No. 33
April 2022

NATO Defense College

The College Series

How are Emerging and Disruptive Technologies affecting NATO's core tasks?

by
SC139 COMMITTEE 8

www.ndc.nato.int

NATO DEFENSE COLLEGE

The College Series - No. 33

How are Emerging and Disruptive Technologies affecting NATO's core tasks?

Senior Course 139 - Committee 8

LTC	Cool (Chairperson)
First Sec.	Erongun (Secretary)
CDR	Dzieciuch
MAJ.	Giorgino
MS	Grout
LTC	Konjar
LTC	Lago
COL	Leiwig
COL	Mlakic
CDR	Ozden
LTC	Rohen

Faculty Adviser: COL Jan Østrup-Møller
Academic Mentor: Dr Andrea Gilli
NATO Sponsor: MGEN. (Ret.) Philippe Montocchio

Each paper in this College Series is the main research assignment by a Course Member or Committee of the NDC Senior Course.

This paper was the Committee Study Project awarded the Eisenhower Prize for Senior Course 139.

Faculty Adviser for this Committee Study Project: COL Jan Østrup-Møller (DNK)
Mentor: Dr Andrea Gilli

The paper is published by the NATO Defense College in its original form (English editing: Peter Mead).

NATO Defense College, Rome, 2022.

Introduction: a new strategic environment

With regard to Emerging and Disruptive Technologies (EDTs), the "NATO 2030: United for a New Era" Reflection Group Report states: "EDTs pose a fundamental challenge but also – if harnessed correctly – an opportunity for the Alliance. Without a strategic surge in this area, allowing adversaries to gain competitive advantage would impede NATO's ability to win on the battlefield, challenge strategic stability and change the fundamentals of deterrence [...] They also could undermine NATO's political cohesion, by raising questions about technology sharing within the Alliance, impairing interoperability, and potentially fueling dependencies on rival states."[1]

Just as the invention of the airplane transformed civilization while opening a new domain of warfare, and the innovation of the tank revolutionized ground maneuver capabilities and tactics, EDTs are having the same profound impact across societies and reshaping activities throughout the spectrum of conflict. The security of NATO Allies is founded on political bonds (specifically Articles 4 and 5) and military capabilities (the Alliance's nuclear and conventional posture). However, rapidly advancing, commercially driven technologies are undermining both, either because they are blurring the distinction between peace and war or because they have the capacity to offset existing force structures.

EDTs have created a 'Technology Flank' for NATO that is currently exposed and raises significant risk to the Alliance's collective defense. In a new multi-domain warfare environment, gaining superiority in EDTs is also a significant opportunity for NATO to address both state and non-state threats. So, how do the dramatic change in the nature of the security environment and further ramifications of the new types of warfare impact the conduct of NATO's core tasks?

Definitions of EDTs vary. This paper will focus on four of the seven[2] identified in the 'NATO Advisory Group on EDTs' report that we identified as game changers, and investigate how these may affect core tasks. Finally, the paper provides eleven recommendations for the future, *inter alia* with a view to the next Strategic Concept.

Emerging and Disruptive Technologies: 'game changers'

Artificial intelligence

Russian President Vladimir Putin's much publicized declaration that the leader of artificial intelligence (AI) will rule the world,[3] warnings by experts that China has won the AI battle against the United States,[4] and other events have prompted NATO leaders to identify AI as a high priority.[5] The promise of AI stems from its general-purpose nature; like the steam engine or

---

1 NATO, *NATO 2030: United for a New Era*. 25 November 2020, https://www.nato.int/nato-static-fl2014/assests/pdf/2020/12/pdf/20121-Reflection-Group-Final-Report-Uni.pdf (accessed 1 November 2021).

2 NATO's seven key areas regarding EDTs include: artificial intelligence, data and computing, autonomy, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space.

3 CNBC.com, "Putin: Leader in artificial intelligence will rule the world," 4 September 2017. https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html (accessed 1 November 2021).

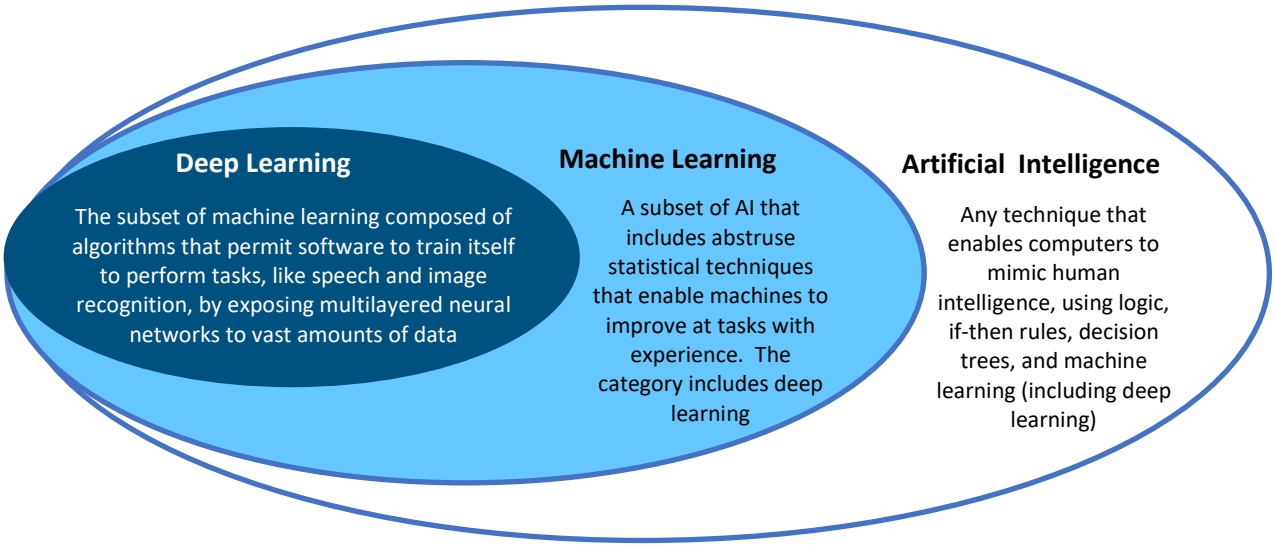
4 Reuters.com, "China has won AI battle with U.S., Pentagon's ex-software chief says," 11 October 2021, https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/ (accessed 1 November 2021).

5 China's *Next Generation AI Development Plan* (July 2017) and Russia's *Decree of the President of the Russian Federation on the Development of AI in the Russian Federation* (Oct 2019) are published open-source documents that give greater detail on their strategic priorities and focus areas. Many NATO published documents and communiqués have expressed the importance of AI technologies, such as the *NATO 2030: United for a New Era* Reflection Group Report, the unclassified *Summary of the NATO AI Strategy*, and the *Annual Report 2020* of the NATO Advisory Group on EDTs. Additionally, NATO's "Brussels Summit Communiqué" (June 14, 2021) indicates, in Section 6.d, the agreement by Heads of State to "foster technological cooperation among Allies in NATO, promote interoperability and encourage the development and adoption of technological solutions to address our military needs …," and the establishment of

electricity, it is touted as capable of leading to a major technological revolution that will affect the distribution of wealth and power among countries (see Figure 1).

Initial areas of opportunity to apply AI technologies include intelligence, operational, and logistical functions, so as to inform faster, more effective decision-making. Analysis of target population social media trends can enable and execute strategic messaging operations within a shorter timeframe. Enabling deeper examination of maintenance programs and operational plans, AI can identify ideal logistical nodes, better determine the amount of resources required, and provide cost-effective repair solutions.[6] Making all this information available provides a more thorough analysis process across multiple domains of warfare, to better guide planning, decision-making, and operational execution, creating both a threat from adversaries and an opportunity to strengthen the Alliance.

Figure 1. AI vs. Machine Learning vs. Deep Learning[7]



Hypersonic weapons

Hypersonic weapon systems are considered to be the greatest advance in missile technology in the last ten years, and a game changer for NATO air defense capabilities (see Figure 2). Until recently, the Armed Forces relied on ballistic missiles and cruise missiles, most of which reach supersonic speeds. Ballistic missiles, while fast, move like a projectile on a predictable trajectory. Cruise missiles are more precise, but slower. Hypersonic systems combine the advantages of both ballistic and cruise missiles: speed and precision.

Of particular importance is maneuverability in the final approach, which according to current assessments could breach all NATO missile and air defense systems. The sheer speed of these weapons creates problems for sensor and interceptor systems, significantly reducing the

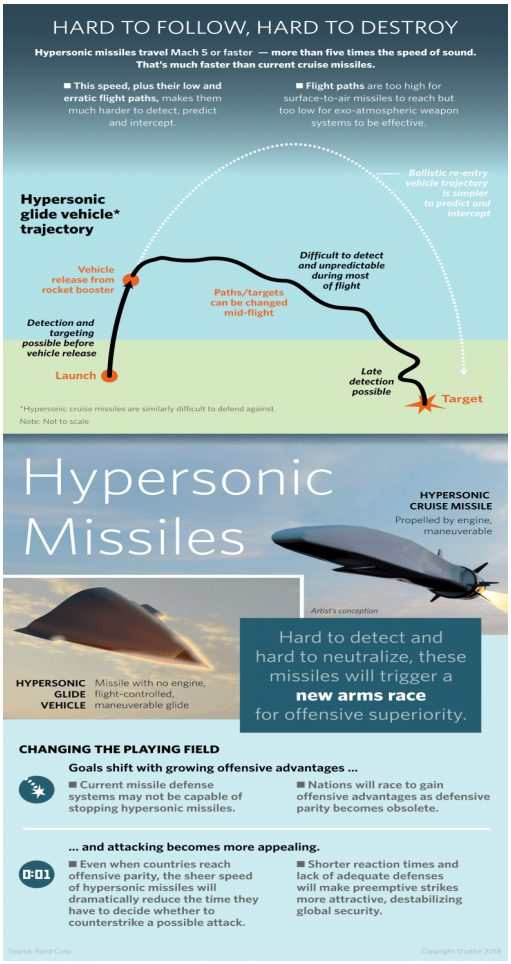
DIANA and the NATO Innovation Fund to support start-ups working on dual-use emerging and disruptive technologies.

[6] M.L. Cummings, Heather M. Roff, Kenneth Cukier, Jacob Parakilas, and Hannah Bryce, "Artificial Intelligence and International Affairs: Disruption Anticipated," Chatham House Report, 14 June 2018, p. 25. https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf

[7] Image from Gowthami Rasanayagam, "AI vs. Machine Learning vs. Deep Learning," Medium, 21 September 2021, https://medium.com/nerd-for-tech/ai-vs-machine-learning-vs-deep-learning-60b3d0611fe9 (accessed 19 November 2021).

reaction time to initiate appropriate defensive countermeasures. Now within technological reach, this emerging capability wields strategic effect and requires a political solution.

Figure 2. Hypersonic Weapons[8]



Autonomous systems

As autonomous systems enabled by other technologies such as AI evolve, so too will the conduct of warfare. Use of autonomous systems is appealing for several reasons: 1) they reduce personal exposure to danger; 2) they enable conduct of operations in degraded environments at a reduced cost; 3) they mitigate probability of human error; and 4) they are not constrained by human limitations. Employment of many systems in a swarm technique has the effect of overwhelming enemy defenses; use of AI-enabled data analytics shortens decision-making cycles to accelerate response actions, resulting in warfare being conducted at a faster pace and on a more impersonal level than ever before.

Autonomous system advances have caused three main concerns in relation to the conduct of NATO's core tasks. First, the increasing ability of conducting more and more tasks without a 'human in the loop' has raised operational, legal, and ethical concerns in an international system without established norms. Second, autonomous system capability development is uneven across NATO's thirty member nations, creating a lack of interoperability and common standards within the Alliance. Third, research and development in autonomous systems and software is occurring

[8] Image taken from RANE Worldview, "Explaining the Hype Around Hypersonic Weapons." 6 January 2018. https://worldview.stratfor.com/article/explaining-hype-around-hypersonic-weapons (accessed 31 December 2021).

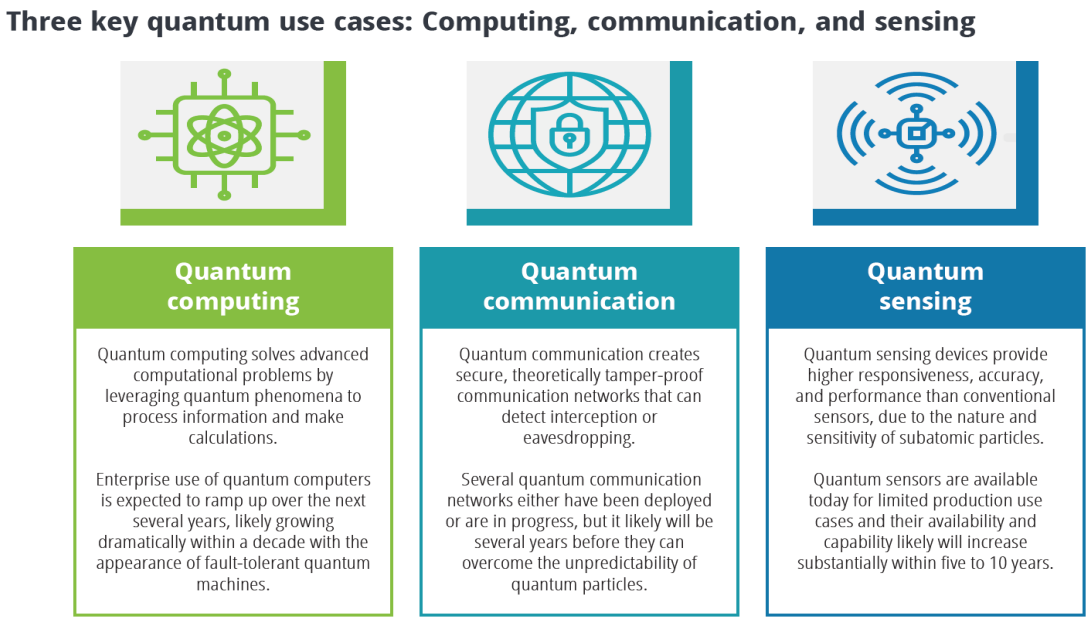
more in the commercial sector than in government, which is driving down procurement costs but creating new proliferation concerns.

Quantum technology

Quantum technology explains and portrays how a natural habitat of molecules, atoms, and electrons works, helping us to understand the events that take place in the microscopic world. Relying on three quantum properties of subatomic nature (quantum superposition, quantum entanglement, and quantum teleportation), it brings significant changes to the way existing technologies are applied today, including weapons applications.

For this reason, scientists have made progress in quantum entanglement and superposition that can potentially lead to advances in many other technologies. When fully developed, these capabilities could produce more reliable navigation, secure communications, accurate sensing, and powerful computing[9] (see Figure 3). Optimistic estimates indicate that applications such as quantum timing will be available for use within five years; however, other capabilities are at least 10 to 20 years away, or even further.[10] However, recent large investments by some nations and technology companies may result in rapid development.

Figure 3. Quantum Technology Uses[11]



Recommendations to NATO decision-makers

[9] Desjardins, J. "Quantum Computers And Their Applications," 2016. https://www.valuewalk.com/2016/03/quantum-computers-applications-graphic/

[10] Paul Martin, "Bringing ingenuity to life". https://www.paconsulting.com/insights/quantum-technology--applications/

[11] Image taken from *The Wall Street Journal*, "Quantum Technology Comes of Age," 01 June 2021, https://deloitte.wsj.com/articles/quantum-technology-comes-of-age-01622574129 (accessed 31 December 2021).

The four EDTs examined are affecting NATO's core tasks in several ways: 1) speed, use, and weaponization of information below the threshold of armed conflict are challenging the Alliance's cohesion more than ever before; 2) they will make missile and air defense systems less effective in the future, putting combat forces and a credible deterrence posture at risk; 3) they create a greater technology interoperability gap across the NATO member nations; 4) they increase the risk of losing the technological edge against adversaries; 5) new capabilities and how they are to be used are not covered in international treaties or official agreements, causing legal, ethical, and policy confusion.

The following 11 recommendations, which seek to address current gaps identified, are not set out in order of importance. They are intended as a basis for future research and analysis.

Recommendation 1: Evolve Article 5 and the deterrence paradigm

The use of cyberspace and the Internet of things (IoT), paired with new AI technologies, provide both opportunities and challenges on a global scale across diplomatic, informational, military, and economic means. The IoT comprises networks of sensors and data exchange between devices and people, extending the power of the Internet beyond computers and mobile devices for a multitude of purposes.[12] Rapid technological development has meant these devices have been integrated into our daily lives and have become an integral part of societies in NATO nations.

While an adversary may not conduct a conventional military armed attack on a NATO member country's territory, attacks conducted through the cyberspace domain nevertheless threaten the Alliance's security nonetheless.[13] NATO must evolve the way it thinks about the criteria for an Article 5 response and the accompanying deterrence strategy, expanding beyond conventional means to consider EDTs and their implications in a new, globalized, interconnected society. Failure to define a legal framework of what constitutes a cyber attack, thresholds for response at the appropriate classification level, and deterrence metrics will further destabilize the security environment and intensify the risk to the Alliance. Acknowledging a certain level of opaqueness is important, to allow a certain freedom of decision for policy-makers: strong, clear signals underpin an effective and credible deterrence strategy.

Prime considerations should include the following:

- Attribution is very important. Those identified must be held accountable; loss of life, economic damage, and disruption of the security environment cannot be tolerated.[14]
- Policies must be established for response escalation options, recognizing the importance of generating clear strategic messaging to potential adversaries.
- A response, whether through public or secret media, will be scoped according to the target of the attack and its consequences, in such a way as to achieve a desired action by the adversary, maintaining deterrence and avoiding escalatory reactions. This will make it possible to address security and economic impacts in the form of diplomatic, information-related, military, and economic actions, as appropriate. Acts must be met with a united and overwhelming response, ruling out achievement of the aggressor's objectives.[15]

---

12 Bojan Jovanović, "Internet of Things statistics for 2021 - Taking Things Apart," 24 March 2021, https://dataprot.net/statistics/iot-statistics/

13 P. Paganini. "NATO officially recognizes cyberspace as warfare domain," https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

14 Horace B. Robertson, Jr. "Self-defense against computer network attack under international law," *International Law Studies*, vol. 76, 2002, pp. 121-145, p. 135. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1396&context=ils

15 M. Lakomy, "Conditions to Invoke the Principle of Article 5 of The North Atlantic Treaty in Case of a Cyber-Attack or a Cyber Conflict," The Kosciuszko Institute, 2016, pp. 37-38, https://ik.org.pl/wp-content/uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf

Recommendation 2: A new Geneva Convention - Establish EDT control treaties and agreements

Ways must be identified, through NATO's political capacities, to advance international efforts so as to address security implications of EDTs. In the absence of established international frameworks protecting privacy and ethical concerns, new technologies produced with no control mechanisms will continue to enable adversarial activities in degrading Alliance cohesion. EDT advances and their impacts on society demand established international norms and safeguards, with special attention given to standardized sharing agreements for AI algorithms and data among NATO nations.

The destabilizing nature of hypersonic weapons means that they must be seen as a strategic asset. Constraints regarding relevant technology, capabilities, numbers, and deployment locations should be discussed and agreed to at UN Security Council level. NATO has an opportunity to initiate a dialogue, making for a more stable security environment.

Advances in AI and autonomous systems continuously challenge the international rules of warfare, presenting new legal and ethical questions. Concepts such as 'human in the loop' and limits to machine autonomy need to be defined by agreement. EDTs are creating a new world, requiring new international frameworks and structures.

Recommendation 3: Modernize and synchronize missile & air defense to meet hypersonic threats

Missile and air defense innovation programs within NATO nations are largely developed in isolation. This lack of coordination among the nations is a serious concern for a synchronized, interoperable missile and air defense. NATO could play a bigger role as a source of coordination for its members.[16] Like the United States with its Hypersonic Roadmap, NATO should work towards entering the R&D field for hypersonic missiles and defense systems. National research institutes such as DLR and the Fraunhofer Institute in Germany, as well as industrial companies such as MDBA Missile Systems and Bayern-Chemie, are examples of potential partners.

Building effective defense measures against hypersonic systems will require a shared approach among NATO nations, pooling their capabilities in the area of sensors and interceptors. A combination of these defense measures, supported by a suitable Command & Control and Communications and Intelligence system, is needed to significantly reduce the advantage that an adversary can gain by using hypersonic weapons. This would make it possible to strengthen NATO's collective defense.

Recommendation 4: Establish an organization and training center for technical interoperability

A credible deterrent must demonstrate a proficient and interoperable multi-domain capability to adversaries and partners alike. EDTs and threats from Russia and China compel the Alliance to establish an organization that can integrate EDTs into strategic and operational planning, testing and exercises. It is necessary to educate leaders and professional staff accordingly, identifying and safeguarding against threats, and applying common capabilities across the Alliance.[17] It is also necessary to establish education and training programs for NATO. Like training centers of the past that combined infantry and armored maneuvers, a new training center should simulate the battlefield of the future, to integrate offensive and defensive EDT capabilities. It should be able to replicate the new battlefield for commanders and staff, enabling them to learn and experiment with how EDTs will affect their operational planning and mission execution. While detailed examination of what such a training center should look like is beyond the scope of this paper, urgent consideration must be given to where small-scale, newly developed technologies can be

[16] Vivienne Machi, "Where Does NATO Fit into the Global Hypersonic Contest?" *Defense News*, 15 March 2021, https://www.defensenews.com/global/europe/2021/03/15/where-does-nato-fit-into-the-global-hypersonic-contest/

[17] NATO, "NATO 2030: United for a New Era," *op. cit.*

tested, exercised, and validated on an appropriate scale for interoperability and common standards across NATO force and command structures.

Recommendation 5: Invest in quantum technology development

Quantum technology is one of the least developed of the EDTs examined and its application, if achieved, presents both a strategic threat and opportunity. Quantum-based technologies will revolutionize the future of warfare and deterrence through C2 (command and control), PNT (positioning, navigation, and timing), sensing, and communications. Assessments identify China as the most advanced power in this regard. Areas where it could jeopardize NATO's collective defense include: 1) adversaries' C2 systems where message transmission would be tamper-proof; 2) development of quantum radar-sonar, a major strategic asset making it possible to track submarines and stealth aircraft.[18] It is therefore critical to invest in quantum-based capabilities and determine how to integrate their application across the Alliance.

Recommendation 6: Develop an EDT partnership strategy

A search of commercial companies conducting EDT research and national governments developing new programs illustrates a complex, chaotic, and uneven environment. It is important to find common ground with like-minded organizations such as the EU and established partnership forums such as Partners Across the Globe, including countries with mature technological sectors like Japan and South Korea: involving government, industry, and academia will make it possible to better synchronize development, while reducing duplication of resources.[19]

Conducting joint summits would allow partners to regularly assess progress, while strengthening relationships through technological diplomacy. Engagement with commercial partners at these summits should address legal, moral, and social impacts of developed technologies. Setting up a European DARPA-like organization would effectively pool resources, enabling a more innovative culture prepared to take risks in technology concept development.

Recommendation 7: Reduce and divest legacy programs

The heart of the Alliance is collective defense. The post-Resolute Support environment marks the appropriate time to re-evaluate the strategic landscape and posture against future threats. Flowery strategic documents and communiqués only go so far to underpin credible deterrence. Hard choices are needed, divesting legacy missions and eliminating programs no longer relevant so as to reallocate finite resources and face new dangers. It is necessary to identify areas where responsibility can be transferred to other organizations such as the UN, the EU, the OSCE, the African Union, and the Arab League. Three questions must find honest answers to drive strategy, prioritization, and resource allocation: 1) What must NATO do? 2) What can NATO do? 3) What is NATO doing that other organizations should do? Supporting every challenge is a noble aspiration; however, there are too many gaps and threats related to EDTs.

Recommendation 8: Prevent the creation of a stronger Russia-China relationship

---

[18] P. Smith-Goodson, "Quantum USA Vs. Quantum China: The World's Most Important Technology Race," 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/

[19] Ester Sabatino and Alessandro Marrone, "Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy," Istituto Affari Internazionali, 17 June 2021. https://www.iai.it/sites/default/files/iaicom2131.pdf (accessed 23 October 2021);
Gustav Lindstrom and Thierry Tardy, "The EU and NATO: The essential partners," European Institute for Security Studies. 2019, https://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1 (accessed 14 November 2021).

Despite a long history of distrust, Beijing and Moscow have increased cooperation across the political, economic, and military spheres in recent years.[20] Russia and China have selectively leveraged each other's respective strengths in scientific joint project ventures.[21] However, current assessments indicate that the Sino-Russian relationship is more characterized by competition than cooperation. NATO must ensure its policies, partnerships, activities, and messages do not exist in a vacuum, without consideration of their strategic effects on the Russia-China relationship. The best of intentions regarding a policy or operation from a NATO perspective may unintentionally create a stronger Russia-China relationship: while the status quo is favorable, deeper engagement between them increases risk.

Recommendation 9: Re-evaluate structure and capabilities of the NRF and VJTF

In the multi-domain warfare environment, the structure and capabilities of the NATO Response Force (NRF) and Very High Readiness Joint Task Force (VJTF) need to evolve. Additional capabilities, tactics, techniques, and procedures to counter threats from AI, hypersonic weapons, and autonomous platforms need to be included in the NRF validation and rotational cycles. A cyber component with additional support enablers, to counter AI-based threats identified in this paper, should be considered as part of the structure. Hypersonic weapons are impossible to intercept, and future air defense platforms will require different capabilities and employment methods. Finally, a further course of action should be the use of the Counter-Hybrid Support Teams (CHSTs) in the NRF or VJTF (see next recommendation), in their own right or as an augmenting capability alongside the Special Operations Forces component.

Recommendation 10: Build on the successes of Counter-Hybrid Support Teams

NATO Counter-Hybrid Support Teams (CHSTs) form a model framework to expand upon in responding to EDT-enabled disinformation threats.[22] CHSTs were established to provide tailorable assistance to member states lacking their own capabilities, with a view to countering gray-zone activities. Examples include CHST deployments to Montenegro and North Macedonia, for a stronger response to cyber disinformation activities originating from Russia.[23] A further example of demand for this is Lithuania's request for a CHST in order to deal with the disinformation and political blackmail created by the Lukashenko regime's hybrid attacks. Incorporating lessons learned, and building upon the CHST concept to counter disinformation campaigns, will contribute to Alliance cohesion and collective defense.

Recommendation 11: Do not ignore integration of the human domain with EDTs

The key to future military advantage will be effective integration of humans, AI, and robotics into combat systems. Education and training will be a critical element in the effective incorporation and use of EDTs with NATO personnel. State-of-the-art technologies sitting on the shelf, without

[20] Paul N. Schwartz, "The Military Dimension in Sino-Russian Relations," In *Sino-Russian Relations in the 21st Century*, edited by Jo Inge Bekkenvold, Bobo Lo, Switzerland: Palgrave Macmillan, 2019, pp. 87-112.

[21] Samuel Bendett and Elsa B. Kania, "*A new Sino-Russian high-tech partnership – Authoritarian innovation in an era of great-power rivalry*," Australian Strategic Policy Institute, 29 October 2019. https://www.afpc.org/publications/articles/a-new-sino-russian-high-tech-partnership

[22] In July 2018, NATO leaders agreed to set up CHSTs, providing tailored targeted assistance to Allies upon request, in preparing against and responding to hybrid activities. Such teams consist of civilian members drawn from a pool of NATO experts, as well as specialists nominated by Allies.

[23] Linda Sanchez, "2021 - Revised Draft Report - Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda." NATO PA, 03 September 2021. https://www.nato-pa.int/document/2021-bolstering-democratic-resilienceof-alliance-against-disinformation-and-propaganda

suitable fusion of systems with the human domain, will result in failure. Human augmentation (HA) will represent a "spice mélange" of technologies that will improve physiological and cognitive abilities of humans to wage war. HA will challenge the conduct of NATO's core tasks in areas such as ethical, legal, and policy issues, as well as in their very implementation.[24] HA is not a panacea, but it could be the glue that joins the technical capabilities of machines with human adaptability, creativity, and cognition.

Conclusion: EDTs require new ways to approach and solve challenges

The strategic landscape and threat environment have changed well beyond what could have been envisioned in 1949: revisionist powers and non-state asymmetric threats are utilizing new means and methods to disrupt international norms. EDTs and rapidly advancing technologies in the digital age challenge NATO's cohesion and the very foundation of collective defense in new ways, through a variety of possible scenarios unfolding on an unprecedented scale and at a speed never seen before.

The Alliance has a variety of military, political, and technological options to counter the destructive repercussions of EDTs in the Euro-Atlantic region, and safeguard the conduct of its core tasks. NATO should consider initiating or leading international efforts in establishing multilateral control mechanisms and norms for EDTs. With this in mind, our recommendations have sought to provide tangible proposals in answer to the "NATO 2030: United for a New Era" Reflection Group Report's identification of the need for a strategic surge in EDTs, so as to maintain political cohesion, win on the battlefield, and strengthen interoperability.

[24] NATO Science & Technology Organization, "NATO Advisory Group on Emerging and Disruptive Technologies, Annual Report 2020," https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

Bibliography

Bendett, Samuel and Elsa B. Kania. "A new Sino-Russian high-tech partnership - Authoritarian innovation in an era of great-power rivalry." Australian Strategic Policy Institute, 29 October 2019. https://www.afpc.org/publications/articles/a-new-sino-russian-high-tech-partnership

CNBC.com. "Putin: Leader in artificial intelligence will rule the world." 04 September 2017. https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html

Cummings, M.L., Heather M. Roff, Kenneth Cukier, Jacob Parakilas, and Hannah Bryce, "Artificial Intelligence and International Affairs: Disruption Anticipated." Chatham House Report, 14 June 2018. https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf

Desjardins, J. "Quantum Computers And Their Applications." 2016. https://www.valuewalk.com/2016/03/quantum-computers-applications-graphic/

Jovanović, Bojan. "Internet of Things statistics for 2021 - Taking Things Apart." 24 March 2021. https://dataprot.net/statistics/iot-statistics/

Lakomy, M. "Conditions to Invoke the Principle of Article 5 of The North Atlantic Treaty in Case of a Cyber-Attack or a Cyber Conflict." The Kosciuszko Institute, 2016. https://ik.org.pl/wp-content/uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf

Lindstrom, Gustav and Thierry Tardy. "The EU and NATO: The essential partners." European Institute for Security Studies, 2019. https://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1 (accessed 14 November 2021).

Machi, Vivienne. "Where Does NATO Fit into the Global Hypersonic Contest?" *Defense News*, 15 March 2021. https://www.defensenews.com/global/europe/2021/03/15/where-does-nato-fit-into-the-global-hypersonic-contest/

NATO. "Brussels Summit Communiqué." 14 June 2021. https://www.nato.int/cps/en/natohq/news_185000.htm

NATO, *NATO 2030: United for a New Era.* 25 November 2020. https://www.nato.int/nato-static-fl2014/assests/pdf/2020/12/pdf/20121-Reflection-Group-Final-Report-Uni.pdf (accessed 1 November 2021).

NATO Science & Technology Organization. "NATO Advisory Group on Emerging and Disruptive Technologies, Annual Report 2020." https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

Paganini, P. "NATO officially recognizes cyberspace as warfare domain." https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

RANE Worldview, "Explaining the Hype Around Hypersonic Weapons." 6 January 2018. https://worldview.stratfor.com/article/explaining-hype-around-hypersonic-weapons (accessed 31 December 2021).

Rasanayagam, Gowthami, "AI vs. Machine Learning vs. Deep Learning." Medium, 21 September 2021. https://medium.com/nerd-for-tech/ai-vs-machine-learning-vs-deep-learning-60b3d0611fe9 (accessed 19 November 2021).

Reuters.com, "China has won AI battle with U.S., Pentagon's ex-software chief says." 11 October 2021. https://www.reuters.com/technology/united-states-has-lost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/ (accessed 01 November 2021).

Robertson, Horace B., Jr. "Self-defense against computer network attack under international law." *International Law Studies*, vol. 76, 2002, pp. 121-145. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1396&context=ils

Sabatino, Ester and Alessandro Marrone. "Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy." Istituto Affari Internazionali, 17 June 2021. https://www.iai.it/sites/default/files/iaicom2131.pdf (accessed 23 October 2021).

Sanchez, Linda. "2021 - Revised Draft Report - Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda." NATO Parliamentary Assembly, 03 September 2021. https://www.nato-pa.int/document/2021-bolstering-democratic-resilienceof-alliance-against-disinformation-and-propaganda

Schwartz, Paul N., "The Military Dimension in Sino-Russian Relations." In *Sino-Russian Relations in the 21st Century*, edited by Jo Inge Bekkenvold, Bobo Lo, Switzerland: Palgrave Macmillan, 2019, pp. 87-112.

Smith-Goodson, P. "Quantum USA Vs. Quantum China: The World's Most Important Technology Race." 2019. https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/

The Wall Street Journal. "Quantum Technology Comes of Age." 01 June 2021. https://deloitte.wsj.com/articles/quantum-technology-comes-of-age-01622574129 (accessed 31 December 2021)