NATO PARLIAMENTARY ASSEMBLY

SCIENCE AND TECHNOLOGY COMMITTEE (STC)

DEFENCE INNOVATION

Special Report

by Leona ALLESLEV (Canada)
Special Rapporteur

041 STC 20 E rev. 1 | Original: English | 20 November 2020

TABLE OF CONTENTS

I. INTRODUCTION

1. In 2020, NATO finds itself in a highly volatile and rapidly changing international security environment. A revisionist Russia is positioning itself as a “strategic competitor” to NATO and a rising China is poised to become a true military peer competitor. In addition to traditional security threats emanating from nation states, the Allies are now also facing new challenges from internationally active terrorist organisations while cyberattacks and disinformation campaigns target critical infrastructure and undermine the cohesion of our societies. At the same time, the power shift towards new and emerging actors and disruptive technologies call into question the existing world order, with considerable implications for NATO.

2. In the past, their technological edge over their adversaries enabled the Allies to balance the numerical superiority of the Warsaw Pact in manpower, tanks, fighter aircraft, submarines, and other military equipment. In the years following the Cold War, NATO Allies, and the United States in particular, benefitted from their earlier, long-standing investment in Research and Development (R&D).

3. Now, however, NATO’s technological edge is rapidly eroding due, among others, to the continued proliferation of advanced weapon systems. Moreover, non-state actors’ easy access to dual-use technology, i.e. technology that can be used both commercially and militarily, magnifies their destructive potential. Therefore, the Alliance is facing expanding asymmetric threats from state and non-state actors, who are increasingly more agile and using inexpensive technology to an incredibly disruptive effect. The COVID-19 crisis demonstrates that there is a threat to our well-being from the health front as well. In addition to challenging the preparedness of our armed forces and the resilience of our health systems, the pandemic provides opportunities our adversaries can exploit. For example, Russia and China are hacking into the vaccine research of our companies and spreading disinformation. Moreover, the risk that the technologies that predict, track and trace the spread of virus infections could be manipulated by state and non-state actors cannot be discounted.

4. More generally, the accelerating pace of innovation and emerging and disruptive technologies (EDT) has the potential to seriously upend the global military balance. NATO therefore needs to address its eroding technological edge in the defence realm as a matter of urgency. The problem is all the more compelling because there is a risk that the COVID-19 crisis will divert attention – as well as financial resources - from the need to address this problem - and hence limit the necessary financial, intellectual, and managerial resources that need to be made available. Given the accelerating pace of innovation and the rapid spread of technology, maintaining the technological edge today and tomorrow is even more important for the transatlantic alliance than in the past.

5. For any innovation to be useful in the defence context it must above all translate into a tangible added military value. Such added value can express itself among other things through reduced costs, time or risk. However, probably most important for the achievement of military superiority will be gains in performance, efficiency, resilience, or agility.

6. This special report provides a brief overview of the challenges that the Alliance is facing on the defence innovation front and how member nations and NATO as an organisation have begun to tackle the issue. Your rapporteur also outlines some of the challenges Allies are facing in implementing innovation and presents ideas of how NATO could increase its value added to addressing these.

II. CHALLENGES TO NATO'S TECHNOLOGICAL EDGE

7. For decades, the military technology available to NATO forces has been superior to that of potential adversaries. For example, the West had a virtual monopoly on precision-guided weapons, signature-reduced platforms like stealth aircraft, and sophisticated intelligence, surveillance, and reconnaissance (ISR) assets. These technologies and their integration into a comprehensive battlefield networking system have been key aspects of NATO's military superiority. The Iraq wars of 1990 and 2003 probably represent the apex of Western, and particularly US, military dominance. US-led military forces defeated Iraq's large forces rapidly and with only few losses to themselves. However, Western military and technological dominance waned with the introduction of the "peace dividend", the dramatic cuts in defence spending after the end of the Cold War, and the new focus on counter-insurgency operations after 9-11.

A. INCREASED EFFORTS FROM NEAR-PEER COMPETITORS

8. In the meantime, other major powers, particularly Russia and the People's Republic of China (PRC), have invested heavily in their armed forces and developed capabilities that allow them to challenge NATO's technological edge. Among others, both China and Russia have pursued the development of advanced "anti-access/area denial" (A2/AD) air defence systems, thereby mitigating NATO air superiority. In a potential military conflict, they could thus impede reinforcing NATO Allies – for instance in the Baltic and the Black Sea regions, thereby putting pressure on NATO's Eastern Flank countries and Partner States in Europe or allow the PRC to block access to the Taiwan Strait and coerce the Republic of China (ROC or Taiwan). Russia and the PRC have also made great strides in developing new, potentially disruptive, military technologies such as hypersonic missiles. Recent Chinese advances in the field of quantum technologies could undermine the lead that the US and other NATO Allies have in stealth, encryption, high-performance computing, and numerous other technologies with military significance.

9. **The People's Republic of China** has made the transformation of the People's Liberation Army (PLA) into a high-tech force a top priority. Under President Xi Jingping a national strategy for "military-civilian fusion" (MCF) was launched in 2015 to incorporate defence innovation into China's overall innovation system. Guidance is provided through the Central Military-Civil Fusion Development Commission, chaired by Xi Jinping. A growing number of "joint cooperation and research partnerships" which are bringing together private business, the defence industry, academic institutions, and the Chinese military have already been established (Bendett and Kania, 2018). Concurrently, China is pursuing a national big data strategy pursuant to its focus on building a dynamic digital economy as well as for defence purposes.

10. The PRC's national security law also requires private companies to transfer novel technology to the government for military gain (Bavisotto, 2020). China has also allegedly circumvented NATO member countries' restrictions on foreign ownership of strategically relevant companies (Ford, 2020). Access to Western technology via joint ownership schemes or venture capital investments, including for technology start-ups, has enabled China to reverse engineer Western military technology. Moreover, China has been accused of stealing sensitive defence information and "sharing the information with its defence industry to incorporate the research and development into China's next generation of weapons platforms. This symbiotic relationship is allowing China to develop clones of some of the United States'

most critical weapons systems, including Lockheed Martin's F-22 Raptor and F-35 Joint Strike Fighters" (Ford, 2020). The monetary cost of the PRC's cyber espionage and intellectual property (IP) theft to the US industry alone is estimated at approximately USD 300 billion annually (Ford, 2020).

11. Beijing has made significant investments in robotics, swarming, and other applications enabled by artificial intelligence (AI) and machine learning (ML) (Kania, 2020). Chinese advances in defence innovation, particularly in the areas of automation and AI/ML-enabled weapons systems, could impact the global military balance and potentially exacerbate threats to global security and strategic stability (Kania, 2020). The PRC has also invested in C4ISR networks to coordinate its missile forces (Cropsey, 2020).

12. In **Russia**, the government under President Vladimir Putin has undertaken significant efforts to reduce the gap in military technology with the West. To that end, Moscow has given priority to start-up style disruption. The Russian Foundation for Advanced Research Projects, modelled after the US Defense Advanced Research Agency (DARPA), plays a central role in efforts to leverage cutting-edge developments in AI to ensure superiority in defence technology (Giridharadas, 2019). Although the Foundation has only a small budget of approximately EUR 61 million (Knight, 2019) it has been able to punch above its weight. Moscow also promotes AI through organising AI-related conferences, workshops and seminars and leverages AI-related innovation towards defence technology. Another focus of Russian innovation effort in the military realm is advanced robotics.

13. The brief Russia-Georgia war of 2008 showed the shortcomings of Russian military technology. It was an inflection point as this experience led the Kremlin to channel massive investments into the modernisation of the Russian armed forces (for more detail see the report of the NATO PA Defence and Security Committee on *Russian Military Modernisation : Challenges ahead for NATO Allies*). The creation of the Foundation for Advanced Research Projects of the Defence Industry was motivated by the desire to close the gap in advanced research with the West after more than twenty years of stagnation of the Russian military industry.

14. Given its relatively small R&D funds compared to NATO, Russia has achieved remarkable progress in its defence modernisation. However, past performance in military technology should not lead to an overestimation of what Russia is able to achieve today. Russia needs foreign buyers to be able to reach an economically viable scale of production.

15. Both China and Russia have advanced their defence innovation through a state-driven model. Industrial espionage and technology transfer have also been major enablers of their military modernisations.

16. To advance innovation in military technology both China and Russia are increasingly integrating their academic, industrial, and high-tech resources into a single, unified effort (Bendett and Kania, 2018). In addition to their national efforts to speed up innovation in the military realm, Russia and China are also cooperating in the development of dual-use technologies. Since 2015, both have concluded several agreements regarding technological cooperation. Moreover, the defence ministers agreed in September 2019 to jointly pursue military and military–technical cooperation (Bendett and Kania, 2019). Russia also apparently plans to aid China in developing a missile defence warning system, as President Vladimir Putin indicated in October 2019. This is a technology that is currently only fully operationalised by the United States and Russia (Bendett and Kania, 2019). Sino-Russian cooperation in

defence technology is likely to pose a considerable challenge for NATO Allies. For example, Russia provided valuable assistance for modernisation of the PRC's indigenous ship building capabilities. Moreover, the sale of Russian advanced destroyers, modern anti-ship cruise missiles and naval air defence systems was pivotal for the modernisation of the PLA's naval surface combat capabilities (Kendall-Taylor, Shulman, and McCormick,2020).

B. NON-STATE ACTORS

17. The widespread availability of modern technologies provides non-state actors with easy access to dual-use technologies that enables them to moderate the military-technological superiority of the Alliance. Non-state militants have been particularly adept at weaponising technology that is widely available commercially. For instance, militant non-state groups such as Daesh and Russian-backed illegally armed militants in eastern Ukraine have successfully weaponised drones intended for civilians (Raffey, 2017).

18. The experience made by the United States and other NATO Allies in Afghanistan and Iraq revealed that asymmetric warfare and the use of dual-use technology can diminish the advantage that superior technology gives to our forces. In both theatres of operations, insurgents have thus far been able to prevent Allied forces from translating their technological edge into strategic victory. At the height of its power, Daesh maintained an effective commercial drone fleet modified for reconnaissance and attacks. Additionally, since 2015, Houthi Rebels in Yemen have launched hundreds of drone and missile attacks against Saudi Arabia, with one such attack resulting in the temporary loss of more than half of total Saudi oil production.

19. Another example is precision-guided munitions (PGMs), a technology that was primarily developed for conventional state-on-state warfare and proved highly effective against the Iraqi army in the Persian Gulf War of 1991. However, PGMs were much less useful against militant insurgents who did not rely on massed armour (Locks, 2015). The larger implication of asymmetric warfare is that NATO countries are compelled to make simultaneous investments in technology designed for great power conflict, as well as technologies suited for low-intensity counter-insurgency military operations. A multitude of factors, including the complexity of modern warfare, the blurring of the line of warfare caused by cyberattacks, and the need to protect critical infrastructure require NATO Allies' continuous investment in technological innovation. As resources are limited and NATO nations are unlikely to simply outspend others in defence innovation (Murray, 2020) they need to improve cooperation in this area.

20. Of particular concern are scientific discoveries in synthetic biology and gene editing. These technologies offer powerful tools to potential adversaries, such as the People's Republic of Korea, to develop an arsenal of biological weapons. Moreover, synthetic biology and gene editing also evoke the spectre that non-state militants gain access to biological weapons. As such, any biological attack they may launch would likely use commercially available products, whose diffusion is difficult to monitor by the NATO defence establishment (Hammes, 2019). By contrast, nation states which are potential adversaries appear less likely to use such weapons both for fear of infecting their own populations and for inviting condemnation, or retaliation, from the world community. Nihilistic terrorist groups would not hesitate to unleash a man-made pandemic.

21. More generally, non-state actors have become more agile and can use inexpensive technology to an incredibly disruptive effect. They are increasingly capable of attacking

governments and private enterprises and undermine the credibility of our media, thereby debilitating the foundations of our democracy as well as our economies.

C. A CHANGING TECHNOLOGICAL ENVIRONMENT

22. Pressure on NATO's technological edge arises not only from near-peer competitors and non-state actors but also from the fact that the environment in which technological progress evolves has changed significantly. In the past, government-run military, and space programmes advanced technology. However, today it is the private sector that is the primary driver for innovation, including in the military sphere. The adaptation of commercial technology into the defence innovation process has therefore become increasingly important. If NATO nations' military forces want to maintain their technological edge, they must be able to quickly capture and integrate civilian innovation – and do this within a process appropriate to the military world.

23. The incorporation of new technologies generated by commercial industry therefore requires the adaptation and modernisation of management processes in the defence realm. The military procurement process is generally cumbersome and time-consuming, due to many bureaucratic layers and intrusive security screenings. These bureaucratic procedures encumber the cooperation between the military and fast-moving technology companies, especially start-ups (Olney, 2019). However, just like established, large defence companies, start-ups can play a pivotal role in in the Allied defence innovation ecosystem. Particularly start-ups, but also SMEs, are more inclined to develop disruptive technologies as this is the best way to succeed. Therefore, inclusion of smaller, fresh-thinking start-ups into NATO's innovation efforts would foster creativity, diversity, and more dynamic competition (Murray, 2020).

24. Rapidly shortening innovation cycles that render technology obsolete very quickly challenge the capacity of our military to keep pace. Another complicating factor is that the life cycles and timelines of commercial and military technology are often very different. Innovation cycles in the commercial world are often short and life cycles of products are limited to a few years. By contrast, the acquisition, introduction and use of equipment in the military area are longer-term projects. The procurement of military hardware is often an expensive and time-consuming process. The introduction of new equipment into the armed forces and the training of personnel takes considerable time and effort. For example, the lifetime of a civilian or dual innovation is four to six years; in the military world it may sometimes be 20 to 40 years. For example, the US Air Force is still using B-52 aircraft which were developed in the 1950s, and the French and German Air Forces are flying the Transall transport aircraft, which was conceived in the 1950s.

25. Because technological advances occur in the commercial field, it will be much more difficult to control, and if necessary, constrain the diffusion of these technologies. The proliferation of dual-use technology enables potential adversaries to reduce the technology gap towards NATO Allies. Dual-use technology also facilitates the proliferation of advanced technologies to non-state actors, including terrorist groups or criminal organisations. This is primarily due to the fact that the commercialisation of emerging technologies is reducing the financial, intellectual, and other barriers for them to obtain these technologies.

26. Against this backdrop it is vital for the Allies to discuss ways to develop a joint regulatory approach to control the proliferation of dual-use technology. A possible solution could be the (re-)establishment of a body that includes NATO Allies and like-minded countries that share

the same values as the Alliance. During the Cold War, this function was fulfilled by the informal Co-ordinating Committee (CoCom).

27. Promoting defence innovation in the Alliance is even more complex and challenging as the inherent characteristics of large, heterogeneous national military forces can be quite different. As an alliance comprising 30 member nations, NATO suffers from a “pacing gap" (Gojowsky et al, 2018). Hence, Alliance agility and interoperability remain one of the core objectives for the Alliance to pursue.

28. The “pacing gap” reflects the time between the introduction of a new technology and the establishment of laws, regulations, and oversight mechanisms for shaping its safe development. According to Wendell Wallach, modern technological innovation is occurring at an unprecedented pace which makes it harder than ever to govern using traditional legal and regulatory mechanisms (Gojowsky et al., 2018). If a new technology is proven successful by one country, the product still must be vetted by each country’s security and intelligence services. This process is time- and resource-consuming, which is a particular problem for poorer nations. Thus, this process exacerbates the pacing gap within NATO as standardisation becomes a protracted process of having to generate consensus among the member states. It could also create interoperability issues if some Allies would not dispose these new technologies (AI, autonomy, etc). This could result in practical operational interoperability concerns with direct impact on deterrence posturing.

29. In addition, there is also institutional resistance to innovation among NATO member states which is driven by the inherent characteristics of managing and maintaining a large, heterogeneous alliance among sovereign entities (Gojowsky et al, 2018). At the same time, NATO Allies have begun to undertake considerable efforts to advance defence innovation. The following chapter looks at the initiatives undertaken by key NATO Allies.

III. NATIONAL EFFORTS TO ENHANCE DEFENCE INNOVATION

30. In an alliance of sovereign states, the primary responsibility to maintain a robust defence S&T base and to discover, develop, and adopt cutting-edge defence technologies naturally lies with NATO member states themselves (NATO PA, 2018). The need to maintain, or regain if necessary, their edge in military technology has meanwhile been recognised by all NATO member states. Several Allies have established national defence innovation initiatives with the United States standing out for the sheer scale of its defence innovation efforts.[1] Moreover, the US defence innovation system has often served as an inspiration for other nations.

31. National initiatives of NATO Allies to advance innovation in the defence realm broadly fall into the following categories:

32. **Promoting the development of high-risk/high-payoff projects** that still stand at the earliest stage of the innovation cycle. The primary goal of this policy is to translate potentially revolutionary concepts and ideas into practical military capabilities. This approach has been pursued first by the Defense Advanced Research Projects Agency (DARPA) which was established in 1958. DARPA’s work not only advanced military capabilities such as stealth

[1] In 2017, the United States spent $55.4 billion on defence-related R&D, four times the combined R&D spending of the remaining OECD countries (Congressional Research Service, 2020b).

technology or precision weapons but also the precursor to the Internet, automated voice recognition, commercially viable GPS, unmanned aerial vehicles, touch screens, or infrared night vision technology (Congressional Research Service, 2020a; Mazzucato, 2013). Depending on their available funding, national initiatives generally seek to enable as broad a scope of innovative solutions as possible. Increasing agility is part and parcel of the defence innovation process here. For example, the Defence Innovation Unit (DIU) in the United Kingdom focuses on projects that achieve "initial operational use within three years" (UK MoD, 2018). The UK's Joint Forces Command's Innovation Hub (jHub) identifies promising mature technologies, assesses their viability in a one to six months pilot phase and then passes successful projects on for review to the JFC Innovation board. Investments are spread across a wide portfolio due to the high risk that any given pilot investment might fail (UK MoD, 2018).

33. **Finding new and innovative ways of utilising already existing weapons systems and military technologies.** This is a rather pragmatic way of using and modernising military hardware that is already available to armed forces. For example, the Strategic Capabilities Office (SCO) in the US is working to rebuild old US aircraft into "arsenal planes" that would serve as a kind of airborne magazine.

34. **Introducing innovations to the frontline military more quickly.** For example, the United Kingdom established the Defence and Security Accelerator (DASA), an innovation hub that seeks to "accelerate ideas from conception through to application" (UK MoD, 2018). DASA's focus is particularly on cooperation with Small and Medium-sized Enterprises (SMEs). It fulfils a broad selection of functions, including the identification of innovative solutions as well as support during development with expertise and finance. The US founded the Defence Innovation Unit (DIU) in 2015 which focuses primarily on AI, human systems, wider IT and space.

35. **Building and educating a network of innovators**. In the US, the National Security Innovation Network (NSIN), formerly Military District 5 (MD5), is mainly aimed at building and educating a network of innovators and equipping them with know-how and resources that enable them to develop and commercialise technology for the DoD. The DIU in the US engages with innovative organisations that do not traditionally work with the military to quickly adapt commercial products for military needs. In France, the Defence Innovation Agency (*l'Agence d'innovation de défense* – AID), established in 2018, both coordinates innovation activities in the MoD and serves as a point of contact for organisations outside of the traditional defence environment. For now, the focus of the agency is primarily on AI. However, the agency is also supposed to oversee the further development of the DGA LAB into a true Innovation Defence Lab. For example, while the bulk of the French *Direction Générale de l'armement* (DGA) R&D funding goes to national champions it also has a number of schemes and programmes to fund SMEs such as the RAPID (*Régime d'appui pour l'innovation duale*) and ASTRID (*Accompagnement spécifique des travaux de recherches et d'Innovation Défense*) that both support research in dual-use technology. Canada's "Innovation for Defence Excellence and Security" (IDEaS) programme allowed to build a network of more than 3,000 stakeholders during the first year of operation. IDEas includes all levels of government, industry, academia, and other actors.

36. **Creating "innovation hubs" and laboratories** that bring together think tanks, experts, start-ups and SMEs to generate new technology in the defence field. In France, the DGA has set up a DGA Lab which is run in collaboration with two private consulting companies CEIS and Sopra Steria. The Lab is supposed to provide a collaborative space for the military, academia, and industry to work together on common issues. Its activities include setting

challenges, exploring new uses for existing technology and showcasing new technology.

37. **Anticipating and identifying innovative trends that are relevant for the military.** The Innovation and Research InSight Unit (IRIS) located at the UK Ministry of Defence (MoD) is designed to anticipate emerging technology and innovation trends by drawing on insights from across "government, academia, industry and international partners" (UK MoD, 2018). Germany's current defence innovation focus is primarily focused on the cyber- and information space. The Cyber Innovation Hub (CIH) was founded in 2017 as a pilot project to serve as an "interface" between the start-up scene and the German armed forces. The key task of the CIH is to provide the German military with quicker access to digital innovations by scouting new ideas, testing and then developing them in concert with start-up companies in order to enable quicker access to digital innovations to the German military. However, the CIH is not solely focused on the technological aspect of innovation but is also supposed to make working methods and decision-making processes more agile. The most recent addition to the German defence innovation environment is the Agency for Innovation in Cybersecurity which is currently being established. The agency draws its inspiration from DARPA and will be jointly run by the German ministries of Defence and the Interior. It is designed to follow a long-term interdisciplinary approach in identifying disruptive innovations and awarding specific research contracts in strategic technological areas such as AI or quantum technologies.

38. **Making financial support available for start-ups and Small and Medium-sized Enterprises (SME)** interested in advancing innovation in the defence realm. NATO Allies are increasingly focusing efforts on SMEs and start-ups which often drive emerging and disruptive technologies. However, start-ups and SMEs are often reluctant to bid for government contracts due, among others, to a slow, bureaucratic process in obtaining funding.

39. Several NATO Allies have therefore set up mechanisms to address this problem. For example, Canada established the IDEaS programme in 2017 which commits Ottawa to invest the equivalent of USD 1.6 billion (USD 313 million in the first 5 years) until 2037. Canada has also established a Strategic Innovation Fund (SIF) with a budget of some USD 1.26 billion over five years and consolidates existing innovation programmes, thereby simplifying and accelerating bureaucratic procedures while also promoting a more results-oriented approach. In the UK, the Defence Innovation Fund is administered by a newly established Defence Innovation Unit (DIU) at the UK Ministry of Defence (MoD) and is supposed to invest approximately GBP 800 million (USD 1.04 billion) over a period of ten years. France set up Definvest, a fund tasked with investing USD 59 million in defence SME's with "potentially disruptive technology propositions"(Budden and Murray, 2019).

40. Several NATO member countries host an impressive array of defence innovation organisations. However, the concurrent existence of many innovation bodies risks making the defence innovation management "somewhat haphazard" (Nimmons, 2019). To remedy this problem several member nations have introduced organisational changes to ensure coherence of innovation approaches in the military realm. For example, Germany set up an "Agency for Innovation in Cybersecurity" under the leadership of the MoD and the Interior Ministry which has the task of stimulating, funding, and coordinating research on cybersecurity issues.

IV. DEFENCE INNOVATION – THE ROLE OF NATO

41. According to the political economist Joseph Schumpeter, “Innovation is the creation of new combinations that represent a departure from established practices” (Gojowsky et al., 2018). In a very general sense, innovation can be defined as gaining value from the exploitation of novelty. However, this does not just encompass new technologies. Innovations can also emerge from the “product, process, market, organisation or operation” areas. Therefore, even the application of existing “concepts, processes and technologies” to the defence sector in novel ways can be defined as defence innovations. In other words, NATO needs to undergo both sustained and disruptive innovation at the same time.

42. As noted in the previous chapter, the primary responsibility for defence innovation lies with the member states of the Alliance. Nevertheless, NATO as an organisation adds significant value to national efforts, among others via the identification of common risks and common opportunities and via the diffusion of knowledge and expertise as well as through concrete cost-effective S&T/R&D efforts to inform inter alia capability development, standards, and interoperability at an early stage.

43. Scientific and technological cooperation has been part and parcel of the Alliance since its beginning. Thus, over seven decades NATO has been able to build an impressive network of commands, institutions and other entities dedicated to advance military technology in support of the Alliance’s strategic objectives.

44. Defence innovation goes obviously beyond a singular focus on technological innovation. Innovation in the defence realm is much more comprehensive and includes technological, procedural, and institutional innovations.

45. Within NATO, defence technological innovation is largely driven in the Science and Technology Organization (STO), by Allied and Partner Nations, and by customers such as Allied Command Transformation (ACT). The STO supports the defence and security posture of the Alliance and its partners through scientific and technological research.

46. Regarding institutional innovation, Allies have decided in 2017 to overhaul the Command Structure as they recognise that the threats posed by potential adversaries are evolving constantly. Moreover, as a result of the latest NATO HQ Functional Review, the Allies established NATO’s Innovation Unit (IU), which has been tasked to be the focal point of innovation at NATO HQ, and the Innovation Board (IVB). The IVB, which is chaired by the NATO Deputy Secretary General, is not a decision taking Committee in which the Allied Nations are represented, like, for example, the Military Committee (MC). Rather, it enables NATO staff to better understand the implications of new technologies and innovation.

47. The IVB is composed of NATO senior staff. Major players include the two Strategic Commands (Allied Command Transformation and Allied Command Operations), Chair MC, NATO Chief Scientist and the Assistant Secretary Generals for Emerging Security Challenges, Defence Investment, as well as DPP & Operations and Public Diplomacy. The IVB is supported by the Innovation Task Force which brings together NATO staff officers. Major players include ACT Innovation Laboratory, ESC Innovation Unit, STO (OCS, CSO, CMRE), NCIA, Defence Investment and Defence Planning & Policy.

48. Moreover, the IVB has an important staff coordination role within NATO. Focus areas of the IVB’s work include capability and warfare development, strategic level implications of

technological innovation, foster adoption of innovation within the Alliance, maritime research, and experimentation, emerging and disruptive technologies, and rapid prototyping (minimum viable products). The IU is to be the focal point for Innovation within NATO Headquarters with the task of creating the right environment so that innovation can flourish across the entire NATO enterprise. The IU's work ranges from writing white papers on new technologies, to adapting policies to embrace new ways of thinking, to undertaking innovation experiments alongside ACT that can inform wider policy thinking. In addition, the IU is also building the NATO Innovation network comprising of Allies, along with private sector start-ups, accelerators, incubators, finance professionals and universities. The aim is to create an environment where Allies can quickly adopt emerging technologies and focus on mission-oriented investment for future technologies.

49. Allied Command Transformation (ACT), headquartered in Norfolk, Virginia (United States), is NATO's "leading agent on innovation". It plays a pivotal role in advancing defence innovation and is tasked with the transformation of NATO's military structures, forces, capabilities, and doctrines to enable the Alliance to meet its level of ambition and fulfil its core missions. ACT's priorities in the realm of defence innovation are focusing on the development of an emerging disruptive technology roadmap, among others.

50. To advance defence innovation, ACT has established an innovation branch as well as the NATO Innovation Hub within its Capability Development directorate. The Hub is currently being developed into a "laboratory" that is capable of independent prototyping and incremental innovation but can also serve as a platform for open innovation. The Hub essentially seeks to build a NATO Innovation Network consisting of end users, providers, and capability designers to solve common challenges. End users (NATO, national militaries) express their operational needs, providers (experts from academia, industry etc.) contribute knowledge and capability designers (NATO and national personnel) translate the providers' contribution into solutions which meet the needs of the end users.

51. This open innovation process is explicitly not just limited to experts or practitioners but also seeks to engage the wider public, through e.g. dedicated online platforms, to come up with solutions. While such an approach obviously has its limitations due to security concerns, it could also help raise societal acceptance for dual-use research within the Alliance by directly engaging the public.

52. As NATO Allies already pursue national efforts to build innovation networks and include non-traditional stakeholders, NATO as an organisation can concentrate on becoming an innovation hub as a platform for the sharing of information, experiences, best practices, and concepts. In a similar fashion, ACT could build on its experience to advise NATO members how their innovation initiatives relate to the evolving defence innovation ecosystem of NATO and its other members. This allows the identification and exploitation of potential synergies and the creation of new initiatives that can generate added value. Cooperation and coordination of defence innovation initiatives on the NATO level can also prevent individual member nations from spreading their limited resources too thin.

V. ACHIEVEMENTS AND CHALLENGES

53. Having realised that their technological edge is eroding rapidly, NATO nations have begun to focus on accelerating innovation in the defence realm. Both on a national and on the Alliance level significant strides have been made making innovation efforts more effective, affordable, and coherent.

54. Efforts that aim to advance defence innovation in the technological realm broadly focus on potentially revolutionary concepts and ideas and translate these into practical military capabilities. Allies also generally recognise the need to concentrate on the development of high-risk/high-payoff projects which are at an early stage of the innovation cycle. Other aspects of defence innovation aspire to find new and innovate ways of utilising already existing weapons systems and military technologies and on getting innovations to the military more quickly.

55. There is also a general trend to utilise commercial and open-source innovation and adapt this into the military realm. To that end NATO nation states and the NATO STO are establishing and expanding networks of innovators which do not traditionally work with the military to develop technology or adapt available commercial technology for military needs. Building up more talent and training as an underlying factor for innovation has also been recognised as a priority to advance defence innovation. A tool that has been used successfully to attract particularly Small and Medium-sized enterprises and young researchers are innovation competitions for concrete security challenges. Several NATO Allies have also begun to devise flexible new procurement mechanisms. However, despite the improvements achieved there is still a need to develop more efficient, timely and streamlined processes.

56. NATO has already taken many positive steps recently and is actively working to take further ones, such as the adoption of an Emerging and Disruptive Technologies (EDT) implementation strategy including scoping the various NATO S&T Programmes of Work. Beyond that, NATO's Strategic Commands have provided initial recommendations on how to adapt NATO's capability development processes to gain more agility. The Innovation Board is also tasked by the North Atlantic Council to identify and bring to the attention of Allies policies that need updating so as to enable innovation. An increase of CD&E efforts to identify promising innovation areas and operational experimentation is necessary.

57. While coordination within NATO has considerably increased, the S&T community still faces a number of challenges. These primarily occur in coordination across the community, lack of resources to actually encourage innovation, and the introduction and application of innovation in Allied nations' armed forces as well as in the national government organisations or in the knowledge base (e.g. defence labs, defence industry). NATO Allies cannot afford to ignore these shortcomings lest they are prepared to put the lives of their soldiers and populations at peril.

58. Allied and Partner Nations mainly drive innovation themselves (they are not in the Innovation Board) and share some of their findings with and within NATO. However, due to the often-sensitive nature of military innovation, members are reluctant to publicly share organisation principles, release capability targets or details on what they are currently working on. One of the laudable exceptions within the NATO innovation network is the US Air Force's AFWERX, which has published a detailed report on how to build a successful environment for defence innovation. Based on their own experience, AFWERX has developed among other things the so-called WATER organisational principles for innovation success:

Warfighter-focused, Agile, True-to-our-Core, Empowered Talent, Relationship-Building. Although such a level of detail may not be necessary for the purpose of building a common framework that could guide national efforts of the Allies, it would be very helpful if more of the Alliance's many innovation institutions were to release similar publications.

59. Increasing the exchange of information and best practices need not necessarily be strictly limited to the members of NATO but could also be extended to our closest Partners like Japan, Australia, Israel, Ukraine, Georgia, or, most importantly, the European Union (EU). Currently, NATO and the EU share 21 members and face similar challenges, making them obvious partners. Enhanced coordination is made even more significant by the EU's growing defence integration initiatives such as the Permanent Structured Cooperation (PESCO), the Coordinated Annual Review on Defence (CARD), the European Defence Fund (EDF) and the newly established Directorate-General for Defence Industry and Space (DG DEFIS) (for more detail on the EU initiatives see the report of the Political Committee of the NATO PA The NATO-EU partnership in a changing global context). The two entities already engage in several ongoing efforts to ensure coherence as well as transparency on the one hand and avoid duplication or decoupling on the other. Nevertheless, coordination is hampered by the absence of a channel to share classified information. Thus, the creation of such a channel could be a promising avenue to enhance EU-NATO cooperation in the field of defence innovation.

60. Yet, both on the EU-NATO and the transatlantic level it is often not interinstitutional relations that have proven to be the biggest stumbling block for greater cooperation, but rather defence-industrial considerations. For example, the EU's PESCO and the EDF have heightened suspicion that they could be used to exclude non-EU members from joint defence research and capability development. In the end, mutual recriminations about the openness of defence markets and discriminatory behaviour add nothing to NATO's common military capability. Instead, the current disagreement should serve as a motivator to build a truly transatlantic market for defence procurement, but also defence innovation. This is of particular importance as national defence innovation systems may link the goal of increasing the capabilities of the Armed Forces with the promotion of the development of the defence industry "as part of a broader industrial policy" (Budden and Murray, 2019). In the current political climate, this may appear to be a rather ambitious goal, but such a common market would entail enormous potential benefits. In fact, there are several low-hanging fruits that could strengthen transatlantic cooperation considerably. Such an agreement would facilitate the identification of common priorities and capability gaps and perhaps even pave the way for future regulatory alignment. This will, of course, be a complicated undertaking, but ultimately only transatlantic unity will be able to maintain NATO's military innovation edge.

61. Another area where NATO Allies need to improve cooperation is the monitoring and mitigation of technology transfer and collaborative research activities. Near-peer countries but also criminal groups are increasingly engaged in Intellectual Property (IP) theft and extra-legal activities. Cooperation among NATO Allies and partners could include expanding information sharing mechanisms. In addition, close joint action of Allies and Partners to thwart IP and cyber espionage and, if necessary, sanction the perpetrators will be needed to protect our IP and defend critical infrastructure.

62. In contrast to near-peer competitors like Russia and China, which have a state-driven, top-down innovation approach, the current model that NATO Allies pursue for defence innovation looks at the commercial sector as the engine of innovation for science and in defence. However, commercial companies are reluctant to invest in defence technology or in

high-risk, early-stage research which is less likely to lead to viable commercial applications. While start-ups and SMEs may generally be more willing to take risks, they often lack the financial resources to do so. A perennial issue is the gap between the development of an innovative product and the introduction of new technology into the national armed forces, the so-called “valley of death”. Therefore, government funding for R&D remains vital to facilitate and encourage the participation of start-ups and SMEs in the defence innovation process.

63. As governments have to invest considerable amounts of financial resources to tackle the COVID-19 crisis, there are reasons for serious concern that defence spending, including outlays for defence R&D, will decline (Barry et al, 2020). However, as military innovation “is emerging as a new frontier for great power rivalry” (Kania, 2018) we cannot allow NATO’s technological advantage to disappear. Therefore, we must invest in the ability to quickly spot, adopt and leverage promising technologies before our competitors do.

64. Government resources should be directed towards helping with the adaptation of dual-use technologies for our militaries and towards technologies which are genuinely for military use as commercial companies are unlikely to invest in them. For example, stealth technology is fundamentally a military technology, while civilian aircraft need to be spotted easily for safety reasons.

65. Another impediment to the deeper integration of commercial and defence technologies is negative public perception of defence technologies. A case in point is Google’s withdrawal from project “Maven”, a US Department of Defense programme that uses machine learning to recognise objects from moving or still imagery. Google withdrew from the programme after company employees wrote an open letter signed by more than 3,000 workers that they did not want to “build warfare technology” (Lynch, 2018). Governments therefore need to improve the effectiveness of their communication strategy and better explain why our military forces are of pivotal importance for our security and why they need the best and most modern equipment. It is necessary to reach out to the public, and particularly researchers and employees of technology firms, and build and increase the understanding and acceptance of the need to have defence technology.

66. While technological innovation is a source of promise and productivity, there is also widespread concern that technological development is a juggernaut beyond human control. There are profound ethical and governance concerns posed by emerging technologies which need to be addressed. Parliaments will play an important role in the necessary public discourse on the societal impact and risks posed by innovative tools and techniques, and in agreeing on legal, and possibly also ethical, standards. The issue is relevant as technology companies can see employees engage in protests when a company contracts with the government on AI-driven military missions or in privacy issues that could potentially threaten human rights. If unaddressed, technology firms working in the defence field may also find it difficult to attract top talent – which is of particular importance because these companies often compete from a small pool of experts.

67. The greatest competitive advantages of NATO member states are the vitality and openness of their innovation ecosystem, which has allowed the West to attract talent from throughout the world. However, there are still bureaucratic tendencies, such as the dilution of responsibilities, inertia, slowness, excessive size, and unmanageable organisations, which hamper progress in defence innovation.

68. Finally, it is important to note that defence innovation is not only about technological innovation but also encompasses the way the Alliance “thinks” about war and military conflict. There is a need to develop our strategic thought as technological progress and other factors, including emerging powers, are changing the character of conflict and war. Among peer competitors Russia and China have continued to develop their strategic thought for years and adapted their capabilities to compensate for their, thus far, military, and technological inferiority to NATO. As one commentator noted “Potential adversaries … have reconceptualized warfare and reimagined conflict without the boundaries the West imposes upon it” (Roberts, 2017). In addition to monitoring recurring Allied defence policy reviews Moscow and Beijing also analyse NATO member nations’ political will to implement their defence investment pledge and to muster public support for their defence policies. Your rapporteur therefore wants to stress the importance of resisting reducing defence budgets in the post-COVID-19 era but instead developing recovery plans that maintain defence spending at current levels.

VI. CONCLUSIONS

69. NATO Allies have recognised the need to modernise and strengthen their defence innovation networks. Good progress has been made with regard to the promotion of innovation in the defence sector. However, the Allies cannot afford to rest on their laurels as they find themselves in a competition with potential adversaries like Russia or China.

70. In addition to national efforts, NATO’s S&T network remains of critical importance to maintaining the S&T edge in the Alliance. It adds significant value to the defence innovation efforts of individual Allied nations, in addition to expanding Allies’ access to a network beyond their national borders, NATO’s S&T network also promotes coherence, collaboration, economy of scale, and efficiency of national efforts. Moreover, it is an important factor for burden sharing, capacity building, interoperability, and standardisation.

71. The need to agree on innovation priorities which allow to better channel government resources and attract private sector investment of NATO Allies is evident. Here, too, NATO is engaged in valuable and constructive initiatives. For example, STO’s Science and Technology Trends 2020-2040 identify the technologies which are likely to impact the security of NATO member nations. ACT’s Emerging and Disruptive Technologies roadmap, together with the NATO Secretary General’s Advisory Group on Emerging and Disruptive Technologies can also offer guidance to NATO member nations. In this context, your rapporteur wants to mention that the group of 12 external experts presented their recommendations on innovative technologies that NATO should be pursuing as a priority in late September 2020 (NATO, 2020).

72. More generally, NATO Allies need to enhance the NATO S&T network by developing a more strategic planning S&T approach and fostering an agile, innovative and risk-tolerant mindset through, inter alia, sharing best practices across the NATO S&T community; and particularly by exploring financial tools for ‘seed money’ in support of technology demonstrations and rapid studies. As Allies’ commitment to increase defence spending to 2% of GDP is under pressure because of the COVID-19 crisis there is the additional need to resource the 2019 NATO Military Strategy, NATO Defence Planning Process capability targets and emerging disruptive technologies. Therefore, Allies have to be more creative and imaginative in leveraging financial tools to achieve all of this.

73. Collaboration should include coordination of technology export controls, screening of investments, IP theft, and restrictions against collaboration with military-linked or otherwise problematic institutions in China, Russia, and other potential adversaries. More generally, to prevent the proliferation of sophisticated military and dual-use technology the Allies could consider establishing a body at NATO HQ to function as a clearing house for technology exports. Moreover, it is critical to improve cooperation and coordination on policy responses to the challenges and opportunities that emerging technologies present. For instance, improvements in sharing data among Allies and partners could be conducive to advancing the future development of AI in a manner that is consistent with our ethics and values. The fact that several Allies, such as the United States, are looking into the ethical and legal implications of AI in warfare is a step forward.

74. Though other countries, and China in particular, have become very successful in introducing new technologies, NATO nations are, on aggregate, second to none in research and technology. Therefore, they find themselves not in a technology race, but in a technology adoption race. Bridging the gap between science and applications, while speeding up the technology adaptation process is paramount to improve the defence innovation process. This requires improvements in the way NATO militaries scan, adopt, and measure innovation.

75. Therefore, seeking to emulate a top-down technological innovation process, similar to Russia’s or China’s approach, would, in the view of your rapporteur, be a missed opportunity for NATO Allies. Instead, NATO Allies should pursue a “blended” approach, one that uses the strengths of our free societies but with both national and alliance vision and strategic direction from the top. NATO should leverage the traditional strengths of free societies such as tolerance for independent decision-making, room for the power of individual creativity and free enterprise. Thus, Allies should strengthen efforts to co-opt their civilian innovation ecosystems and reform their defence innovation process according to the best practices established by the commercial world. That said, reforming the defence innovation process merely according to "commercial best practices" would be fraught with too much risk as commercial entities, in their desire for speed to market and lowest cost, tend to overlook or downplay potential risks to our critical infrastructure.

76. Successful defence innovation requires a profound cultural change of all defence stakeholders, who must accept and integrate a smart risk-taking culture as it is crucial to enable innovation in defence and to adapt and absorb civilian innovation. To that end, NATO member nations should also share best practices to facilitate the participation of SMEs and start-ups in the defence procurement process.

77. Moreover, the Allies should also seek synergies of their efforts to maximise impact and economy of scale. To that end, member states should continue to support developing and utilising the NATO S&T Programmes database.

78. NATO member states have undeniably made great strides towards improving defence innovation. However, we need to intensify our efforts to regain the technological edge and prevent losing focus. It will require continued, and ideally increased financial, intellectual, and managerial investment into defence innovation lest the Allies want to risk the progress achieved. We must not allow this to happen. The COVID-19 pandemic and the aftermath of this crisis have a significant impact on the political and financial situation in all member states which will likely increase demands to lower defence budgets. However, the threats to our security are increasing, not decreasing and we cannot afford to repeat past mistakes. Weakening our defence only emboldens and empowers our enemies. Investment in defence

innovation is therefore of crucial importance – and it is comparatively cheap and can reap great benefits. Key areas of improvement remain, in the view of your rapporteur, the financing of SMEs and start-ups and the IP protection against cyber espionage. The former is a low-hanging fruit, as the required financial investments in high-risk defence research by SMEs and start-ups are small in comparison with the protection they provide against cyber espionage and other threats that would serve our collective security, our economies and societies overall.

SELECTED BIBLIOGRAPHY

Barry, Douglas, Childs, Nick, McGerty Fenella, *Government spending and plans: Will the Pandemic Take its Toll?*, IISS Military Balance Blog, 1 April 2020,

Bavisotto, Jenny, *China's Military-Civil Fusion Strategy Poses Risk to National Security*, US Department of State, 2020.

Bendett, Samuel, Kania, Elsa B., *Chinese and Russian Defense Innovation, with American Characteristics? Military Innovation, Commercial Technologies, and Great Power Competition*, RealClear Defense 2 August 2018.

Bendett, Samuel, Kania, Elsa B., *A new Sino-Russia High-tech Partnership*, Australian Strategic Policy Institute, Policy Brief 22/19, November 2019.

Budden, Phil, Murray, Fiona, *Defense Innovation Report: Applying MIT's Innovation Ecosystem&Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis*, MIT Lab for Innovation Science and Policy, May 2019.

Congressional Research Service, *Defense Advanced Research Projects Agency: Overview and Issues for Congress,* 2020a.

Congressional Research Service, *Government Expenditures on Defense Research and Development by the United States and Other OECD Countries: Fact Sheet*, 2020b.

Cropsey, Seth, *The Pentagon must not falter in its drive to network its weapons and sensors*, Defense One, 19 June 2020.

Du Cluzel, François, *How NATO is innovating towards the Future*, The Cipher Brief, 14 May 2020.

Ennis, Henry, Estevez, Alan, Mariani, Joe, Moran, Jessica, Pauloski, Joe, *National Security and Technology Regulation*, Deloitte Insights, 12 July 2019.

Fitt, Joshua, FitzGerald, Ben, Lee, Kristine, Kliman, Daniel, *Forging an Alliance Innovation Base*, Center for a New American Security, March 2020.

Ford, Christopher Ashley, *Preventing U.S. Industry's Exploitation by China's "Military-Civil Fusion" Strategy, US Department of State*, 2020.

Giridharadas, Akshobh, *Russia's Military Is Transforming (And Getting Stronger) Right Before Our Eyes*, National Interest, 2019

Gojowsky, Torsten, Koegler, Sebastian, Haspels, Bernardus, Haar, Flemming, Wetteland, Sverre, *Resistance to Innovation in NATO*, The Strategybridge, 16 August 2018.

Government of Canada, *Strategic Innovation Fund*.

Government of Canada, *2018-2019 Annual report – Innovation for Defence Excellence and Security program*.

Haas, Michael, *The Eclipse of Western Military-Technological Superiority*, in "Strategic Trends 2019", Thompson, Jack and Thränert, Oliver (eds), Center for Security Studies ETH Zürich, 2019.

Hammes, T. X., *Technology Converges; Non-State Actors Benefit,* Hoover Institution, 2019.

Jones, Jeff, *Confronting China's Efforts to Steal Defense Information*, Belfer Center, May 2020

Kania, Elsa B., *'AI Weapons' in China's Military Innovation*, Brookings Global China, April 2020.

Kania, Elsa B., *Innovation in the New Era of Chinese Military Power*, The Diplomat, 25 July 2019.

Kania, Elsa B., *Strategic Innovation and Great Power Competition*, The Strategybridge.org, 31 January 2018.

Kendall-Taylor, Andrea, Shulman, David, McCormick, Dan, *Navigating Sino-Russian Defense Cooperation*, War on the Rocks, 5 August 2020.

Knight, James, *Current Challenges of Defense Innovation in France and in Europe*, Open Innovation, 4 April 2019.

Locks, Benjamin, *Bad Guys Know What Works: Asymmetric Warfare and the Third Offset*, War on the Rocks, 2015.

Lynch, Justin, *Why Project Maven is a 'Moral Hazard for Google'*, C4ISRNet, 28 June 2018.

Murray, Rob, *Building a resilient Innovation Pipeline for the Alliance*, NATO Review, 1 September 2020.

Raffey, Nick, *Cheap and Effective: the Weaponization of Commercial Drones on the Battlefield*, NATO Association of Canada, 2017.

Roberts, Peter, *Designing Conceptual Failure in Warfare*, RUSI Journal, Vol. 162 3 April 2017.

Matelly, Sylvie, *Defense Innovation and the Future of Transatlantic Strategic Superiority: A French Perspective*, German Marshall Fund of the United States Policy Brief, 9 April 2018.

Mazzucato, Mariana, *State of innovation: Busting the private-sector myth*, New Scientist, 2013.

Mölling, Christian, *Defense Innovation and the Future of Transatlantic Strategic Superiority: A German Perspective*, German Marshall Fund of the United States Policy Brief, 23 March 2018.

NATO, Allied Command Transformation, *Innovation at the Centre of Allied Command Transformation's Efforts*, 8 May 2019.

NATO, *Alliance's future Innovation priorities discussed in High-level Meeting*, 1 October 2020.

NATO PA, *Maintaining The Edge and Enhancing Alliance Agility*, STC Special Report, presented by Leona Alleslev (Canada), 2018.

Nimmons, Steve, *Innovation and technological superiority in UK defence*, February 2019.

Olney, Rachel, *The Rift Between Silicon Valley and the Pentagon Is Economic, Not Moral*, War on the Rocks, 28 January 2019.

Tirpak, John A., *The Chinese Air Force's Great Leap Forward*, Air Force Magazine, 29 May 2018.

United Kingdom Ministry of Defence, *Ministry of Defence Annual Report and Accounts 2018–19*.

United Kingdom Ministry of Defence, *Advantage Through Innovation: The Defence Innovation Initiative.*