ukraine/32467795.html

Swanson, Ana, Don Clark and Mara Hvistendahl, "The Multimillion-Dollar Machines at the Center of the U.S.-China Rivalry", The New York Times, 20 October, 2023, https://www.nytimes.com/2023/10/20/business/economy/us-china-chip-manufacturing-asml.html?action=click&module=RelatedLinks&pgtype=Article

The Under Secretary of Defense for Research and Engineering (USD(R&E) Website, U.S. Department of Defence, https://www.cto.mil/usdre-strat-vision-critical-tech-areas/

Vergun, David, "DOD Modernization Relies on Rapidly Leveraging Commercial Technology", 25 January, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3277453/dod-modernization-relies-on-rapidly-leveraging-commercial-technology/

Veugelers, Reinhilde, "The challenge of China's rise as a science and technology powerhouse: China's ambition to be a global leader in science and innovation by 2050 seems well within reach", Policy Contribution, Issue no.19, July 2017, https://www.bruegel.org/sites/default/files/wp_attachments/PC-19-2017.pdf

The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", 30 October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

The White House, "Fact Sheet: Joined by Allies and Partners, the United States Imposes Devastating Costs on Russia," 24 February 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/fact-sheet-joined-by-allies-and-partners-the-united-states-imposes-devastating-costs-on-russia/

UK Department for Science, Innovation & Technology, Foreign, Commonwealth & Development Office, "The UK's International Technology Strategy", 22 March 2023, https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy

Zandt, Florian, "Where Can the Most Chips Be Manufactured?", Statista, 5 December 2023, https://www.statista.com/chart/31371/distribution-of-global-semiconductor-fabricating-capacity/#:~:text=According%20to%20data%20from%20semiconductor,13%20percent%20share%20in%202022