Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

J.-M. Rickli & G. Vllasi
Connections QJ 24, no. 1 (2025): 91-112
https://doi.org/10.11610/Connections.24.1.07

Research Article

The Weaponization of Emerging Technologies and Their Impact on Global Risk: A Perspective from the PfPC Emerging Security Challenges Working Group

Jean-Marc Rickli* and *Gëzim Vllasi

Geneva Centre for Security Policy, Switzerland, https://gcsp.ch

Abstract: This article examines the shift in international security from traditional threat-centric models to risk-based approaches, focusing on the role of emerging technologies in shaping perceptions and responses. While offering significant benefits, emerging technologies such as artificial intelligence, biotechnology, and quantum computing have also created new vulnerabilities, particularly when weaponized. Traditional state-centric security frameworks are inadequate in addressing these risks, especially as non-state actors gain access to these powerful technologies. The article categorizes global risks into catastrophic and existential types, exploring how their management demands a shift in risk analysis methods and proactive strategies. It advocates for a multi-stakeholder approach and global cooperation to enhance resilience, with a particular focus on NATO's adaptive strategies for combatting cyber, cognitive, and hybrid threats.

Keywords: global risks, emerging technologies, risk management, catastrophic risk, existential risk, weaponization, artificial intelligence, synthetic biology, neurotechnology, cognitive warfare, quantum computing.

Introduction

In the modern security environment, security policy discussions have shifted from a traditional countering-threat model to a "management of risks" approach. This evolution reflects the growing complexity of international relations and the ever-changing global security landscape, making the shift crucial for navigating current and future international security challenges. In the context of emerging technologies, such as artificial intelligence (AI) and biotechnology, new approaches are essential for proactively managing global risks.

Traditionally, threats were identified through an approach that focused on assessing the capabilities and intentions of potential actors[1] (very often state actors) to do harm. However, this approach often overlooked the complexities introduced by non-state actors and the new vulnerabilities arising from new and emerging technologies. The increasing number of non-state actors, such as terrorist or criminal organizations and multinational corporations, along with the potential security threats posed by individuals empowered by modern technologies, are transforming how risks evolve and should be managed. As the international system becomes increasingly unpredictable and interdependent, the number of actors capable of causing harm has grown substantially, expanding the attack surface of any organization.

Given the changing nature of the international system, a risk-based approach to security has become essential as traditional models struggle to adapt to the complexities and interconnectedness of new risks. This shift demands a new risk management framework that accounts for the dynamic and often unpredictable nature of emerging risks. Traditional methods of security policy-making, which rely heavily on predetermined outcomes, are increasingly inadequate in a world where risks are multifaceted and rapidly evolving. A risk-based approach, by contrast, emphasizes the ability to adapt, anticipate potential effects, and consider the interdependencies of various global risks. As strategic considerations expand to include not only military risks but also societal, economic, and technological challenges, policymakers must shift their focus from traditional defense models to frameworks that offer flexibility and proactive management of diverse and interconnected risks.

The severity of a risk is determined by its scope (how many people—and other morally relevant beings—would be affected), its intensity (how badly these individuals would be affected), and its probability (how likely the disaster is to occur).[2] These factors become especially critical in the context of emerging technologies, which this article examines in relation to international security and risk management. Exploring how risk definitions and management approaches evolve alongside new security challenges, it provides a framework for understanding risk in today's environment, where emerging technologies are increasingly weaponized.

As security challenges grow more complex, risk management has evolved from merely identifying threats to actively addressing them. This shift in perspective recognizes that threats are interconnected and require a comprehensive approach for effective mitigation. Today's risks demand a holistic framework that

[1] David Strachan-Morris, "Threat and Risk: What Is the Difference and Why Does It Matter?" *Intelligence and National Security* 27, no. 2 (2012): 172-186, https://doi.org/10.1080/02684527.2012.661641.

[2] Nick Bostrom and Vlatko Vedral Cirkovic, eds., *Global Catastrophic Risks* (Oxford: Oxford University Press, 2008).

evaluates impact and likelihood, emphasizing the limitations of traditional models that focus solely on capabilities and intentions.

In this evolving landscape, emerging technologies—such as artificial intelligence, biotechnology, and cyber capabilities—are transforming the nature and impact of risks, necessitating thorough risk assessments and proactive strategies. This article explores the transformative roles these technologies play in shaping current security risks and examines their implications for international security and policy frameworks. It emphasizes the need for adaptive responses in an interconnected world.

This article provides a comprehensive overview of the impact of emerging technologies on security challenges structured as follows. First, it defines the various risks associated with these technologies, categorizing them into global, catastrophic, and existential risks. Following this definition, the article discusses the new types of risks that derive from emerging technologies such as artificial intelligence, quantum computing, and synthetic biology. The subsequent section explores how these technologies can be weaponized. This is followed by an assessment of how to adapt risk analysis to account for these new types of risks. The article then highlights the contributions of the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group to these discussions, addressing key topics such as artificial intelligence, swarming technologies, cybersecurity, hybrid threats, cognitive warfare, neurotechnology, generative AI, synthetic biology, and global power shifts. The article concludes by emphasizing the need for proactive strategies to mitigate the risks posed by emerging technologies in order to manage and enhance global security.

Defining Risks: Global, Catastrophic and Existential

The transition from a threat-based to a risk-based approach reflects a deeper understanding of modern security complexities. Beck refers to these as “manufactured risks” [3] created by human activity, particularly through technological advancements. Unlike natural risks, manufactured risks transcend national borders, making them a critical focus of contemporary risk management and security policies.[4] For Beck, modernity represents a transformative phase in which traditional industrial societies evolve, driven by technological and social changes. This evolution is characterized by what he calls “reflexive modernization,” [5]—indicating that society is increasingly aware of its own risks and consequences—rather than merely pursuing progress as understood by earlier frameworks.

This shift is underscored by the inherent uncertainty associated with new technologies. Despite the growing role of foresight approaches in security anal-

[3] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE, 1992).

[4] Beck, *Risk Society: Towards a New Modernity*.

[5] Beck, *Risk Society: Towards a New Modernity*.

ysis, the inherent uncertainty surrounding the potential and evolution of emerging technologies introduces unprecedented new potential risks.[6] For instance, the growing role of autonomy in AI-enabled weapons or cyber warfare introduces risks that are very difficult to anticipate fully.[7] In addition, the continuously evolving nature of these risks highlights the need for continuous adaptation in policy frameworks and strategic planning.

As these risks become more complex, the academic literature on international security has expanded, focusing on new types of risks. A risk-based environment requires clarity on the definitions of global catastrophic risks (GCRs) and existential risks (X-risks) and how they differ from traditional security threats. Global catastrophic risks and existential risks must be examined through the lens of networked vulnerability. These risks are no longer confined to the actions of states but are now driven by the complex interdependence among states, non-state actors, and technological infrastructures. For instance, an AI-driven cyberattack could disrupt global financial systems [8] – a risk that cannot be mitigated by state actors alone.

When defining catastrophic and existential risks, there is a tendency to define them through their quantitative impact. Millett and Snyder-Beatti [9] define catastrophic risks as those leading to the death of 100 million people. However, such

[6] Adrian Currie and Seán Ó hÉigeartaigh, "Working Together to Face Humanity's Greatest Threats: Introduction to the Future of Research on Catastrophic and Existential Risk," *Futures* 102 (2018): 1-5, https://doi.org/10.1016/j.futures.2018.07.003.

[7] Vincent Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv preprint arXiv:1802.07228, 2018, last revised December 1, 2024, https://doi.org/10.48550/arXiv.1802.07228. See also, Jean-Marc Rickli, "The Strategic Implications of Artificial Intelligence," in *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, ed. Al Naqvi and J. Mark Munoz (London: Anthem Press, 2020), 41-54.

[8] Rehab Osman and Sherif El-Gendy, "Interconnected and Resilient: A CGE Analysis of AI-Driven Cyberattacks in Global Trade," *Risk Analysis* (2024), https://doi.org/10.1111/risa.14321.

[9] Piers Millett and Andrew Snyder-Beattie, "Existential Risk and Cost-Effective Biosecurity," *Health Security* 15, no. 4 (2017): 373-383, https://doi.org/10.1089/hs.2017.0028; Owen Cotton-Barratt et al., *Global Catastrophic Risk Annual Report 2016* (Global Challenges Foundation and Global Priorities Project, 2016), https://globalprioritiesproject.org/wp-content/uploads/2016/04/Global-Catastrophic-Risk-Annual-Report-2016-FINAL.pdf. Instead, a more functional approach looks at existential risks as those that critically compromise essential functions necessary for the long-term survival of an organization, society, or species. For example, Stanford's Existential Risks Conference supports viewing existential risks as those that threaten to permanently incapacitate core functions or infrastructure needed for societal resilience, rather than focusing solely on mortality numbers. This includes threats like climate destabilization, AI misalignment, or bioengineered pathogens, which may severely disrupt key societal functions even without directly causing a specific number of deaths. Such risks require resilience-focused frameworks that build capacity in vital functions to withstand

thresholds are arbitrary. If a disaster causes 99 million deaths, does it no longer qualify as catastrophic or existential? Toby Ord critiques the limitations of defining risks purely by quantitative measures, such as the number of deaths. He argues that while quantitative measures provide a clear threshold, they often fail to capture broader impacts on humanity's long-term potential.[10]

We argue for a more comprehensive approach that considers the functional impact of risks—specifically, how they affect the essential functions necessary for humanity's survival and proper functioning. Instead of relying solely on quantitative indicators, risks should be defined by their *impact* on the critical functions an organization or system must perform to survive and perform effectively.

Every organization or individual has centers of gravity, defined as functions that, if lost, lead to the collapse or death of the entity.[11] For instance, humans have four centers of gravity: they must eat, drink, breathe, and sleep. If any of these functions are lost, survival becomes impossible. Thus, existential risks can be more effectively defined as those that threaten the very existence of an entity, whether it is an organization, group, or individual. Existential risks are those that undermine *vital functions*, essential for survival.

Catastrophic risks, on the other hand, can be defined as those that disrupt the proper execution of an entity's *key functions* that, if lost, would lead to its collapse. By analyzing vital and key functions, we can conduct a more granular assessment, as each organization has different functions crucial for its survival or proper operation.

This approach also facilitates the development of strategies to counter such risks through the concept of resilience,[12] defined as the ability of an organization to absorb shocks while continuing to function. Therefore, once the vital and key functions of an organization are identified, a resilience strategy can focus on protecting these functions.

Global risks are inherently transnational in nature and encompass threats that affect multiple countries or populations, often interconnected, amplifying their impact. A recent RAND report, for instance, identifies six major global

shocks and adapt – a concept frequently championed in resilience research. See "Stanford Existential Risks Conference," https://cisac.fsi.stanford.edu/events/stanford-existential-risks-conference-0.

[10] Benedikt Namdar and Thomas Pölzler, "Toby Ord, The Precipice: Existential Risk and the Future of Humanity, Bloomsbury, 2020," *Ethical Theory and Moral Practice* 24 (2021): 855-857, https://doi.org/10.1007/s10677-021-10181-9.

[11] Antulio J. Echevarria II, "Clausewitz's Center of Gravity: It's Not What We Thought," *Naval War College Review* 56, no. 1 (2003): 108-123, https://digital-commons.usnwc.edu/nwc-review/vol56/iss1/6.

[12] Stephanie Duchek, "Organizational Resilience: A Capability-Based Conceptualization," *Business Research* 13 (2020): 215246, https://doi.org/10.1007/s40685-019-0085-7. See also Igor Linkov et al., "Applying Resilience to Hybrid Threats," *IEEE Security and Privacy* 17, no. 5 (2019): 78-83, https://doi.org/10.1109/MSEC.2019.2922866.

threats: artificial intelligence, asteroid and comet impacts, climate change, nuclear war, severe pandemics (both natural and synthetic), and supervolcanoes.[13]

The term "global catastrophic risk" has recently emerged in the literature. Similar to the discussion above, it lacks a precise definition but generally refers to risks with the potential to inflict severe harm to human health or survival on a global scale.[14] GCRs can thus be defined as high-impact hazards that could trigger failures in critical systems essential for human survival.[15] Avin and coworkers[16] classify GCRs into two categories: *natural risks*, such as pandemics or asteroid impacts, which are beyond human control or very difficult to manage but still pose threats to global stability, and *anthropogenic risks*, such as nuclear war, AI misalignment, or biotechnology hazards, where human actions could lead to far-reaching, unintended consequences.

A significant subset of global catastrophic risks is existential risks, defined as those that threaten the extinction of intelligent life or permanently and drastically reduce its quality. The key distinction is that "existential catastrophes curtail the possibility of recovery and future development."[17] For example, while a global financial crisis could severely disrupt society and thus represent a catastrophic risk, an existential catastrophe—such as a global pandemic with an unknown pathogen or nuclear war—could destroy civilization's capacity to rebuild and lead to its extinction.[18]

The interdependence of nations, populations, and global infrastructure within the global economy means that risks in one area can trigger cascading effects elsewhere. Unlike traditional security threats, which could often be addressed within national borders, global risks necessitate multinational cooperation to safeguard global commons – defined as "those parts of the planet that fall outside national jurisdictions and to which all nations have access."[19] The COVID-19 pandemic is a recent example of a global risk where no single country could effectively mitigate the threat alone.

[13] Henry H. Willis, Anu Narayanan et al., *Global Catastrophic Risk Assessment,* Research Report RRA2981, October 30, 2024, https://www.rand.org/pubs/research_reports/RRA2981-1.html.

[14] Clarissa Rios Rojas et al., *Building the Science-Policy Interface for Tackling Global Governance of Catastrophic and Existential Risks* (University of Cambridge, 2023), https://www.cser.ac.uk/resources/report-building-science-policy-interface-tackling-global-governance-catastrophic-and-existential-risks/.

[15] Rojas et al., *Building the Science-Policy Interface for Tackling Global Governance of Catastrophic and Existential Risks*.

[16] Shahar Avin, Bonnie C. Wintle, Julius Weitzdörfer, Seán S. Ó hÉigeartaigh, William J. Sutherland, and Martin J. Rees, "Classifying Global Catastrophic Risks," *Futures* 102 (2018): 20-26, https://doi.org/10.1016/j.futures.2018.02.001.

[17] Currie and Ó hÉigeartaigh, "Working Together to Face Humanity's Greatest Threats."

[18] Bostrom and Cirkovic, *Global Catastrophic Risks.*

[19] United Nations, *Global Governance: A New Approach to Address Global Challenges* (New York: United Nations, 2013), 5.

Therefore, the literature on global risks emphasizes the need for international cooperation and collective action to mitigate them. For instance, Schwartz and Randall[20] have explored the complexities of forecasting and managing global risks, advocating for a more integrated approach to addressing these issues. Their integrated approach focuses on scenario planning, interdisciplinary analysis, proactive risk mitigation, and international collaboration to enhance resilience against climate change and global risks.[21] Similarly, Currie and Ó hÉigeartaigh[22] emphasize that X-risks often require global cooperation, as they arise from multiple sources that extend beyond national interests. Their work highlights the need for international governance frameworks to manage risks such as AI-driven conflicts or biological warfare effectively. This argument echoes Beck's concept of "reflexive modernization,"[23] where society continually confronts the side effects of its technological advancements.

In line with this perspective, the 2023 report from the Centre for the Study of Existential Risk stresses that addressing catastrophic and existential risks demands robust frameworks integrating science, policy, and international collaboration to ensure timely and effective responses.[24] To bridge the gap between science and policy, Turchin and Denkenberger[25] propose a framework that communicates to policymakers the severity and likelihood of both existential and global catastrophic risks. This structured communication is crucial for international security institutions like NATO, which must address these emerging risks and adapt their policies accordingly. Recognizing this necessity, NATO's Emerging Security Challenges Division now focuses on issues such as cyber warfare, AI governance, and biotechnology, acknowledging that these challenges transcend traditional military concerns and are of national security importance.

The next section analyses the impact of emerging technologies on new risks.

New Risks and Security Challenges Stemming from Emerging Technologies

Emerging technologies, such as artificial intelligence, quantum computing, and synthetic biology, are fundamentally reshaping the international security envi-

[20] Peter Schwartz and Doug Randall, *An Abrupt Climate Change Scenario and Its Implications for United States National Security* (Minneapolis, MN: Institute for Agriculture and Trade Policy, October 2003), 20-21, https://www.iatp.org/documents/abrupt-climate-change-scenario-and-its-implications-united-states-national-security.

[21] Schwartz and Randall, *An Abrupt Climate Change Scenario and Its Implications*.

[22] Currie and Ó hÉigeartaigh, "Working Together to Face Humanity's Greatest Threats."

[23] Beck, *Risk Society: Towards a New Modernity*.

[24] Rojas et al., *Building the Science-Policy Interface for Tackling Global Governance of Catastrophic and Existential Risks*.

[25] Alexey Turchin and Daniel Denkenberger, "Global Catastrophic and Existential Risks Communication Scale," *Futures* 102 (2018): 27-38, https://doi.org/10.1016/j.futures.2018.01.003.

ronment. While these technologies hold significant promise for advancing humanity, they also present considerable risks due to their dual-use nature.[26] As noted in a recent report by the Center for International Governance Innovation, these technologies can provide substantial socio-economic benefits through increased productivity. However, they also pose risks that may undermine entire societies, including livelihoods and social norms.[27]

The complexity of assessing risks in these areas cannot be overstated. AI, for example, is increasingly embedded in digital and robotic applications, including military and defense systems, offering both opportunities and substantial risks. AI and AI-enabled systems are deployed on battlefields in command and control systems or weapon systems, such as increasingly autonomous drones. Their performance is expected to surpass that of humans in many tasks, and they are already outpacing humans in speed of execution and data processing.[28] With growing autonomy, technology is increasingly becoming an actor in warfare, potentially serving as a surrogate.

The potential for AI misalignment, misuse, or malicious use calls for new global governance structures and international agreements to regulate the emerging domain of AI-enabled autonomy.[29] For instance, since 2015, the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS) has debated whether LAWS should be banned. So far, no agree-

[26] The terms "dual-use" and "multi-use" in relation to emerging technologies have been used differently by scholars. For example, "dual-use" has multiple meanings depending on the context – see Jonathan B. Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (MIT Press, 2012). It can describe materials, hardware, and knowledge that have peaceful applications but could be exploited for the illicit production of nuclear, chemical, or biological weapons. These technologies pose a "dual-use" dilemma because it is challenging to prevent their misuse without forgoing beneficial applications. Thea Riebe, *Technology Assessment of Dual-Use ICTs – How to Assess Diffusion, Governance and Design* (Springer Nature, 2023) emphasizes the diffusion of innovation between civilian and military industrial sectors. The concept of "multi-use" in scholarly literature extends beyond dual use, making it suitable for a wide range of contexts. Emerging technologies can be described as "multi-use" – see, for example, Margaret E. Kosal, ed., *Proliferation of Weapons- and Dual-Use Technologies* (Cham: Springer, 2021).

[27] Paul Samson, S. Yash Kalash, Nikolina Zivkovic, Tracey Forrest, and Bessma Momani, *Scenarios of Evolving Global Order*, Special Report (Waterloo, ON, Canada: Centre for International Governance Innovation, 2024), 21, https://www.cigionline.org/static/documents/Scenarios_of_Evolving_Global_Order.pdf.

[28] Nestor Maslej et al., *AI Index Report 2024* (Stanford, CA: Institute for Human-Centered AI, Stanford University, April 2024), https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf.

[29] Stephen Herzog and Dominika Kunertova, "NATO and Emerging Technologies – Alliance's Shifting Approach to Military Innovation," *Naval War College Review* 77, no. 2 (2024): 47-69, https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/5/.

ment has been reached aside from a set of eleven non-binding guiding principles.[30] Parallel initiatives, such as the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy,[31] demonstrate that states are increasingly concerned with the weaponization of AI and autonomy. Although these initiatives are a welcome step toward norm creation, they lack global consensus, especially among major powers and states driving the development of these technologies.

Adding another layer of complexity to this landscape is the role of non-state actors, such as terrorist groups, organized crime organizations, and multinational corporations. Whereas multinational corporations in the technology or critical infrastructure sectors are often excluded from national security discussions, even though their activities and products could have massive international security implications, malicious non-state actors and even some individuals leverage emerging technologies to amplify their impact for nefarious and criminal purposes.[32]

Addressing these interconnected risks requires a broader risk analysis perspective that extends beyond the strictly military dimension. Governments and international security organizations must adapt their risk management frameworks to include non-traditional security actors and emerging technologies. For example, Al-Qaeda's attacks on September 11, 2001, demonstrated the capacity of non-state actors to cause global disruption using rudimentary technology. ISIS was the first organization to understand how to weaponize social media, combining the virality of these platforms with the horror of crude execution videos. Organized crime organizations increasingly exploit the cyber realm, creating substantial threats to global security with concrete costs. The cost of cybercrime is projected to surpass $ 10 trillion by 2025.[33] By comparison, the global war on terror is estimated to have cost the U.S. government $ 5.4 trillion from 2001 to 2020.[34] As these groups operate transnationally, it is very difficult for states to act against them alone, as they evade traditional legal enforcement's jurisdiction.[35]

[30] Group of Governmental Experts on Lethal Autonomous Weapons Systems, *Final Report* (United Nations, 2019).

[31] "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," U.S. Department of State, November 9, 2023, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/.

[32] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford, Oxford University Press, 2020).

[33] Ani Petrosyan, "Estimated Cost of Cyber Crime Worldwide 2018-2029," *Statista*, July 30, 2024, https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

[34] Veera Korhonen, "Total Budgetary Cost to the United States of the Global War on Terror between FY 2001 and FY 2020, by Category," *Statista*, August 9, 2024, www.statista.com/statistics/1075849/total-us-war-costs-war-terror-category/.

[35] Wookyung Jung and Sean Doyle, "Police Agencies Must Partner Up to Prevent a Ransomware Crisis – Here's How," World Economic Forum, November 12, 2021.

Companies operating in the technology, telecommunications, and energy sectors can also significantly impact national security, whether through data breaches, supply chain vulnerabilities, or environmental impacts.[36] For instance, a CrowdStrike update in July 2024 caused the largest IT outage in history, costing Fortune 500 companies over $ 5.4 billion.[37] The actions of these non-state actors frequently fall beyond the control of individual governments, complicating the landscape of international security governance and thus necessitating innovative, cooperative, and multi-stakeholder approaches.

These transformations require a shift in how security threats are perceived. While conventional military threats still exist and have re-emerged since the war in Ukraine, the power granted to non-state actors and individuals by the proliferation of emerging technologies has blurred the lines between combatants and civilians, creating a more complex security environment.[38] The democratization of powerful technologies means that individuals or small groups could potentially develop biological weapons or launch cyberattacks with global consequences. It also increasingly empowers individuals or companies whose actions could have international security implications. Furthermore, the increasing AI-enabled autonomy of machines necessitates the involvement of non-state actors in serious global risk analysis.

For instance, while conflict escalation between states has been extensively studied and modeled, there is limited understanding of how such dynamics might evolve with the incorporation of autonomous elements in nuclear command, control, and communications (C3) [39] systems. Although conventional and nuclear C3 systems [40] are potential areas for increased autonomy, current policies and trends emphasize that humans must remain in the decision-making

https://www.weforum.org/stories/2021/11/police-agencies-must-partner-up-to-prevent-a-ransomware-crisis-heres-how/.

[36] Jean-Marc Rickli and Christina Liang, "New and Emerging Technologies for Terrorists," in *The Routledge Companion to Terrorism Studies*, ed. Max Abrahms (London: Routledge, 2024), Chapter 15.

[37] Sean Michael Kerner, "Crowdstrike Outage Explained: What Caused it and What's Next," *Techtarget*, October 29, 2024, https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

[38] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2023).

[39] João Eduardo Costa Gomes et al., "Surveying Emerging Network Approaches for Military Command and Control Systems," *ACM Computing Surveys* 56, no. 6 (2024): 1-38, https://doi.org/10.1145/3626090.

[40] The Geneva Centre for Security Policy (GCSP) in cooperation with Strategic Foresight Group (SFG) has steered a process of dialogue for thought leaders from P5 countries (China, France, Russia, UK, and USA) on global catastrophic risks with a focus on the application of AI and other technologies in the nuclear command, control, and communications including decision support infrastructure. For more detailed information, refer to: Strategic Foresight Group, "Roundtable on AI-NC3 Interface," December 6, 2024, https://www.strategicforesight.com/news_inner.php?id=228; Strategic Foresight Group, "P5 Experts' Roundtable on Nuclear Risk Reduction: Co-Convenors'

loop. A useful analogy for analyzing potential risks could be drawn from flash crashes in high-frequency trading,[41] illustrating the unintended consequences of such systems. In this context, a cautious approach to risk management would involve examining the implications of crisis escalation in scenarios where autonomous technologies play a supporting role.

Consequently, traditional military strategies and risk analysis frameworks are no longer sufficient to understand and manage these complexities, thereby requiring comprehensive strategies that integrate technological and foresight-based solutions while developing new governance structures to manage the risks posed by emerging technologies effectively.

The Weaponization of Emerging Technologies

Emerging technologies are transforming the global security landscape in ways that require policymakers to anticipate new challenges. The weaponization of AI, synthetic biology, quantum computing, and neurotechnologies represents new national and international security risks.

AI is increasingly integrated into military and intelligence operations worldwide. AI-driven tools are used for everything from surveillance to cyber defense, as force multipliers for legacy platforms, or as new weapons such as drones.[42] However, the risks associated with the weaponization of AI are substantial, ranging from misuse of the technology to purposefully malicious uses of AI.[43] For instance, adversarial AI, where AI systems are manipulated to produce harmful or incorrect outcomes, represents a growing threat to military and civilian systems. An adversary could exploit vulnerabilities in an AI system to misdirect an autonomous drone or disrupt critical military communications.[44]

Summary," Geneva, December 11-13, 2023, https://www.strategicforesight.com/conference_pdf/Geneva%20Roundtable%20Report.pdf; "P5 Experts Roundtable Online Meeting: AI-Nuclear Nexus, 24 June 2024," *GCSP News*, www.gcsp.ch/global-insights/p5-experts-roundtable-online-meeting-ai-nuclear-nexus-24-june-2024. See also Alice Saltini, "AI and Nuclear Command, Control and Communications: P5 Perspectives," *European Leadership Network,* November 13, 2023, https://europeanleadershipnetwork.org/report/ai-and-nuclear-command-control-and-communications-p5-perspectives/.

[41] Christian Borch, "High-Frequency Trading, Algorithmic Finance and the Flash Crash: Reflections on Eventalization," *Economy and Society* 45, no. 3-4 (2016): 350-378, https://doi.org/10.1080/03085147.2016.1263034.

[42] K. LNC Prakash, Santosh Kumar Ravva, M.V. Rathnamma, and G. Suryanarayana, "AI Applications of Drones," in *Drone Technology: Future Trends and Practical Applications*, ed. Sachi Nandan Mohanty et al. (Scrivener Publishing, 2023), https://doi.org/10.1002/9781394168002.ch7.

[43] Brundage et al., "The Malicious Use of Artificial Intelligence," 7.

[44] "Weapons Powered by Artificial Intelligence Pose a Frontier Risk and Need to Be Regulated," World Economic Forum, June 23, 2021, https://www.weforum.org/stories/2021/06/the-accelerating-development-of-weapons-powered-by-artificial-risk-is-a-risk-to-humanity/.

Advancements in *synthetic biology* have enhanced our understanding of disease mechanisms and enabled the development of innovative medical therapeutics.[45] However, these technologies also pose significant biosecurity risks, as they may allow the recreation of dangerous pathogens without access to natural sources.[46] For instance, it would be theoretically possible to synthetically engineer a new type of pathogen.

Natural pathogens are either lethal or viral but cannot be both, as they would kill the host before being able to spread.[47] However, modern biotechnology and synthetic biology techniques enable the creation of new viruses and bacteria. This includes creating pathogens from scratch and modifying existing ones to be more transmissible or deadly.[48] Additionally, it is possible to engineer living systems to enhance growth and increase pathogenicity, with these modified bacteria and viruses potentially adapted for belligerent purposes.[49] Thus, governments and international organizations must develop new governance structures to address these challenges and ensure the responsible use of synthetic biology.

Although the militarization of *quantum computing* has not yet materialized, it holds the potential to render existing encryption methods obsolete, creating new vulnerabilities in everything from military communications to global financial systems.[50] Such technologies could be used to "decrypt cybersecurity protocols, vastly improve navigation systems, and design and fabricate components for weapons of mass destruction." [51]

The developments of increasingly *immersive technologies*, such as metaverses and neurotechnologies—which could be both invasive and non-invasive—aim to influence human cognition and decision-making. The militariza-

[45] Cassidy Nelson, "Engineered Pathogens: The Opportunities, Risks and Challenges," *Biochemist* 41, no. 3 (2019): 34-39, https://doi.org/10.1042/BIO04103034.

[46] Kevin M. Esvelt, "Delay, Detect, Defend: Preparing for a Future in which Thousands Can Release New Pandemics," *Geneva Papers* 29/22, Geneva Centre for Security Policy, November 14, 2022, https://www.gcsp.ch/publications/delay-detect-defend-preparing-future-which-thousands-can-release-new-pandemics.

[47] Samuel Alizon, A.K. Hurford, N. Mideo, and M. van Baalen, "Virulence Evolution and the Trade-Off Hypothesis: History, Current State of Affairs and the Future," *Journal of Evolutionary Biology* 22, no. 2 (2009): 245-259, https://doi.org/10.1111/j.1420-9101.2008.01658.x.

[48] Nelson, "Engineered Pathogens," 34.

[49] J. Kenneth Wickiser et al., "Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology," *CTC Sentinel* 13, no. 8 (2020): 1-7, https://ctc.westpoint.edu/engineered-pathogens-and-unnatural-biological-weapons-the-future-threat-of-synthetic-biology/.

[50] Emily Grumbling and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019), 12, https://doi.org/10.17226/25196.

[51] Herzog and Kunertova, "NATO and Emerging – Alliance's Shifting Approach to Military Innovation."

tion of these technologies will alter the nature of warfare by adding a sixth domain[52] – cognition and the human brain. *Cognitive warfare* refers to "activities designed to control others' mental states and behaviors."[53] It is about controlling how and what people think in order to influence how they act. Cognitive warfare encompasses information warfare, which aims to control the flow of information to influence behavior.[54] Trying to influence behavior is nothing new. What is new, though, is the granularity, precision, and scale that emerging technologies afford. For instance, the current debate in the United States over whether TikTok should be banned highlights how powerful social media can influence an entire generation of users by pushing specific narratives.[55]

Combining immersive technologies and *neurotechnologies* creates unprecedented possibilities for measuring the impact of external stimuli (e.g., from the metaverse) on a subject's emotional response. Advances in invasive neurotechnologies, especially in brain-computer interfaces (BCIs), allow for the stimulation of neurons and altering their responses. One could imagine a future where such technologies could potentially manipulate thoughts and thought patterns with remarkable precision. The proliferation of these technologies could allow for a level of individual manipulation on a global scale that has never been seen in the history of manipulation or persuasion.

If this becomes a reality, physical violence would no longer be required to compel an adversary to change their mind, which is the objective of war as postulated by Clausewitz, who defines war as an act of force to compel the enemy to do one's will.[56] Such technological developments would fundamentally alter the nature of warfare itself – something no previous technology has managed to achieve. It is worth mentioning that although these technologies are not yet mature enough to realize such capabilities, they have already demonstrated impressive results. For example, BCIs are already used to treat psychiatric disorders

[52] The established domains of warfare are land, air, sea, space, and cyber.

[53] Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," *Journal of Global Security Studies* 7, no. 4 (December 2022): ogac016, https://doi.org/10.1093/jogss/ogac016.

[54] Marie Morelle, Cegarra Julien, Damien Marion, and André Jean-Marc, "Towards a Definition of Cognitive Warfare," Conference on Artificial Intelligence for Defense, DGA Maîtrise de l'Information, November 2023, Rennes, France, https://hal.archives-ouvertes.fr/hal-04328461.

[55] David McCabe, "TikTok Faces U.S. Ban After Losing Bid to Overturn New Law," *The New York Times*, December 6, 2024, https://www.nytimes.com/2024/12/06/business/media/tiktok-ban-court-decision.html; Evelyn Douek, "The Government's Disturbing Rationale for Banning TikTok," *The Atlantic*, December 12, 2024, www.theatlantic.com/ideas/archive/2024/12/social-media-national-security-ban/680963/.

[56] Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton University Press, 1976), 75.

such as epilepsy,[57] and the combination of functional MRI with algorithms increasingly enables machines to read what people see.[58] Mind reading is no longer science fiction and is within reach of military applications. The next step in these developments will be mind writing, although it is still technologically distant.

Nonetheless, the potential of these advancements has led NATO to take cognitive warfare seriously, publishing several studies on the topic and highlighting the significance of this new form of warfare enabled by emerging technologies.[59]

Given the rapid pace of technological change, risk analysis and security policies must increasingly address the implications of these emerging technologies. The traditional security toolkit, designed to manage state-based threats, is inadequate for tackling the multifaceted risks posed by the malicious use and/or weaponization of AI, synthetic biology, quantum computing, or neurotechnologies.[60] Additionally, non-state actors and individuals empowered by advanced technologies add another layer of complexity to risk analysis. Hackers, criminal organizations, and even individuals now possess the power to cause widespread harm through means such as cyberattacks, biotechnological experiments, or AI-driven disinformation.

Risk Assessment

The concept of risk lacks a universally accepted definition, encompassing interpretations centered on probability, expected outcomes, hazards, or uncertainties.[61] As international security evolves, traditional risk frameworks must adapt to address complex challenges, particularly those posed by technologies like artificial intelligence and synthetic biology.[62] These technologies introduce inter-

[57] Xiaoke Chai et al., "Brain-Computer Interface Digital Prescription for Neurological Disorders," *CNS Neuroscience & Therapeutics* 30, no. 2 (2024): e14615, https://doi.org/10.1111/cns.14615.

[58] Kamal Nahas, "AI Re-Creates What People See by Reading Their Brain Scans," *Science*, March 7, 2023, https://www.science.org/content/article/ai-re-creates-what-people-see-reading-their-brain-scans.

[59] Yvonne R. Masakowski and Janet M. Blatny, "Mitigating and Responding to Cognitive Warfare," *STO Technical Report* TR-HFM-ET-356 (Paris: NATO Science and Technology Organization, 2023).

[60] Ricardo Chavarriaga, Jean-Marc Rickli, and Federico Mantellassi, "Neurotechnologies: The New Frontier for International Governance," *Strategic Security Analysis* 29, Geneva Centre for Security Policy, April 2023, https://dam.gcsp.ch/files/doc/ssa-2023-issue29.

[61] Terje Aven, "The Risk Concept – Historical and Recent Development Trends," *Reliability Engineering & System Safety* 99 (2012): 33-44, https://doi.org/10.1016/j.ress.2011.11.006.

[62] Doug Irving, "Artificial Intelligence and Biotechnology: Risks and Opportunities," RAND, March 21, 2024, https://www.rand.org/pubs/articles/2024/artificial-intelligence-and-biotechnology-risks-and.html.

connected risks that demand novel approaches for accurate assessment and effective mitigation.[63] For example, the "black box" issue,[64] where algorithmic decision-making lacks transparency,[65] creates potential cross-domain impacts. When combined, technologies such as AI and synthetic biology amplify complexity due to the compounding effects of their interactions.

These merging risks necessitate proactive strategies, such as scenario analysis and environmental scanning,[66] to anticipate threats more effectively. The convergence of AI and biological systems presents security concerns that exceed the scope [67] of conventional frameworks, particularly through nonlinear risk escalation,[68] where impacts increase disproportionately relative to initial probability or severity. Climate change exemplifies this dynamic, amplifying issues like resource scarcity and geopolitical instability, which complicate single-domain [69] responses and highlight the need for risk models equipped to handle interconnected systems.

[63] Volkan Evrin, "Risk Assessment and Analysis Methods: Qualitative and Quantitative," *ISACA Journal* 2 (April 2021), https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods; Sanober Naheed, "Understanding Disaster Risk Reduction and Resilience: A Conceptual Framework," in *Handbook of Disaster Risk Reduction for Resilience*, ed. Saeid Eslamian and Faezeh Eslamian (Cham: Springer, 2021), 1-25, https://doi.org/10.1007/978-3-030-61278-8_1.

[64] Bartosz Brożek, Michał Furman, Marek Jakubiec, and Bartłomiej Kucharzyk, "The Black Box Problem Revisited. Real and Imaginary Challenges for Automated Legal Decision Making," *Artificial Intelligence and Law* 32 (2024): 427-440, https://doi.org/10.1007/s10506-023-09356-9; Vikas Hassija et al., "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence," *Cognitive Computation* 16, no. 1 (2024): 46, https://doi.org/10.1007/s12559-023-10179-8.

[65] Vikas Hassija et al., "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence," *Cognitive Computation* 16, no. 1 (2024): 45-74, https://doi.org/10.1007/s12559-023-10179-8.

[66] Mary Carmichael, "Eight Overlooked Emerging Tech Risks and How to Mitigate Them," *@ISACA* 9, May 6, 2024, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-9/eight-overlooked-emerging-tech-risks-and-how-to-mitigate-them.

[67] Sarah R. Carter, Nicole E. Wheeler, Sabrina Chwalek, Christopher R. Isaac, and Jaime Yassif, *The Convergence of Artificial Intelligence and the Life Sciences*, Nuclear Threat Initiative, October 30, 2021, https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/; Katarzyna Adamala et al., "Confronting Risks of Mirror Life," *Science*, December 12, 2024, https://doi.org/10.1126/science.ads9158.

[68] Pablo Gutiérrez Cubillos and Roberto Pastén, "Nonlinear Risks: A Unified Framework," *Theory and Decision* 95 (2023): 11-32, https://doi.org/10.1007/s11238-022-09912-w.

[69] Roshanka Ranasighe et al., "Climate Change Information for Regional Impact and for Risk Assessment," in *Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*, ed. Valerie Masson-Delmotte et al. (Cambridge University Press, 2021), 1767-1926, https://doi.org/10.1017/9781009157896.

To improve risk assessment, it is essential to incorporate systemic interconnectedness and the evolving nature of technologies, resulting in a more comprehensive risk assessment.[70] Network analysis, which has proven effective in fields such as finance and cybersecurity, can provide insights into how risks propagate across interconnected systems, identifying vulnerabilities at critical junctures.[71] Applied to AI and biotechnology, this approach could uncover dependencies that traditional models overlook, facilitating more effective risk management.

Predictive analytics and probabilistic models, such as Monte Carlo simulations,[72] enhance accuracy by providing decision-makers with actionable insights for preemptive action. The inherent interdependence of technologies like AI and synthetic biology makes it difficult to assess them in isolation. Network effects, where the failure or misuse of one component impacts multiple systems, very often in a cascading manner, highlight the need for systemic risk analysis. For instance, autonomous AI systems may introduce unexpected network effects that disrupt essential infrastructure.[73] Complexity science and network analysis[74] can quantify these interdependencies, enabling comprehensive risk management frameworks that address the demands of an interconnected world.

In an increasingly complex and rapidly evolving threat landscape, decision-makers must prioritize adaptability and robustness in their strategies. Traditional predictive models often fall short when faced with novel or unexpected challenges. By focusing on these principles, organizations can develop systems capable of responding to scenarios that exceed conventional predictions, ensuring greater resilience in the face of uncertainty. This approach is particularly important when dealing with the integration of advanced technologies like artificial intelligence, which introduces not only technical risks but also profound ethical and societal implications.[75] For instance, deploying autonomous systems raises

[70] Monica Billio, Mila Getmansky, Andrew W. Lo, and Loriana Pelizzon, "Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors," *Journal of Financial Economics* 104, no. 3 (2012): 535-559, https://doi.org/10.1016/j.jfineco.2011.12.010.

[71] David Forscey, Jon Bateman, Nick Beecroft, and Beau Woods, *Systemic Cyber Risk: A Primer* (Carnegie Endowment for International Peace, March 2022), https://carnegieendowment.org/research/2022/03/systemic-cyber-risk-a-primer.

[72] Studies based on Monte Carlo simulations result in more flexible models, as variables can be described using probability distributions. This approach provides a better understanding of the behavior of specific outputs and enhances the ability to identify the model's most representative variables.

[73] Victor Galaz et al., "Artificial Intelligence, Systemic Risks, and Sustainability," *Technology in Society* 67 (November 2021): 101741, https://doi.org/10.1016/j.techsoc.2021.101741.

[74] Stefano Boccaletti, Vito C. Latora, Yamir Moreno, Mario Chavez, and Dong-uk Hwang, "Complex Networks: Structure and Dynamics," *Physics Reports* 424, no. 4-5 (2006): 175-308, https://doi.org/10.1016/j.physrep.2005.10.009.

[75] Esmat Zaidan and Imad Antoine Ibrahim, "AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective," *Humanities and Social Sciences Communications* 11 (2024), 1121, https://doi.org/10.1057/s41599-024-03560-x.

accountability and control issues that complicate traditional risk management frameworks. Therefore, a comprehensive risk-focused approach should include systemic analyses that consider the interdependencies between technological, ethical, and societal risks. Such an approach would enable decision-makers to anticipate and manage the effects of threats, ensuring that responses are both timely and effective in a dynamically shifting environment.

As emerging technologies become increasingly complex, effective risk management requires advanced modeling and interdisciplinary collaboration to understand their societal impacts. Incorporating network analysis into modern risk assessment is essential for addressing the growing complexity of interconnected systems, improving the accuracy of predictions, and facilitating proactive management of systemic risks.[76] Integrating these methods allows analysts to understand better the intricate risks associated with the combinatorial impacts of emerging technologies. The next section will review how the Emerging Security Challenges Working Group (ESCWG) of the Partnership for Peace Consortium (PfPC) has addressed the risks stemming from the weaponization of emerging technologies.

How Does the PfPC Emerging Security Challenges Working Group Address These Issues?

Over the last five years, the PfPC Emerging Security Challenges Working Group has extensively discussed emerging risks, focusing on critical areas such as artificial intelligence, swarming technologies, cybersecurity, hybrid threats,[77] cognitive warfare, neurotechnology, generative AI (GenAI), synthetic biology,[78] and global power shifts.

Cyber Warfare and NATO's Response

One of the most significant challenges NATO faces is cyber warfare. Cyberattacks have become increasingly sophisticated, disrupting critical infrastructures, military systems, and democratic institutions. According to a NATO report, these threats are evolving rapidly, with adversaries using advanced techniques to undermine national security and stability across member states.[79] The evolution of

[76] Billio, Getmansky, Lo, and Pelizzon, "Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors"; Prasanna Gai and Sujit Kapadia, "Contagion in Financial Networks," *Proceedings of the Royal Society A* 466 (2010): 2401-2423, https://doi.org/10.1098/rspa.2009.0410.

[77] Sean S. Costigan and Michael A. Hennessy, eds., *Hybrid Threats and Hybrid Warfare Reference Curriculum* (NATO and PfP Consortium, 2024), https://www.pfp-consortium.org/media/570/download.

[78] "Synthetic Biology and AI: Emerging Challenges in International Security," *PfP Consortium News*, August 2024, https://www.pfp-consortium.org/news/synthetic-biology-and-ai-emerging-challenges-international-security.

[79] "Cyber Defence," *What We Do*, last updated July 30, 2024, https://www.nato.int/cps/da/natohq/topics_78170.htm.

cyber capabilities not only intensifies threats but also reshapes global power dynamics, making it imperative for NATO to enhance its cyber resilience. The competition for technological dominance has become a defining feature of international relations, as emerging technologies can empower both state and non-state actors.[80]

In a recent workshop hosted by the ESCWG, experts highlighted how adversaries have weaponized technologies such as swarming and AI, creating new tools to exploit vulnerabilities in NATO's cyber defenses. NATO has responded by enhancing its cyber resilience, focusing on improving detection, defense, and recovery capabilities following cyber incidents.[81]

Initiatives such as the Cyber Coalition exercises exemplify NATO's efforts to strengthen member states' cybersecurity capabilities through collective training.[82] The Cyber Coalition is a key multinational exercise that tests and improves the ability of NATO and partner nations to respond to cyber threats.[83]

NATO recognizes the need for an integrated response as hybrid warfare—which incorporates conventional, cyber, and asymmetric tactics—becomes more widespread. Russia's actions in Ukraine and its ongoing cyber campaigns against NATO members highlight the urgency for NATO to address threats that transcend traditional military domains.[84] To that end, the PfPC, under the leadership of the ESCWG, has just published a reference curriculum on hybrid threats and hybrid warfare to provide core references for teaching these topics.[85]

Swarming Technologies and AI in Warfare

The use of AI and autonomous systems presents both opportunities and challenges for NATO. Swarming technology, which enables unmanned drones and other AI-powered devices to act in concert, represents a significant shift in the balance of offensive and defensive strategies. This technology can overwhelm traditional defense systems by coordinating multiple attacks simultaneously,[86] thereby reducing the effectiveness of conventional defenses.

[80] Kai A. Konrad, "Dominance and Technology War," *European Journal of Political Economy* 81 (2024), 102493, https://doi.org/10.1016/j.ejpoleco.2023.102493; Samson et al., *Scenarios of Evolving Global Order*, 22.

[81] "NATO Exercises to Enhance Its Cyber Resilience," NATO Allied Command Transformation, November 20, 2024, https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/.

[82] "Cyber Coalition: NATO's Flagship Cyber Exercise," NATO Allied Command Transformation, accessed December 13, 2024, https://www.act.nato.int/activities/cyber-coalition/.

[83] "Cyber Coalition: NATO's Flagship Cyber Exercise."

[84] Herzog and Kunertova, "NATO and Emerging – Alliance's Shifting Approach to Military Innovation," 51.

[85] Costigan and Hennessy, eds., *Hybrid Threats and Hybrid Warfare Reference Curriculum.*

[86] Jean-Marc Rickli, "The Impact of Autonomous Weapons Systems on International Security and Strategic Stability," Geneva Centre for Security Policy, January 15, 2018.

For example, the growing use of increasingly autonomous drones *en masse* in Ukraine and the Middle East, though not yet representing true swarms,[87] has demonstrated their capability to outmaneuver traditional defense systems, illustrating a new paradigm in warfare.[88] Drone swarms, or multi-UAV systems, consist of multiple UAVs collaborating in hierarchical groups to overcome the limitations of single UAVs. These systems exemplify multiagent systems, enabling them to undertake missions that individual drones cannot. Additionally, drone swarms can perform numerous distributed tasks simultaneously.[89] To address these challenges, NATO must invest in counter-swarming technologies and AI-driven defensive systems capable of operating independently against these threats.

Recent ESCWG workshops have emphasized the importance of integrating AI into military doctrine. However, the proliferation of these technologies means that adversaries, including non-state actors, can also utilize them at relatively low cost. The use of lethal autonomous weapons (LAWs), while offering significant military advantages, also poses risks of unpredictable failures and ethical and moral dilemmas.[90]

Cognitive Warfare and Generative AI

In the field of cognitive warfare, the ESCWG's workshop emphasized that GenAI poses significant risks as it can produce highly realistic synthetic content, including deepfakes and fabricated synthetic media. These capabilities amplify misinformation campaigns, enabling adversaries to undermine trust in institutions and manipulate public opinion during conflicts. A RAND Corporation report corroborates this, highlighting the detrimental impact of deepfakes on societal trust and information integrity, demonstrating how easily GenAI can distort reality and influence perceptions.[91]

Moreover, the accessibility of GenAI tools increases the likelihood that state and non-state actors and even single individuals will exploit these technologies

[87] Wilfried Yves Hamilton Adoni et al., "Intelligent Swarm: Concept, Design and Validation of Self-Organized UAVs Based on Leader–Followers Paradigm for Autonomous Mission Planning," *Drones* 8, no. 10 (2024): 575, https://doi.org/10.3390/drones8100575.

[88] Jun Tang, Haibin Duan, and Songyang Lao, "Swarm Intelligence Algorithms for Multiple Unmanned Aerial Vehicles Collaboration: A Comprehensive Review," *Artificial Intelligence Review* 56 (2023): 4295-4327, https://doi.org/10.1007/s10462-022-10281-7.

[89] Tang, Duan, and Lao, "Swarm Intelligence Algorithms for Multiple Unmanned Aerial Vehicles Collaboration."

[90] Ioana Puscas and Alisha Anand, "Proposals Related to Emerging Technologies in the Area of Lethal Autonomous Weapons Systems: A Resource Paper (updated)," *UNIDIR* (Geneva: United Nations Institute for Disarmament Research, May 2023), https://unidir.org/publication/proposals-related-to-emerging-technologies-in-the-area-of-lethal-autonomous-weapons-systems-a-resource-paper-updated/.

[91] Todd C. Helmus, "Artificial Intelligence, Deepfakes, and Disinformation: A Primer," *Perspective*, RAND Corporation, July 6, 2022, https://www.rand.org/pubs/perspectives/PEA1043-1.html.

for their own agendas, such as extorting money, spreading disinformation, or influencing democratic processes like elections.[92] Recognizing these intertwined threats, NATO is fostering collaborations with academic institutions and member states to develop frameworks that address cognitive threats, including disinformation amplified by generative AI. As these technologies evolve, NATO must adapt its strategies to counter cognitive warfare and the proliferation of AI-generated disinformation, thereby ensuring resilience against these multifaceted challenges.

Great Powers Competition

Although emerging technologies represent new risks, the international environment in which these technologies evolve also matters for any global risk analysis. The geopolitical landscape is undergoing significant changes, with power disparities not only among nations but also among non-state actors, including terrorist groups and private entities. The ongoing competition for technological superiority, particularly between the United States and China, underscores the strategic challenges NATO faces that go beyond its immediate borders. As the report by Samson and coworkers highlights, the interplay between technological advancement and power dynamics complicates NATO's role in maintaining stability and security in a multipolar world.[93]

China's rise as a global power, its Belt and Road Initiative, and its assertiveness in regions like the South China Sea, coupled with its projections of military capabilities beyond its immediate neighborhood, present new strategic challenges for NATO. As the United States prioritizes great power competition, NATO must reaffirm its strategies to remain relevant in a multipolar world. China's growing influence in Europe, particularly through investments in critical infrastructure such as ports, raises concerns about security dependencies that could be exploited during crises. The "weaponization of interdependencies" [94]—defined as a "condition under which an actor can exploit its position in an embedded network to gain a bargaining advantage over others in a contained system"—becomes an avenue of choice to undermine its adversary. The weaponization of interdependencies in our globalized networks can be used to discover and exploit vulnerabilities, compel policy change, or deter unwanted actions.[95]

Great power competition with Russia and China is driving NATO to innovate and integrate these technologies into its strategic framework. However, global

[92] Brundage et al., "The Malicious Use of Artificial Intelligence," 19.

[93] Samson et al., *Scenarios of Evolving Global Order* (2024), 22.

[94] Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021).

[95] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.

and decentralized supply chains and manufacturing systems [96] make these technologies vulnerable to exploitation through weaponized interdependencies.[97] In addition, maintaining technological superiority and interoperability among member states is crucial to effectively addressing these new threats. Herzog and Kunertova [98] argue that while NATO has the potential to lead in the military application of emerging technologies, achieving this will require significant transformations in bureaucratic practices and greater involvement from European allies in technological burden-sharing.

Conclusion and Recommendations

The third decade of the 21st century is marked by traditional great power competition and the weaponization of emerging technologies. Traditional power politics and associated risks characterize the international security environment. The increasing interconnection between geopolitics and technology has intensified competition, with China and the United States competing for control over the rules and institutions that will shape future international relations.[99]

The rapid development, diffusion, and democratization of emerging technologies such as artificial intelligence, synthetic biology, and cyber capabilities induce new types of risks that are much more difficult to comprehend and mitigate. Global risks are interconnected, making modern security challenges more complex. The concepts of global catastrophic risk and existential risk have been increasingly applied to issues such as climate change, biotechnology, and nuclear war – issues that require global rather than national solutions.

Security policies must, therefore, transition from a threat-based to a risk-based perspective to identify the weak spots. The effective mitigation of emerging risks will depend on global cooperation, public-private partnerships, and innovative governance frameworks, with NATO taking a leading role in promoting the effective use of disruptive technologies. The shift from a traditional threat-based approach to a risk-based framework is crucial for NATO, especially as NATO's 2030 Agenda acknowledges these challenges, though more effort is needed.

[96] Nadia Hewett and Andrew Ballinger, "3 Ways to Use Digital Identity Systems in Global Supply Chains," World Economic Forum, May 14, 2019, www.weforum.org/stories/2019/05/3-options-to-transform-global-supply-chains/.

[97] Farrell and Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion."

[98] Herzog and Kunertova, "NATO and Emerging – Alliance's Shifting Approach to Military Innovation."

[99] Xiangning Wu, "Technology, Power, and Uncontrolled Great Power Strategic Competition between China and the United States," *China International Strategy Review* 2 (2020): 99-119, https://doi.org/10.1007/s42533-020-00040-0.

Disclaimer

The views expressed in this article are those of the authors and do not necessarily reflect the official policies of the Partnership for Peace Consortium or its governance stakeholders.

About the Authors

Dr. **Jean-Marc Rickli** is the Head of Global and Emerging Risks and Director of the Polymath Initiative at the Geneva Centre for Security Policy in Geneva. He is also co-chair of the Partnership for Peace Consortium's (PfPC) Emerging Security Challenges Working Group and the co-curator of the International Security Map of the Strategic Intelligence Platform of the World Economic Forum.
E-mail: j.rickli@gcsp.ch
https://orcid.org/0000-0003-4459-1802

Dr. **Gëzim Vllasi** is a Senior Program Advisor in the Mediation and Peace Support Department at the Geneva Centre for Security Policy (GCSP) in Geneva, Switzerland. Previously, Dr. Vllasi was a Doctoral Researcher at the University of Graz, Austria, and a Doctoral Fellow at GCSP.
E-mail: G.Vllasi@gcsp.ch; https://orcid.org/0009-0000-2151-6151

Bibliography

“Cyber Coalition: NATO’s Flagship Cyber Exercise,” NATO Allied Command Transformation, accessed December 13, 2024, https://www.act.nato.int/activities/cyber-coalition/.

“Cyber Defence,” What We Do, last updated July 30, 2024, https://www.nato.int/cps/da/natohq/topics_78170.htm.

“NATO Exercises to Enhance Its Cyber Resilience,” NATO Allied Command Transformation, November 20, 2024, https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/.

“P5 Experts Roundtable Online Meeting: AI-Nuclear Nexus, 24 June 2024,” GCSP News, www.gcsp.ch/global-insights/p5-experts-roundtable-online-meeting-ai-nuclear-nexus-24-june-2024.

“Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy,” U.S. Department of State, November 9, 2023, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/.

“Stanford Existential Risks Conference,” https://cisac.fsi.stanford.edu/events/stanford-existential-risks-conference-0.

“Synthetic Biology and AI: Emerging Challenges in International Security,” PfP Consortium News, August 2024, https://www.pfp-consortium.org/news/synthetic-biology-and-ai-emerging-challenges-international-security.

“Weapons Powered by Artificial Intelligence Pose a Frontier Risk and Need to Be Regulated,” World Economic Forum, June 23, 2021, https://www.weforum.org/stories/2021/06/the-accelerating-development-of-weapons-powered-by-artificial-risk-is-a-risk-to-humanity/.

Adamala, Katarzyna, et al., “Confronting Risks of Mirror Life,” *Science*, December 12, 2024, https://doi.org/10.1126/science.ads9158.

Adoni, Wilfried Yves Hamilton, et al., “Intelligent Swarm: Concept, Design and Validation of Self-Organized UAVs Based on Leader–Followers Paradigm for Autonomous Mission Planning,” *Drones* 8, no. 10 (2024): 575, https://doi.org/10.3390/drones8100575.

Alizon, Samuel, A.K. Hurford, N. Mideo, and M. van Baalen, “Virulence Evolution and the Trade-Off Hypothesis: History, Current State of Affairs and the Future,” *Journal of Evolutionary Biology* 22, no. 2 (2009): 245-259, https://doi.org/10.1111/j.1420-9101.2008.01658.x.

Aven, Terje, “The Risk Concept – Historical and Recent Development Trends,” *Reliability Engineering & System Safety* 99 (2012): 33–44, https://doi.org/10.1016/j.ress.2011.11.006.

Avin, Shahar, Bonnie C. Wintle, Julius Weitzdörfer, Seán S. Ó hÉigeartaigh, William J. Sutherland, and Martin J. Rees, "Classifying Global Catastrophic Risks," *Futures* 102 (2018): 20-26, https://doi.org/10.1016/j.futures.2018.02.001.

Beck, Ulrich, *Risk Society: Towards a New Modernity* (London: SAGE, 1992).

Billio, Monica, Mila Getmansky, Andrew W. Lo, and Loriana Pelizzon, "Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors," *Journal of Financial Economics* 104, no. 3 (2012): 535–559, https://doi.org/10.1016/j.jfineco.2011.12.010.

Boccaletti, Stefano, Vito C. Latora, Yamir Moreno, Mario Chavez, and Dong-uk Hwang, "Complex Networks: Structure and Dynamics," *Physics Reports* 424, no. 4–5 (2006): 175–308, https://doi.org/10.1016/j.physrep.2005.10.009.

Borch, Christian, "High-Frequency Trading, Algorithmic Finance and the Flash Crash: Reflections on Eventalization," *Economy and Society* 45, no. 3–4 (2016): 350-378, https://doi.org/10.1080/03085147.2016.1263034.

Bostrom, Nick, and Vlatko Vedral Cirkovic, eds., *Global Catastrophic Risks* (Oxford: Oxford University Press, 2008).

Brożek, Bartosz, Michał Furman, Marek Jakubiec, and Bartłomiej Kucharzyk, "The Black Box Problem Revisited. Real and Imaginary Challenges for Automated Legal Decision Making," *Artificial Intelligence and Law* 32 (2024): 427-440, https://doi.org/10.1007/s10506-023-09356-9.

Brundage, Vincent, et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv preprint arXiv:1802.07228, 2018, last revised December 1, 2024, https://doi.org/10.48550/arXiv.1802.07228.

Carmichael, Mary, "Eight Overlooked Emerging Tech Risks and How to Mitigate Them," *@ISACA* 9, May 6, 2024, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-9/eight-overlooked-emerging-tech-risks-and-how-to-mitigate-them.

Carter, Sarah R., Nicole E. Wheeler, Sabrina Chwalek, Christopher R. Isaac, and Jaime Yassif, "The Convergence of Artificial Intelligence and the Life Sciences," Nuclear Threat Initiative, October 30, 2021, https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/.

Chai, Xiaoke et al., "Brain-Computer Interface Digital Prescription for Neurological Disorders," *CNS Neuroscience & Therapeutics* 30, no. 2 (2024): e14615, https://doi.org/10.1111/cns.14615.

Chavarriaga, Ricardo, Jean-Marc Rickli, and Federico Mantellassi, "Neurotechnologies: The New Frontier for International Governance," *Strategic Security Analysis* 29, Geneva Centre for Security Policy, April 2023, https://dam.gcsp.ch/files/doc/ssa-2023-issue29.

Costigan, Sean S., and Michael A. Hennessy, eds., *Hybrid Threats and Hybrid Warfare Reference Curriculum* (NATO and PfP Consortium, 2024), https://www.pfp-consortium.org/media/570/download.

Cotton-Barratt, Owen, et al., *Global Catastrophic Risk Annual Report 2016* (Global Challenges Foundation and Global Priorities Project, 2016), https://globalprioritiesproject.org/wp-content/uploads/2016/04/Global-Catastrophic-Risk-Annual-Report-2016-FINAL.pdf.

Cronin, Audrey Kurth, P*ower to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford, Oxford University Press, 2020).

Cubillos, Pablo Gutiérrez, and Roberto Pastén, "Nonlinear Risks: A Unified Framework," *Theory and Decision* 95 (2023): 11–32, https://doi.org/10.1007/s11238-022-09912-w.

Currie, Adrian, and Seán Ó hÉigeartaigh, "Working Together to Face Humanity's Greatest Threats: Introduction to the Future of Research on Catastrophic and Existential Risk," Futures 102 (2018): 1-5, https://doi.org/10.1016/j.futures.2018.07.003.

Douek, Evelyn, "The Government's Disturbing Rationale for Banning TikTok," *The Atlantic*, December 12, 2024, https://www.theatlantic.com/ideas/archive/2024/12/social-media-national-security-ban/680963/.

Drezner, Daniel W., Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021).

Duchek, Stephanie, "Organizational Resilience: A Capability-Based Conceptualization," *Business Research* 13 (2020): 215246, https://doi.org/10.1007/s40685-019-0085-7.

Echevarria, Antulio J., "Clausewitz's Center of Gravity: It's Not What We Thought," *Naval War College Review* 56, no. 1 (2003): 108-123, https://digital-commons.usnwc.edu/nwc-review/vol56/iss1/6.

Esvelt, Kevin M., "Delay, Detect, Defend: Preparing for a Future in which Thousands Can Release New Pandemics," Geneva Papers 29/22, Geneva Centre for Security Policy, November 14, 2022, https://www.gcsp.ch/publications/delay-detect-defend-preparing-future-which-thousands-can-release-new-pandemics.

Evrin, Volkan, "Risk Assessment and Analysis Methods: Qualitative and Quantitative," *ISACA Journal* 2 (April 2021), https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods.

Farrell, Henry, and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.

Forscey, David, Jon Bateman, Nick Beecroft, and Beau Woods, *Systemic Cyber Risk: A Primer* (Carnegie Endowment for International Peace, March 2022), https://carnegieendowment.org/research/2022/03/systemic-cyber-risk-a-primer.

Gai, Prasanna, and Sujit Kapadia, "Contagion in Financial Networks," *Proceedings of the Royal Society A* 466 (2010): 2401-2423, https://doi.org/10.1098/rspa.2009.0410.

Galaz, Victor, et al., "Artificial Intelligence, Systemic Risks, and Sustainability," *Technology in Society* 67 (November 2021): 101741, https://doi.org/10.1016/j.techsoc.2021.101741.

Galeotti, Mark, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2023).

Gomes, João Eduardo Costa, et al., "Surveying Emerging Network Approaches for Military Command and Control Systems," *ACM Computing Surveys* 56, no. 6 (2024): 1-38, https://doi.org/10.1145/3626090.

Group of Governmental Experts on Lethal Autonomous Weapons Systems, Final Report (United Nations, 2019).

Grumbling, Emily, and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019), 12, https://doi.org/10.17226/25196.

Hassija, Vikas, et al., "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence," *Cognitive Computation* 16, no. 1 (2024): 46, https://doi.org/10.1007/s12559-023-10179-8.

Hassija, Vikas, et al., "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence," *Cognitive Computation* 16, no. 1 (2024): 45-74, https://doi.org/10.1007/s12559-023-10179-8.

Helmus, Todd C., "Artificial Intelligence, Deepfakes, and Disinformation: A Primer," *Perspective*, RAND Corporation, July 6, 2022, https://www.rand.org/pubs/perspectives/PEA1043-1.html.

Herzog, Stephen, and Dominika Kunertova, "NATO and Emerging Technologies – Alliance's Shifting Approach to Military Innovation," *Naval War College Review* 77, no. 2 (2024): 47-69, https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/5/.

Hewett, Nadia, and Andrew Ballinger, "3 Ways to Use Digital Identity Systems in Global Supply Chains," World Economic Forum, May 14, 2019, https://www.weforum.org/stories/2019/05/3-options-to-transform-global-supply-chains/.

Hung, Tzu-Chieh, and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," *Journal of Global Security Studies* 7, no. 4 (December 2022): ogac016, https://doi.org/10.1093/jogss/ogac016.

Irving, Doug, "Artificial Intelligence and Biotechnology: Risks and Opportunities," RAND, March 21, 2024, https://www.rand.org/pubs/articles/2024/artificial-intelligence-and-biotechnology-risks-and.html.

Jung, Wookyung, and Sean Doyle, "Police Agencies Must Partner Up to Prevent a Ransomware Crisis – Here's How," World Economic Forum, November 12, 2021. https://www.weforum.org/stories/2021/11/police-agencies-must-partner-up-to-prevent-a-ransomware-crisis-heres-how/.

Kerner, Sean Michael, "Crowdstrike Outage Explained: What Caused it and What's Next," *Techtarget*, October 29, 2024, https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

Konrad, Kai A., "Dominance and Technology War," *European Journal of Political Economy* 81 (2024), 102493, https://doi.org/10.1016/j.ejpoleco.2023.102493.

Korhonen, Veera, "Total Budgetary Cost to the United States of the Global War on Terror between FY 2001 and FY 2020, by Category," *Statista*, August 9, 2024, https://www.statista.com/statistics/1075849/total-us-war-costs-war-terror-category/.

Kosal, Margaret E., ed., *Proliferation of Weapons- and Dual-Use Technologies* (Cham: Springer, 2021).

Linkov, Igor, et al., "Applying Resilience to Hybrid Threats," *IEEE Security and Privacy* 17, no. 5 (2019): 78-83, https://doi.org/10.1109/MSEC.2019.2922866.

Masakowski, Yvonne R., and Janet M. Blatny, "Mitigating and Responding to Cognitive Warfare," *STO Technical Report* TR-HFM-ET-356 (Paris: NATO Science and Technology Organization, 2023).

Maslej, Nestor, et al., AI Index Report 2024 (Stanford, CA: Institute for Human-Centered AI, Stanford University, April 2024), https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf.

McCabe, David, "TikTok Faces U.S. Ban After Losing Bid to Overturn New Law," *The New York Times*, December 6, 2024, https://www.nytimes.com/2024/12/06/business/media/tiktok-ban-court-decision.html.

Millett, Piers, and Andrew Snyder-Beattie, "Existential Risk and Cost-Effective Biosecurity," *Health Security* 15, no. 4 (2017): 373-383. https://doi.org/10.1089/hs.2017.0028.

Morelle, Marie, Cegarra Julien, Damien Marion, and André Jean-Marc, "Towards a Definition of Cognitive Warfare," Conference on Artificial Intelligence for Defense, DGA Maîtrise de l'Information, November 2023, Rennes, France, https://hal.archives-ouvertes.fr/hal-04328461.

Nahas, Kamal, "AI Re-Creates What People See by Reading Their Brain Scans," *Science*, March 7, 2023, https://www.science.org/content/article/ai-re-creates-what-people-see-reading-their-brain-scans.

Naheed, Sanober, "Understanding Disaster Risk Reduction and Resilience: A Conceptual Framework," in *Handbook of Disaster Risk Reduction for Resilience*, ed. Saeid Eslamian and Faezeh Eslamian (Cham: Springer, 2021), 1-25, https://doi.org/10.1007/978-3-030-61278-8_1.

Namdar, Benedikt, and Thomas Pölzler, "Toby Ord, The Precipice: Existential Risk and the Future of Humanity, Bloomsbury, 2020," *Ethical Theory and Moral Practice* 24 (2021): 855-857, https://doi.org/10.1007/s10677-021-10181-9.

Nelson, Cassidy, "Engineered Pathogens: The Opportunities, Risks and Challenges," *Biochemist* 41, no. 3 (2019): 34–39, https://doi.org/10.1042/BIO04103034.

Osman, Rehab, and Sherif El-Gendy, "Interconnected and Resilient: A CGE Analysis of AI-Driven Cyberattacks in Global Trade," *Risk Analysis* (2024), https://doi.org/10.1111/risa.14321.

Petrosyan, Ani, "Estimated Cost of Cyber Crime Worldwide 2018-2029," *Statista*, July 30, 2024, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

Prakash, K. LNC, Santosh Kumar Ravva, M.V. Rathnamma, and G. Suryanarayana, "AI Applications of Drones," in *Drone Technology: Future Trends and Practical Applications*, ed. Sachi Nandan Mohanty et al. (Scrivener Publishing, 2023), https://doi.org/10.1002/9781394168002.ch7.

Puscas, Ioana, and Alisha Anand, "Proposals Related to Emerging Technologies in the Area of Lethal Autonomous Weapons Systems: A Resource Paper (updated)," UNIDIR (Geneva: United Nations Institute for Disarmament Research, May 2023), https://unidir.org/publication/proposals-related-to-emerging-technologies-in-the-area-of-lethal-autonomous-weapons-systems-a-resource-paper-updated/.

Ranasighe, Roshanka, et al., "Climate Change Information for Regional Impact and for Risk Assessment," in *Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*, ed. Valerie Masson-Delmotte, Panmao Zhai, Anna Pirani et al. (Cambridge University Press, 2021), 1767-1926, https://doi.org/10.1017/9781009157896.

Rickli, Jean-Marc, "The Impact of Autonomous Weapons Systems on International Security and Strategic Stability," Geneva Centre for Security Policy, January 15, 2018.

Rickli, Jean-Marc, "The Strategic Implications of Artificial Intelligence," in *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, ed. Al Naqvi and J. Mark Munoz (London: Anthem Press, 2020), 41-54.

Rickli, Jean-Marc, and Christina Liang, "New and Emerging Technologies for Terrorists," in *The Routledge Companion to Terrorism Studies*, ed. Max Abrahms (London: Routledge, 2024), Chapter 15.

Riebe, Thea, *Technology Assessment of Dual-Use ICTs – How to Assess Diffusion, Governance and Design* (Springer Nature, 2023).

Rojas, Clarissa Rios, et al., *Building the Science-Policy Interface for Tackling Global Governance of Catastrophic and Existential Risks* (University of Cambridge, 2023), https://www.cser.ac.uk/resources/report-building-science-policy-interface-tackling-global-governance-catastrophic-and-existential-risks/.

Saltini, Alice, “AI and Nuclear Command, Control and Communications: P5 Perspectives,” European Leadership Network, November 13, 2023, https://europeanleadershipnetwork.org/report/ai-and-nuclear-command-control-and-communications-p5-perspectives/.

Samson, Paul, S. Yash Kalash, Nikolina Zivkovic, Tracey Forrest, and Bessma Momani, *Scenarios of Evolving Global Order* (Waterloo, ON, Canada: Center for International Governance Innovation, 2024), https://www.cigionline.org/static/documents/Scenarios_of_Evolving_Global_Order.pdf.

Schwartz, Peter, and Doug Randall, *An Abrupt Climate Change Scenario and Its Implications for United States National Security* (Minneapolis, MN: Institute for Agriculture and Trade Policy, October 2003), https://www.iatp.org/documents/abrupt-climate-change-scenario-and-its-implications-united-states-national-security.

Strachan-Morris, David, “Threat and Risk: What Is the Difference and Why Does It Matter?” *Intelligence and National Security* 27, no. 2 (2012): 172-186, https://doi.org/10.1080/02684527.2012.661641.

Strategic Foresight Group, “P5 Experts’ Roundtable on Nuclear Risk Reduction: Co-Convenors’ Summary,” Geneva, December 11-13, 2023, https://www.strategicforesight.com/conference_pdf/Geneva%20Roundtable%20Report.pdf.

Strategic Foresight Group, “Roundtable on AI-NC3 Interface,” December 6, 2024, https://www.strategicforesight.com/news_inner.php?id=228.

Tang, Jun, Haibin Duan, and Songyang Lao, “Swarm Intelligence Algorithms for Multiple Unmanned Aerial Vehicles Collaboration: A Comprehensive Review,” *Artificial Intelligence Review* 56 (2023): 4295-4327, https://doi.org/10.1007/s10462-022-10281-7.

Tucker, Jonathan B., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (MIT Press, 2012).

Turchin, Alexey, and Daniel Denkenberger, “Global Catastrophic and Existential Risks Communication Scale,” *Futures* 102 (2018): 27–38, https://doi.org/10.1016/j.futures.2018.01.003.

United Nations, *Global Governance: A New Approach to Address Global Challenges* (New York: United Nations, 2013).

Vogel, Isabel, *Review of the Use of ‘Theory of Change’ in International Development* (London: UK Department for International Development, 2012).

von Clausewitz, Carl, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton University Press, 1976,).

Wickiser, J. Kenneth, et al., “Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology,” *CTC Sentinel* 13, no. 8 (2020): 1-7, https://ctc.westpoint.edu/engineered-pathogens-and-unnatural-biological-weapons-the-future-threat-of-synthetic-biology/.

Willis, Henry H., Anu Narayanan et al., *Global Catastrophic Risk Assessment*, Research Report RRA2981, October 30, 2024, https://www.rand.org/pubs/research_reports/RRA2981-1.html.

Wu, Xiangning, "Technology, Power, and Uncontrolled Great Power Strategic Competition between China and the United States," *China International Strategy Review* 2 (2020): 99-119, https://doi.org/10.1007/s42533-020-00040-0.

Zaidan, Esmat, and Imad Antoine Ibrahim, "AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective," *Humanities and Social Sciences Communications* 11 (2024), 1121, https://doi.org/10.1057/s41599-024-03560-x.