Ploughshares

REPORT

The future of global conflict:

A synthesis of contextual and technological perspectives

By Carlos Cantafio Apitz and Branka Marijan

OCTOBER 2023

The future of global conflict: A synthesis of contextual and technological perspectives

Authors: Carlos Cantafio Apitz and Branka Marijan

Editor: Wendy Stocker

Designer: Tasneem Jamal

First published: October 2023

With funding from the Mobilizing Insights in Defence and Security (MINDS) program of the Canadian Department of National Defence

Project Ploughshares

140 Westmount Road North

Waterloo, Ontario N2L 3G6

Canada

Telephone: 519-888-6541

Email: plough@ploughshares.ca

Table of contents

Introduction 5

Methodological considerations 6

Analysis of data 6

Technological considerations on the future of armed conflict 7

Conclusion 11

Appendix A: Defining the six emerging military technology clusters 12

Appendix B: Technology Readiness Levels (TRLs) spectrum & definitions 13

Appendix C: Literature review reports 14

Authors

Carlos Cantafio Apitz is a Master's of Global Affairs candidate at the University of Toronto and a former Project Ploughshares Research Assistant. The research assistantship was supported by a Mobilizing Insights in Defence and Security (MINDS) grant from the Canadian Department of National Defence.

Dr. Branka Marijan is a Senior Researcher with Project Ploughshares.

Introduction

How will technological changes affect global security in the next 20 years? In what ways? Which developments and innovations are most likely to significantly impact how states approach conflict? The rapid technological advancements occurring today, across multiple fields, have the potential to transform global security dynamics.

State actors are already finding it challenging to align policy with the current pace of technological innovation. More and more, the dual-use nature of many of these technologies and their vulnerability to exploitation produce effects that are not limited to one state and can only be controlled through multilateral global efforts.

This brief aims to review perspectives from such organizations as governments, think tanks, and businesses on the technological readiness of emerging technologies and how they could change the future of battlespaces. It first highlights relevant economic, environmental, political, social/demographic, and technological trends and factors. Then, it introduces six emerging technology clusters that came out of a categorization exercise that mapped specific technologies identified in the literature review. Finally, their current state of technological readiness and the expected maturity of select military applications are explored.

This brief identifies and synthesizes three distinct insights from the literature:

1. Known military applications of artificial intelligence (AI) and big data analytics, as well as novel delivery technologies, are likely to be mature and leveraged within the battlespace by 2030, as government and commercial actors have years of continuous investment in their development.
2. A combination of current state regulatory constraints, global normative ethical considerations, and technological constraints, including restrictions on accessing material and technologies, is likely to impact the launch of military applications of advanced materials and manufacturing, autonomy and robotics, biomedical sciences and human augmentation, and quantum technologies until 2035-2040 or later.
3. Transformative and disruptive effects are most likely to occur when militaries combine or interconnect two or more of these emerging technologies. Therefore, state and nonstate actors across the decision-making spectrum should not focus on siloed technologies.

Methodological considerations

The literature reveals differences in how emerging military technologies are classified and assessed. While some reports focus directly on military applications, others look first at science and technology developments and then highlight potential military uses. Findings in this brief are based on the collection of data points from 20 reports by private, public, and nonprofit actors from North America and Europe (see Appendix C), including the European Defence Agency, NATO, the Joint Chiefs of Staff of the United States, and the European Parliament. Perspectives are likely influenced by relevant regional dynamics; findings may change when non-Western perspectives are included.

Data from these 20 reports reveals a consensus on the following emerging technology clusters (see also Appendix A):

1. AI & big data analytics
2. Autonomy & robotics
3. Novel delivery technologies
4. Advanced materials & manufacturing
5. Biomedical sciences & human augmentation
6. Quantum technologies.

Technologies that enable space military efforts are widely covered in the researched reports. While some technological developments will depend on or impact space assets, space is not covered in this brief.

A database was generated to organize information taken directly from the reports, as well as evidence that could be derived from report context. Figure 1 represents an aggregation of collected perspectives, which may be subject to change with the addition of new data.

Analysis of data

Data taken from these 20 reports was analyzed through multiple lenses to frame existing security-focused research within anticipated global trends that cover a timeframe from 2025 until 2040 and later.

It is likely that new or continuing complex, multifaceted, cross-border conflicts will arise from multiple and interrelated factors that are influenced by some or all of the trends below, which include a changing world order, developments in science and technology, and human geography. Due to the integration and interconnectedness of these trends, the international community will be hard pressed to coordinate responses to such conflicts.

- ***Economic***: The next two decades will likely see further advances in the interconnectedness of financial systems, although trade nationalism, growing protectionism, and 'friendshoring' (sourcing from geopolitical allies) might cause a trend that is more regional than global. The world could also see the rise of emerging economies as developed states with significant welfare economies experience increased costs in response to rapidly aging populations, diminishing workforces, and global inequities. This new dynamic could be linked to shifting workforce trends, lower advanced economy productivity gains, and a rise in youth unemployment.

- ***Social/Demographic***: Regions are likely to experience lower fertility rates and an older overall population, as we are seeing in Canada. Some states will experience higher rates of urbanization and intensified population concentration along coastal areas, possibly coupled with increased cross-border and internal human migration.

- ***Political***: The changing world order is predicted to result in a redistribution of geopolitical power that will foster a continuing need for strong alliances and partnership networks. Increasing great power competition, coupled with the rise of emerging economies, could result in novel geopolitical rivalries. It is possible that a state military will play a smaller role in security, replaced by outsourced military actors, particularly in relation to cybersecurity. As well, the ongoing democratization of access to information could lead to increasing political polarization among the general population and reduced trust in government leaders and institutions.

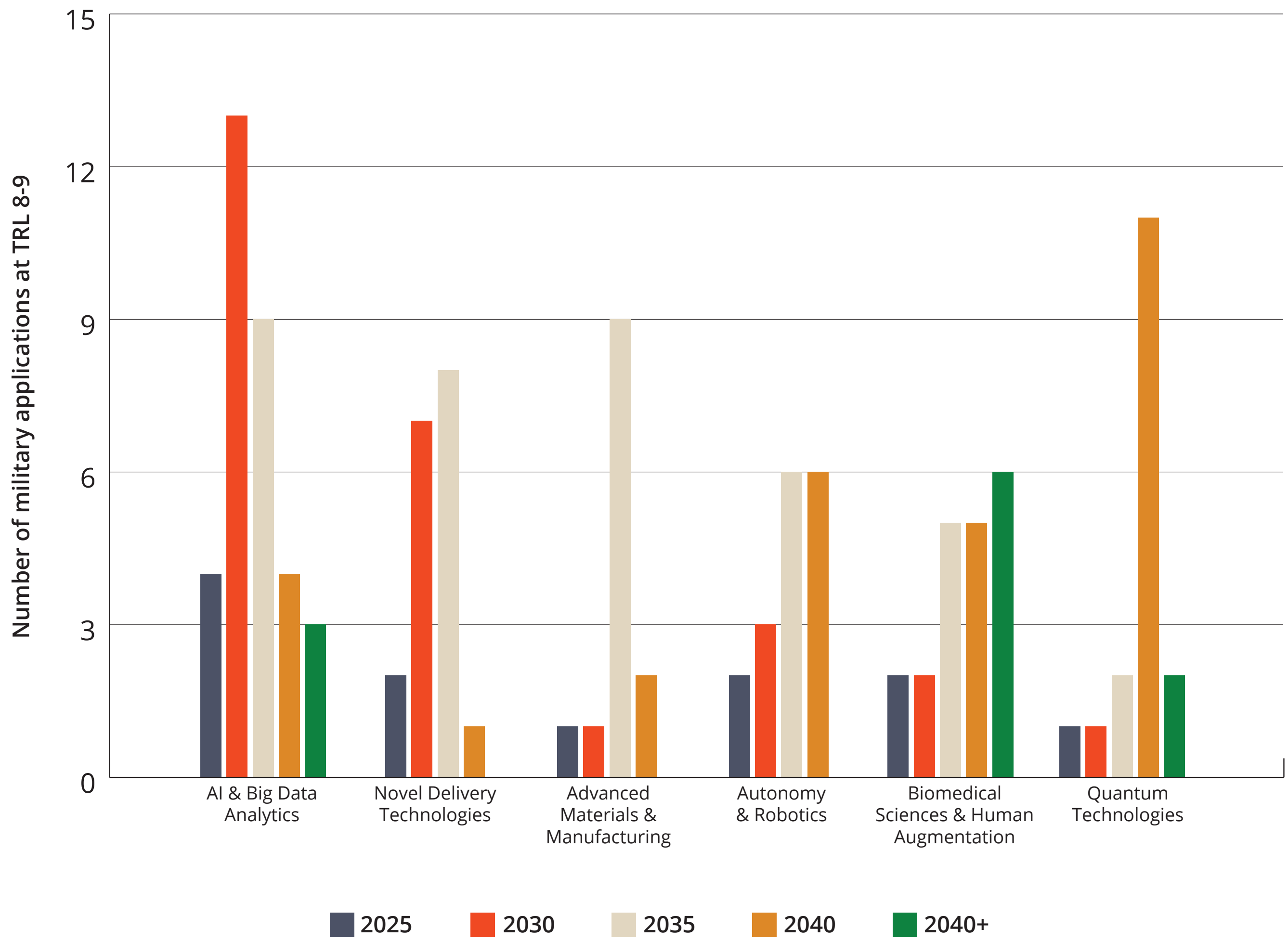
- ***Technological***: The rate of this development will increase, with innovations becoming more complex. Civilian and dual-use sectors will drive growth. These changes will likely accelerate reliance on information and communications technology (ICT) networks by social, economic, and defence sectors. The regulation and maintenance of Internet governance systems and institutions will become more complex. Militaries will increasingly rely on commercial technology as defence departments seek cost efficiencies. Such reliance will produce more vulnerabilities, specifically in cybersecurity, because commercial systems will be more vulnerable to hacks and might not have rigorous safety testing for security and defence contexts.

- ***Environmental***: Climate change will bring about widespread environmental changes that produce significant economic and political effects. Water and food scarcity will become more prevalent, as will intense natural disasters, infectious diseases, and pollution. State and nonstate competition over natural resources and global commons, including outer space, will increase.

Technological considerations on the future of armed conflict

Generating forecasts for the six identified technology clusters (see Appendix A for expanded definitions) is a complex exercise. Figure 1 organizes military applications of the six technology clusters from most likely to impact defence applications beginning in the next two/seven/12/17 years) due to recent technological progress and embeddedness factors (AI & big data analytics) to most likely to impact defence applications beginning in the next 17-20 years because of the complexities associated with developing such technology (quantum technologies).

Figure 1: Estimated number of military applications reaching Technology Readiness Level (TRL) 8-9 (see Appendix B for definitions), per emerging military technology cluster for the period 2025-2040+



Data collected and aggregated from literature review. See also Appendix B and C.

Insight #1: Known military applications of AI and big data analytics as well as novel delivery technologies are likely to be mature and leveraged on the battlefield by 2030, as government and commercial actors have a long history of continuous investment in their development.

Growth and innovation in AI and big data analytics are likely to be primarily fueled by the commercial sector and are expected to outpace research and development (R&D) by the national security sector. National defence actors could be at a disadvantage in the race for talent and capacity building. It appears that militarized AI or big data analytics is likely to develop from the dual-use nature of these technologies. Moreover, much of the technological innovation is dominated by a handful of companies whose investments continue to outpace spending by smaller companies and governments. Experts have noted concern about regulatory capture and the potential for a few companies to act as "gatekeepers" in accessing technology.

Several applications (e.g., AI for cyber operations and information warfare) will be considered mature within the next two years. The bulk of military applications will mature by 2030-2035; these could range from AI for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and exploitation of C4ISR vulnerabilities, to multi-data analysis and connectivity of sensor data for advanced decision-making. Advancements related to artificial general intelligence (replication of human intelligence) and artificial superintelligence (exceeding human comprehension) are debated by experts; there is not yet certainty on how these technologies will develop over the longer term.

Several states have made advancements in novel delivery technologies that result in greater speed, survivability, accuracy, and range. The United States, China, and Russia are the current leaders in military R&D for hypersonic vehicle applications, while China and Russia demonstrate considerable progress on hypersonic flights. Greater intolerance for civilian casualties and heightened demand for accountability are driving advancements in precision technology. While few mature applications exist now, the 2030-2035 period is likely to see an increased use of direct energy weapons (DEWs), hypersonic drones carrying ISR technology, and hypersonic weapon systems. Currently, it is estimated that applications in 2040 will include operational non-nuclear electromagnetic pulse weapons and high-energy lasers.

Insight #2: A combination of current state regulatory constraints, global normative ethical considerations, and limited technological progress is likely to delay the launch of military applications of advanced materials and manufacturing, autonomy and robotics, biomedical sciences and human augmentation, and quantum technologies until at least 2035.

Additive manufacturing processes will likely be more widespread than the ability to source and fund advanced materials; the high cost of scaling up the production of advanced materials may deter financially handicapped actors. Commercial and government sectors will benefit from the proliferation of additive manufacturing; however, a wide number of states and nonstate actors will likely have access to this technology at about the same time. Inconsistencies in export control regimes on machines, materials, and technologies necessary for additive manufacturing could lower barriers to access by smaller states and nonstate groups. The 2025-2030 period will be characterized by improvements in additive manufacturing and energy storage (e.g., 3D printing, batteries) that are partially driven by efforts to combat climate change. Military uses are expected to be mature by 2035, with some applications, including nano-enabled and programmable smart materials for ISR and flexible electronics, available on a global scale.

The number of applications of autonomous technologies is also likely to increase in the 2030-2040 timeframe. However, widespread adoption of autonomous technologies is being challenged globally, with major international civil society organizations advocating for an international ban on lethal autonomous weapon systems (LAWS). Different perspectives elicit concerns, including:

1. Ethical concerns about the lack of moral and contextual human judgement in decision loops
2. Operational concerns related to the potential hacking of autonomous systems, errors, and accidents that would be difficult to control with increasingly autonomous systems
3. International Humanitarian Law concerns about attribution and distinction, as well as other IHL principles.

Human-in-the-loop machine teaming and autonomous sensors will be the points of entry for military uses. They could be followed by non-lethal technologies, such as autonomous ISR and uncrewed logistics systems. There is continued disagreement on the maturity and time of entry of autonomous armed systems in the battlefield. Several existing systems, such as Elbit's SkyStriker loitering munition, are believed to have the ability to autonomously locate, engage, and target predetermined targets. Moreover, there are claims that SkyStriker can also function with a human-in-the-loop in communication-denied environments.

Biomedical and quantum technologies will likely be the last to be battlefield ready. Clear prohibitions and strong norms on biological weapons are upheld by the Biological Weapons Convention (1975). Collaboration on biotechnology R&D will vary greatly by jurisdiction as each state has different regulations, policy objectives, and operational and ethical standards. Legal and ethical considerations will likely prevent accelerated R&D on human augmentation in most states, while R&D on weaponized biotechnology will likely develop more quickly. Civilian developments on bioinformatics and synthetic biology will pave the way for more advanced military applications. The period after 2035 is likely to feature biological engineering on genomes, cybernetic augmentation, pharmaceuticals that improve physical and cognitive resilience and injury recovery on soldiers, and exoskeletons that increase on-the-ground capabilities.

And, while quantum technologies are developing rapidly, progress is uneven across four potential security applications related to computing, communications, precision, and sensing. The growth of quantum computing is primarily due to commercial R&D, while advancements across the remaining three categories are driven by security actors. Collaboration between states could be hindered by conflicting national security considerations and different rates of investment. Widespread availability of militarized quantum technology does not seem likely in the near future. Most reports place uses of militarized quantum technology no earlier than 2040; uses include quantum computing for C4ISR and hardening/exploiting systems, enabling simulations for drug and novel materials discovery, and quantum key distribution and cryptanalysis.

Insight #3: Transformative and disruptive effects are most likely to occur when militaries combine or interconnect two or more of these emerging technologies. Therefore, state and nonstate decision-makers should not focus solely on siloed technology concerns.

While this brief does not attempt to predict the likely points of interconnection of the studied technology clusters, it does assume that the battlespace of the future will reflect a combination of these emerging military technologies, amplifying potential effects and blurring the lines between conventional, unconventional, and asymmetric warfare. Interconnectedness is likely to increase as systems become more intelligent, digital, and distributed. These systems will be enabled by greater semiautonomous and autonomous features, improved knowledge analytics and communications, abundant and decentralized ISR, and synergistic environments (e.g., physical and virtual domains as well as increased human-machine teaming that could be interchangeably used by actors to exploit technological and battlefield advantages).

Most of the contemporary literature in this field considers and evaluates each technological cluster individually, likely because of the complexity of predicting TRL horizons along with likely interconnected uses. However, the integrated and/or overlapping applications of these emerging technologies will have multiple, multiplying, and intertwined effects that could significantly impact international stability and human security. Concerns are compounded as these technologies are developed and integrated in times of heightened geopolitical tensions involving the United States, Russia, and China. Moreover, easily accessible commercial technologies such as generative artificial intelligence will be exploited both for information and in decision-making in the deployment of weapons.

Such developments could make the enactment of meaningful international arms control agreements more difficult. To effectively regulate this complex geopolitical-technological advancement dynamic, all relevant actors should first aim to recognize the effects of the interconnectedness of these technologies. Future policy research should be dedicated to narrowing the knowledge gap of decision-makers on the effects of the interactions of emerging military technology clusters.

Conclusion

While the dynamics and characteristics of warfare are constantly evolving, the current accelerated pace of change demands our attention. The emerging technology-security environment, coupled with the rise of great power competition, will likely challenge existing global norms.

Using five lenses, this brief outlines trends and conditions that could converge and intersect to create future conflicts. These conflicts will be characterized by materially different military landscapes populated by a wide array of new technologies. Militarized applications of AI & big data analytics and novel delivery technologies are likely to come online first, changing the nature of C4ISR and defence preparedness.

The environment in the period 2030-2040, however, is likely to differ significantly from today's, as additive manufacturing, autonomous systems, biotechnology advancements, and quantum technologies change how actors will engage in activities from logistics and C4ISR to kinetic and non-kinetic warfare. Further study is needed to understand non-Western perspectives, particularly as China continues to indigenize technological supply chains. In anticipation of the expected transformations that emerging technologies will bring to warfare, international governance bodies should ensure that overseeing technological development and prioritizing arms control frameworks are at the top of their agendas.

Appendix A: Defining the six emerging military technology clusters

ARTIFICIAL INTELLIGENCE & BIG DATA ANALYTICS

Software-based technologies that perform advanced computing based on vast amounts of data that enable analysis, interpretation, and response (software capable of emulating human-level cognition). Included are machine learning, unsupervised deep learning, synthetic environments, virtual and augmented realities, predictive algorithms, AI-supported decision-making, communications, and cybersecurity.

AUTONOMY & ROBOTICS

Technologies that allow for the operation of uncrewed systems with a range of self-directed behaviours. Included are advances in navigation and precision landing, human-machine teaming, logistics/sustainment, army replacement, and autonomous lethal weapons.

NOVEL DELIVERY TECHNOLOGIES

Weapons and subsystems that facilitate the delivery of novel kinetic and non-kinetic impacts, as well as the delivery of traditional/conventional impacts in a novel manner. Included are hypersonics and launching/delivery of hypersonic attacks across domains (e.g., hypersonic swarms or underwater launch), directed energy weapons (e.g., lasers), and atmospheric defensive shields.

ADVANCED MATERIALS & MANUFACTURING

Artificial materials with unique functionalities (e.g., improvements in performance of traditional materials, including coating for extreme weather resistance, energy harvesting, superconductivity), as well as improved processes/advanced techniques for manufacturing (e.g., 3D printing/additive manufacturing and nanotechnology).

BIOMEDICAL SCIENCES & HUMAN AUGMENTATION

Innovations that can optimize and augment human performance, such as human enhancement technologies (cognitive and/or physical), AI-powered diagnoses, and prosthetics integration into the nervous system. Also included are biological weapons and synthetic biology (printed DNA and using marine bacteria as sensors).

QUANTUM TECHNOLOGIES

Technologies that take advantage of/use quantum physics (atomic- and subatomic-scale dynamics). Included are technological applications such as cryptography, computing, sensors, and communications. Most reports consider such technologies to be in their nascent phase; once mature, they could disrupt other existing computing, communication, and encryption technologies.

Appendix B: Technology Readiness Levels (TRLs) spectrum & definitions

RESEARCH	1. Basic principles observed
	2. Technology concept formulated
	3. Experimental proof of concept
DEVELOPMENT	4. Technology validated in lab
	5. Technology validated in relevant environment
	6. Technology demonstrated in relevant environment
DEPLOYMENT	7. System prototype demonstration in operational environment
	8. System complete and qualified
	9. Actual system proven in operational environment

Source: Adapted from Favaro

Appendix C: Literature review reports

1. Bellasio, J., Slapakova, L., Huxtable. L., Black, J., Ogden, T., Dawaele, L., and RAND Europe. *Innovative technologies shaping the 2040 battlefield.* European Parliament - Directorate General for Parliamentary Research Services. 2021. https://data.europa.eu/doi/10.2861/620590.
2. Bidwell, Christopher A., MacDonald, J.D., and MacDonald, Bruce W. *Emerging disruptive technologies and their potential threat to strategic stability and national security*. Federation of American Scientists. September 2018. https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf.
3. Development, Concepts, and Doctrine Centre. *Future operating environment 2035*. UK Ministry of Defence. November 2014. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1076877/FOE.pdf.
4. Fast track action subcommittee on critical and emerging technologies. *Critical and emerging technologies list update.* National Science and Technology Council (U.S.). February 2022. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.
5. Favaro, M., Renic, N., and Kühn, U. *Negative multiplicity: Forecasting the future impact of emerging technologies on international stability and human security*. Institute for Peace Research and Security Policy, University of Hamburg. September 2022. https://ifsh.de/file/publication/Research_Report/010/Research_Report_010.pdf.
6. Global Aerospace & Defense Research Team. *US Department of Defense 2023 budget assessment and growth opportunities*. Frost & Sullivan. August 2022. https://store.frost.com/us-department-of-defense-2023-budget-assessment-and-growth-opportunities.html.
7. Gokhberg, L., Sokolov, A., and Chulok, A. "Russian S&T Foresight 2030: Identifying new drivers of growth." *Foresight*, Vol. 19 No. 5, pp. 441-456 (2017). https://doi.org/10.1108/FS-07-2017-0029.
8. Hoehn, Andrew R., Parasiliti, Andrew, Efron, Sonni, and Strongin, Steven. *Discontinuities and distractions — Rethinking security for the year 2040: Findings from a RAND Corporation workshop.* RAND Corporation, April 27, 2018. https://www.rand.org/pubs/conf_proceedings/CF384.html.
9. ISDEFE and European Defence Agency. *EDA Technology Foresight Exercise 2021 – 1st event results – Publishable summary*. August 2021. https://eda.europa.eu/docs/default-source/documents/eda-technology-foresight-exercise-(2021)---1st-event-results---publishable-summary72ffba3fa4d264cfa776ff000087ef0f.pdf.
10. Kavanagh, Camino. *New tech, new threats, and new governance challenges: An opportunity to craft smarter responses?* Carnegie Endowment for International Peace. August 2019. https://carnegieendowment.org/files/WP_Camino_Kavanagh___New_Tech_New_Threats1.pdf.
11. Kepe, Maria, Black, James, Melling, Jack, and Plumridge, Jess. *Exploring Europe's capability requirements for 2035 and beyond – Insights from the 2018 update of the long-term*

strand of the Capability Development Plan. RAND Europe for the European Defence Agency. June 2018. https://eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf.

12. Kindvall, Göran, Lindberg, Anna, Trané, Camilla, and Westman, Jonatan. *Exploring future technology development*. FOI – Swedish Defence Research Agency. June 2017. https://www.foi.se/rest-api/report/FOI-R--4196--SE.
13. Kott, Alexander and Perconti, Philip. "Long-term forecasts of military technologies for a 20–30 year horizon: An empirical assessment of accuracy." *Technological Forecasting and Social Change* 137: 272–79, December 2018. https://doi.org/10.1016/j.techfore.2018.08.001.
14. NATO Office of the Chief Scientist. *Science & technology trends 2020-2040: Exploring the S&T edge*. NATO Science & Technology Organization. March 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.
15. Office of the Deputy Assistant Secretary of the Army (Research & Technology). *Emerging science and technology trends: A synthesis of leading forecasts*. 5th Edition. U.S. Army. March 2019. https://apps.dtic.mil/sti/pdfs/AD1078879.pdf.
16. O'Hanlon, Michael. *Forecasting change in military technology, 2020-2040*. Foreign Policy at Brookings. September 2018. https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf.
17. Raska, Michael. "Strategic competition for emerging military technologies: Comparative paths and patterns." *PRISM* 8, no. 3 (2019): 64–81. https://www.jstor.org/stable/26864277.
18. Sayler, Kelley M. *Emerging military technologies: Background and issues for Congress*. Congressional Research Service. November 2022. https://sgp.fas.org/crs/natsec/R46458.pdf.
19. U.S. Joint Chiefs of Staff. *Joint Operating Environment 2035: The Joint Force in a contested and disordered world*. July 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf.
20. Mittal, V. and Davidson, A. "Combining wargaming with modeling and simulation to project future military technology requirements." *IEEE Transactions on Engineering Management*, vol. 68, no. 4, pp. 1195-1207, August 2021. https://ieeexplore.ieee.org/document/9184821.

Ploughshares

Project Ploughshares is a Canadian peace research institute with a focus on disarmament efforts and international security, specifically related to the arms trade, emerging military and security technologies, nuclear weapons, and outer space.

For more information please visit: www.ploughshares.ca.