Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Жан-Марк Рикли, Гёзим Влласи
Connections QJ 24, № 1 (2025): 97-120
https://doi.org/10.11610/Connections.rus.24.1.07

Рецензированная статья

Применение новых технологий как оружия и их влияние на глобальные риски: Взгляд рабочей группы Консорциума ПРМ по новым вызовам безопасности

Жан-Марк Рикли, Гёзим Влласи

Женевский центр политики безопасности, Швейцария, https://gcsp.ch

Аннотация: В статье рассматривается переход международной безопасности от традиционных моделей, ориентированных на угрозы, к подходам, основанным на рисках, с упором на роль новых технологий в формировании восприятия и реагирования. Предлагая значительные преимущества, новые технологии, включая искусственный интеллект, биотехнологии и квантовые вычисления, создали и новые уязвимости, особенно при их применении в качестве оружия. Традиционные государственные структуры безопасности недостаточны для устранения этих рисков, особенно если доступ к этим мощным технологиям получают негосударственные субъекты. В статье глобальные риски подразделяются на катастрофические и экзистенциальные и рассмотрено, как противодействие им требует изменения методов анализа рисков и упреждающих стратегий. Предлагается многосторонний подход и глобальное сотрудничество для повышения устойчивости, с особым акцентом на адаптивные стратегии НАТО по борьбе с кибернетическими, когнитивными и гибридными угрозами.

Ключевые слова: глобальные риски, новые технологии, управление рисками, катастрофический риск, экзистенциальный риск, использование в качестве оружия, искусственный интеллект, синтетическая биология, нейротехнологии, когнитивная война, квантовые вычисления.

Вступление

В современных условиях безопасности обсуждение политики безопасности сместилось от традиционной модели противодействия угрозам к подходу «управления рисками». Эта эволюция отражает растущую сложность международных отношений и постоянно меняющуюся картину мировой безопасности, делая этот сдвиг критически важным для ориентации в текущих и будущих вызовах международной безопасности. С учётом новых технологий, таких, как искусственный интеллект (ИИ) и биотехнологии, новые подходы имеют важное значение для упреждающего противодействия глобальным рискам.

Традиционно угрозы определялись с помощью подхода на основе оценки способностей и намерений потенциальных игроков [1] (очень часто относящихся к государству) причинить вред, но этот подход часто упускал из виду сложности, привносимые негосударственными субъектами, и новые уязвимости, возникающие из-за новых технологий. Растущее число негосударственных субъектов, включая террористические, преступные организации и международные корпорации, наряду с потенциальными угрозами безопасности, создаваемыми операторами современных технологий, меняют развитие и подход к управлению рисками. Поскольку международная система становится всё более непредсказуемой и взаимозависимой, число субъектов, способных причинить вред, существенно возросло, увеличивая уязвимость любой организации.

Учитывая меняющуюся природу международной системы, необходим подход к безопасности на основе оценки рисков, поскольку традиционные модели с трудом адаптируются к сложностям и взаимосвязи новых рисков. Этот сдвиг требует новой структуры управления рисками, учитывающей динамичный и часто непредсказуемый характер появляющихся рисков. Традиционные методы разработки политики безопасности, в значительной степени полагающиеся на предопределённые результаты, всё менее адекватны в условиях многогранных и быстро меняющихся рисков. Подход, основанный на оценке риска, напротив, делает упор на способности адаптироваться, предвидеть потенциальные последствия и учитывать взаимозависимость различных глобальных рисков. Поскольку стратегическое мировосприятие расширяется и включает не только военные риски, но и социальные, экономические и технологические угрозы, политики должны переключиться с традиционных моделей обороны на структуры, обеспечивающие гибкость и упреждающее противодействие разнообразным взаимосвязанным рискам. Серьёзность риска определяется его масштабом (сколько людей и других важных для человечества существ он затрагивает), интенсивностью (насколько сильно они будут затронуты) и вероятностью (насколько

[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.

вероятна катастрофа).[2] Эти факторы особенно важны в контексте новых технологий, которые в этой статье рассмотрены в связи с международной безопасностью и управлением рисками. Изучив изменение определения рисков и подходов к их разрешению с новыми вызовами безопасности, она даёт основу для понимания рисков в сегодняшних условиях, когда новые технологии всё чаще используют в качестве оружия.

По мере усложнения проблем безопасности управление рисками эволюционировало от простого выявления угроз до активного их устранения. Этот сдвиг во взглядах учитывает, что угрозы взаимосвязаны и требуют комплексного подхода для их эффективного смягчения. Нынешние риски требуют целостной структуры оценки их воздействия и вероятности, учитывая ограниченность традиционных моделей, охватывающих исключительно возможности и намерения.

В этих меняющихся условиях новые технологии, включая искусственный интеллект, биотехнологии и киберспособности, трансформируют природу и воздействие рисков, требуя тщательной оценки и упреждающих стратегий противодействия рискам. В статье рассмотрена революционная роль этих технологий в формировании нынешних рисков безопасности и изучены их последствия для международной безопасности и основ политики. В ней подчёркивается необходимость гибких ответов во взаимосвязанном мире.

В статье представлен всесторонний обзор влияния новых технологий на проблемы безопасности, структурированный следующим образом. Во-первых, определяются различные риски, связанные с этими технологиями, с разбивкой на глобальные, катастрофические и экзистенциальные. На основе этого определения рассмотрены новые виды рисков, вытекающие из новых технологий, таких, как искусственный интеллект, квантовые вычисления и синтетическая биология. В следующем разделе рассмотрено, как эти технологии могут использоваться в качестве оружия. Далее следует оценка возможной адаптации анализа рисков с учётом этих новых видов рисков. Затем в статье освещается вклад рабочей группы по новым вызовам безопасности Консорциума «Партнёрство ради мира» (ПРМ) в обсуждение таких ключевых тем, как искусственный интеллект, роевые технологии, кибербезопасность, гибридные угрозы, когнитивная война, нейротехнологии, генеративный ИИ, синтетическая биология и глобальные изменения соотношения сил. Статья завершается указанием на необходимость упреждающих стратегий снижения рисков, создаваемых новыми технологиями, для обеспечения и повышения глобальной безопасности.

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

Определение рисков: глобальные, катастрофические и экзистенциальные

Переход от подхода на основе угроз к подходу на основе рисков отражает более глубокое понимание современных сложностей безопасности. Бек называет их «искусственными рисками»,[3] созданными деятельностью человека, особенно техническим прогрессом. В отличие от естественных рисков, искусственные риски выходят за рамки национальных границ, что определяет их важность для современной политики управления рисками и безопасности.[4] По мнению Бека, сейчас мы наблюдаем этап преобразований, когда традиционные индустриальные общества развиваются под воздействием технологических и социальных изменений. Эта эволюция характеризуется тем, что он называет «рефлексивной модернизацией» [5] – общество всё больше осознает создаваемые им риски и их последствия, а не просто стремится к прогрессу, как на более ранних этапах.

Этот сдвиг связан с неопределённостью, присущей новым технологиям. Несмотря на растущую роль предвидения при анализе безопасности, неопределённость, присущая потенциалу и развитию новых технологий, потенциально влечёт беспрецедентные новые риски.[6] Например, растущая автономия оружия на базе ИИ и кибервойны создают риски, которые очень трудно полностью предвидеть.[7] Кроме того, постоянно меняющийся характер этих рисков указывает на необходимость постоянной адаптации политики и стратегического планирования.

С усложнением этих рисков расширяется и научная литература по международной безопасности, рассматривающая новые виды рисков. Наличие рисков требует ясности в определении глобальных катастрофических рисков (global catastrophic risks, GCR) и экзистенциальных рисков (X-рисков) и их отличия от традиционных угроз безопасности. Глобальные катастрофические риски и экзистенциальные риски нужно рассматривать через призму сетевой уязвимости. Эти риски более не ограничиваются действиями государств, но обусловлены сложной взаимозависимостью между государствами, негосударственными субъектами и технологической инфраструкту-

---

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*.

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. См. также, 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.

рой. Например, управляемая ИИ кибератака может нарушить работу мировых финансовых систем [8] – этот риск не могут устранить одни лишь государственные органы.

При определении катастрофических и экзистенциальных рисков существует тенденция определять их через количественное воздействие. Миллетт и Снайдер-Беатти [9] считают катастрофическими риски, вызывающие гибель 100 миллионов человек, но такие пороговые значения произвольны. Если катастрофа приводит к гибели 99 миллионов человек, разве она уже не считается катастрофической или экзистенциальной? Тоби Орд критикует ограничение определения рисков исключительно количественной меркой – например, числом смертей. Он утверждает, что количественная мерка даёт чёткий порог, но часто не способна учесть более широкое воздействие на долгосрочные возможности человечества.[10]

Мы выступаем за более комплексный подход, учитывающий функциональное воздействие рисков, в частности, их *влияние* на основные функции, необходимые для выживания и надлежащего функционирования человечества. Не полагаясь исключительно на количественные показатели, риски следует определять по их влиянию на критические функции, которые организация или система должны выполнять, чтобы выжить и эффективно действовать.

---

[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. Напротив, при более функциональном подходе экзистенциальными считаются риски, критически угрожающие основным функциям, необходимым для выживания организации, общества или вида. Например, Конференция по экзистенциальным рискам Стэнфордского университета считает экзистенциальными риски, угрожающие навсегда нарушить базовые функции или инфраструктуру, необходимые для устойчивости общества, не фокусируясь исключительно на цифрах смертности. Сюда входят такие угрозы, как дестабилизация климата, неадекватность ИИ или искусственные патогены, способные серьёзно нарушить базовые функции общества, даже не вызывая напрямую некоего количества смертей. Такие риски требуют ориентированных на устойчивость структур, усиливающих потенциал жизненно важных функций для противостояния потрясениям и адаптации – эта концепция популярна в исследованиях устойчивости. См. “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.

У каждой организации или отдельного человека есть «центры тяжести» – функции, потеря которых приводит к краху или смерти.[11] Например, у людей четыре центра тяжести: они должны есть, пить, дышать и спать. Если какая-то из этих функций утрачена, выживание невозможно. Таким образом, экзистенциальные риски правильнее определить как риски, угрожающие самому существованию организации, группы или индивидуума. Экзистенциальные риски – это риски, которые нарушают *жизненно важные функции*, необходимые для выживания.

Катастрофические же риски можно определить как риски, нарушающие надлежащее выполнение *ключевых функций*, потеря которых ведёт к коллапсу. Анализируя жизненно важные и ключевые функции, мы можем провести более детальную оценку, поскольку у каждой организации есть свои функции, имеющие критическое значение для её выживания или надлежащего функционирования.

Этот подход также облегчает разработку стратегий противодействия таким рискам на основе понятия устойчивости,[12] которая определяется как способность организации переживать потрясения, продолжая функционировать. Поэтому, когда определены жизненно важные ключевые функции организации, стратегия устойчивости может сосредоточиться на защите этих функций.

Глобальные риски по своей природе транснациональны и охватывают угрозы, затрагивающие несколько стран или групп населения; они часто взаимосвязаны, что усиливает их воздействие. Так, в недавнем отчете RAND названы шесть основных глобальных угроз: искусственный интеллект, удары астероидов и комет, изменение климата, ядерная война, серьёзные пандемии (естественные или искусственные) и супервулканы.[13]

Термин «глобальный катастрофический риск» появился в литературе недавно. Как указано выше, он не имеет точного определения, но в целом означает риск, способный нанести серьёзный вред здоровью или выживанию человечества.[14] Таким образом, глобальный катастрофический риск можно определить как угрозу серьёзных последствий, способную вызвать

---

[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. См. также 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.

[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/.

сбой критических систем, необходимых для выживания человечества.[15] Эйвин с коллегами [16] подразделяют глобальные катастрофические риски на две категории: *природные риски*, например, пандемии или падение астероидов, которые не зависят от человека или очень трудно поддаются управлению, но представляют угрозу глобальной стабильности, и *антропогенные риски*, такие, как ядерная война, неадекватность ИИ или угрозы биотехнологий, когда действия человека могут вызвать далеко идущие непреднамеренные последствия.

Значительную часть глобальных катастрофических рисков составляют экзистенциальные риски, определяемые как риски, угрожающие полным исчезновением разумной жизни или радикально снижающие её качество. Ключевое отличие состоит в том, что «экзистенциальные катастрофы ограничивают возможность восстановления и дальнейшего развития».[17] Например, глобальный финансовый кризис может серьёзно нарушить жизнь общества и тем самым представлять собой катастрофический риск, а экзистенциальная катастрофа – глобальная пандемия с неизвестным патогеном или ядерная война – может подорвать способность цивилизации к восстановлению и привести к её исчезновению.[18]

В силу взаимозависимости стран, групп населения и глобальной инфраструктуры в глобальной экономике риски в одной области могут вызвать каскадные эффекты в других. В отличие от традиционных угроз безопасности, которые часто можно устранить в пределах национальных границ, глобальные риски требуют международного сотрудничества для защиты общечеловеческого достояния – «элементов планеты, выходящих за рамки национальной юрисдикции, которыми пользуются все страны».[19] Недавним примером глобального риска стала пандемия COVID-19, с которой ни одна страна не могла эффективно справиться в одиночку.

Поэтому в литературе о глобальных рисках отмечается необходимость международного сотрудничества и коллективных действий для их смягчения. Например, Шварц и Рэндалл [20] исследовали сложности прогнозирова-

---

[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.

[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.

ния и противодействия глобальным рискам, выступая за более комплексный подход к решению этих проблем. Их комплексный подход сосредоточен на планировании сценариев, междисциплинарном анализе, упреждающем смягчении рисков и международном сотрудничестве для повышения устойчивости к изменению климата и глобальным рискам.[21] Карри и О'Хейгертей [22] также отмечают, что Х-риски часто требуют глобального сотрудничества, поскольку они возникают из-за множества причин, выходящих за национальные рамки. В их работе подчёркнута необходимость международных структур управления для эффективного разрешения таких рисков, как конфликты из-за ИИ или биологическая война. Этот аргумент перекликается с концепцией «рефлексивной модернизации» [23] Бека, когда общество постоянно сталкивается с побочными эффектами технического прогресса.

В соответствии с этой точкой зрения, в отчете Центра по изучению экзистенциального риска за 2023 год отмечено, что для разрешения катастрофических и экзистенциальных рисков необходимы прочные структуры, объединяющие науку, политику и международное сотрудничество, для обеспечения своевременной и действенной реакции.[24] Чтобы преодолеть разрыв между наукой и политикой, Турчин и Денкенбергер [25] предлагают структуру, информирующую политиков о серьёзности и вероятности экзистенциальных и глобальных катастрофических рисков. Эта структурированная связь необходима для международных институтов безопасности, таких как НАТО, призванных разрешать возникающие риски и соответствующим образом адаптировать свою политику. Понимая эту необходимость, Отдел новых вызовов безопасности НАТО теперь фокусируется на таких вопросах, как кибервойна, управление ИИ и биотехнологии, признавая, что эти вызовы выходят за рамки традиционных военных проблем и важны для национальной безопасности.

В следующем разделе мы рассмотрим влияние новых технологий на новые риски.

---

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.

Новые риски и проблемы безопасности, возникающие из-за новых технологий

Новые технологии, включая искусственный интеллект, квантовые вычисления и синтетическую биологию, кардинально меняют международную безопасность. Эти технологии обещают большие возможности для развития человечества, но одновременно создают серьёзные риски из-за своего двойного применения.[26] Как отмечено в недавнем отчете Центра инноваций международного управления, эти технологии могут принести существенные социально-экономические выгоды за счет повышения производительности. Но они несут и риски, способные разрушить целые общества, включая их средства к существованию и социальные нормы.[27]

Сложность оценки рисков в этих областях невозможно переоценить. Например, ИИ все чаще используют в цифровых и роботизированных приложениях, включая военные и оборонные системы, что несёт как возможности, так и серьёзные риски. ИИ и системы с поддержкой ИИ используют на полях сражений, в системах командования и управления и в системах вооружений, таких как всё более автономные БПЛА. Ожидается, что их производительность превзойдёт производительность людей при решении многих задач, и они уже опережают людей по скорости работы и обработки данных.[28] С ростом автономности технологии всё больше превращаются в некий суррогат комбатантов.

Возможность неадекватности, нецелевого или злонамеренного использования ИИ требует создания новых глобальных структур управления и

---

[26] Учёные по-разному применяют термины «двойное использование» и «множественное использование» к новым технологиям. Например, «двойное использование» имеет несколько значений в зависимости от контекста – см. Jonathan B. Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (MIT Press, 2012). Оно может означать материалы, оборудование и знания, которые имеют мирное применение, но могут быть использованы для незаконного производства ядерного, химического или биологического оружия. Эти технологии несут дилемму «двойного назначения», поскольку сложно предотвратить их нецелевое использование, не отказываясь от полезных применений. В Thea Riebe, *Technology Assessment of Dual-Use ICTs – How to Assess Diffusion, Governance and Design* (Springer Nature, 2023) отмечено смешение инноваций в гражданском и военном секторах промышленности. Понятие «множественного использования» в научной литературе выходит за рамки двойного использования, означая пригодность для широкого спектра ситуаций. Новые технологии можно назвать «многоцелевыми» - см., например, 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.

международных соглашений для регулирования новой области автономности с применением ИИ.[29] Например, Группа правительственных экспертов ООН по летальным автономным системам вооружений (ЛАСВ) с 2015 года обсуждает, надо ли запретить ЛАСВ. До сих пор никакого соглашения нет, кроме набора из одиннадцати необязательных принципов.[30] Такие параллельные инициативы, как Политическая декларация об ответственном военном использовании искусственного интеллекта и автономности,[31] свидетельствуют о том, что государства всё больше обеспокоены военным использованием и автономностью ИИ. Эти инициативы на пути к созданию норм приветствуются, но им не хватает глобального консенсуса, особенно среди крупных держав, разрабатывающих эти технологии.

Картину усложняет роль негосударственных игроков, включая террористические группы, преступные организации и международные корпорации. При обсуждении национальной безопасности о международных технологических и инфраструктурных корпорациях часто забывают, хотя их деятельность и продукты могут иметь огромные последствия для международной безопасности, а преступные организации и даже отдельные преступники используют новые технологии для усиления своего влияния в преступных целях.[32]

Для разрешения этих взаимосвязанных рисков нужен более широкий анализ рисков, выходящий за рамки сугубо военного подхода. Правительства и международные структуры безопасности должны адаптировать свои структуры управления рисками, расширив их на нетрадиционных игроков в сфере безопасности и новые технологии. Например, атаки Аль-Каиды 11 сентября 2001 года продемонстрировали способность негосударственных игроков вызывать глобальные потрясения с помощью элементарных технологий. ИГИЛ стала первой организацией, в которой поняли, как превратить социальные сети в оружие, объединив вирусность этих платформ с ужасами видеороликов казней. Преступные организации всё шире используют киберпространство, создавая серьёзные угрозы глобальной безопасности с реальными издержками. Прогнозируется, что цена киберпреступности к 2025 году превысит 10 триллионов долларов.[33] Для сравнения, глобальная

[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/.

[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.

война с терроризмом в 2001-2020 гг. обошлась правительству США примерно в 5,4 триллиона долларов.[34] Поскольку эти группы действуют невзирая на границы, государствам очень сложно бороться с ними в одиночку, так как они не подпадают под юрисдикцию традиционных правоохранительных органов.[35]

Технологические, телекоммуникационные и энергетические компании тоже могут серьёзно влиять на национальную безопасность из-за утечки данных, уязвимости цепочек поставок или воздействия на окружающую среду.[36] Например, обновление CrowdStrike в июле 2024 года вызвало крупнейший сбой в работе ИТ в истории, который обошёлся компаниям из списка Fortune 500 более чем в 5,4 млрд. долларов.[37] Действия этих негосударственных игроков часто выходят за сферу контроля отдельных правительств, усложняя картину управления международной безопасностью, и, соответственно, требуют инновационных, совместных и многосторонних подходов.

Эти трансформации требуют изменений в восприятии угроз безопасности. Обычные военные угрозы по-прежнему существуют и вновь актуализировались с войной в Украине, но власть, полученная негосударственными субъектами и отдельными лицами с распространением новых технологий, размыла границы между комбатантами и гражданскими лицами, усложняя среду безопасности.[38] Благодаря доступности высокоэффективных технологий отдельные лица или небольшие группы могут разрабатывать биологическое оружие или совершать кибератаки с глобальными последствиями. Это также расширяет возможности отдельных лиц или компаний, чьи действия могут влиять на международную безопасность. Кроме того, растущая автономность техники с ИИ требует участия негосударственных субъектов в серьёзном глобальном анализе рисков.

Например, в то время как эскалация конфликта между государствами тщательно изучена и смоделирована, понимание того, как может разви-

---

[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. 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).

ваться его динамика с включением автономных элементов в системы ядерного командования, управления и связи (С3), ограничено.[39] Хотя в обычных и ядерных системах командования, управления и связи[40] предполагается повышение автономии, текущая политика и тенденции показывают, что в цикле принятия решений должны оставаться люди. Полезную аналогию для анализа потенциальных рисков можно провести с внезапными сбоями в высокочастотной торговле,[41] иллюстрирующими незапланированные последствия таких систем. В этом контексте осторожный подход к управлению рисками будет включать изучение последствий эскалации кризиса в сценариях, в которых автономные технологии играют вспомогательную роль. Поэтому традиционные военные стратегии и структуры анализа рисков уже недостаточны для понимания и управления этими сложностями, и требуются комплексные стратегии, объединяющие технологические и прогностические решения при разработке новых структур управления для эффективного противодействия рискам, возникающим из-за новых технологий.

Использование новых технологий в качестве оружия

Новые технологии меняют глобальную картину безопасности, требуя от политиков предвидеть новые вызовы. Использование ИИ, синтетической биологии, квантовых вычислений и нейротехнологий в качестве оружия создаёт новые риски для национальной и международной безопасности. ИИ всё шире используют в военных операциях и разведке по всему миру. Технику на основе ИИ применяют везде, от наблюдения до киберзащиты, для

---

[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] Женевский центр политики безопасности (GCSP) совместно с Группой стратегического прогнозирования (SFG) руководил диалогом экспертов из стран – постоянных членов Совета безопасности (Китай, Франция, Россия, Великобритания и США) о глобальных катастрофических рисках с акцентом на применение ИИ и других технологий в ядерном командовании, управлении и связи, включая инфраструктуру обеспечения принятия решений. Подробнее см. Strategic Foresight Group, “Roundtable on AI-NC3 Interface,” December 6, 2024, www.strategic foresight.com/news_inner.php?id=228; 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; “P5 Experts Roundtable Online Meeting: AI-Nuclear Nexus, 24 June 2024,” *GCSP News*, https://www.gcsp.ch/global-insights/p5-experts-roundtable-online-meeting-ai-nuclear-nexus-24-june-2024. См. также Alice Saltini, “AI and Nuclear Command, Control and Communications: P5 Perspectives,” *European Leadership Network,* November 13, 2023, https://european leadershipnetwork.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.

усиления устаревших платформ или в новом оружии, включая беспилотники.[42] Но риски, связанные с военным применением ИИ, велики: от неправомерного использования технологий до умышленного вредоносного применения ИИ.[43] Например, ИИ противника, использующий системы ИИ для генерирования вредных или неверных результатов, представляет растущую угрозу для военных и гражданских систем. Противник может использовать уязвимости в системе ИИ, чтобы сбить с пути автономный БПЛА или нарушить критически важную военную связь.[44]

Прогресс *синтетической биологии* расширил наше понимание механизмов заболеваний и позволил разработать новые методы лечения.[45] Однако эти технологии также представляют значительный риск для биобезопасности, поскольку они могут привести к воссозданию опасных патогенов без доступа к природным источникам.[46] Например, теоретически возможно синтезировать новый тип патогена.

Естественные патогены либо смертельны, либо вирусны, но не могут быть и тем, и другим одновременно, поскольку они убьют носителя, ещё не распространившись.[47] Однако современные биотехнологии и методы синтетической биологии позволяют создавать новые вирусы и бактерии, включая создание патогенов с нуля и модификацию существующих, делая их более заразными или смертоносными.[48] Также можно спроектировать живые системы для усиления роста и повышения патогенности, с модифицирован-

---

[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/.

[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.

ными бактериями и вирусами, потенциально пригодными для военных целей.[49] Поэтому правительства и международные организации должны разработать новые структуры управления для решения этих проблем и обеспечения ответственного использования синтетической биологии.

Хотя милитаризация *квантовых вычислений* ещё не материализовалась, она может сделать существующие методы шифрования устаревшими, создав новые уязвимости во всём, от военной связи до глобальных финансовых систем.[50] Такие технологии можно будет использовать для «расшифровки протоколов кибербезопасности, существенного улучшения систем навигации, а также для проектирования и изготовления компонентов оружия массового поражения».[51]

Дальнейшее развитие *технологий виртуальной реальности*, таких, как метавселенные и нейротехнологии, как инвазивных, так и неинвазивных, влияет на человеческое познание и принятие решений. Милитаризация этих технологий изменит природу войны, добавив шестую область[52] – познание и человеческий мозг. Когнитивная война – это «деятельность, направленная на контроль чужого ума и поведения».[53] Речь идет о контроле мыслей человека для влияния на его действия. Когнитивная война включает информационную войну, направленную на контроль потока информации для влияния на поведение.[54] Попытки повлиять на поведение не новы. Однако новой стала детализация, точность и масштаб, которые обеспечивают новые технологии. Например, нынешние дебаты в США о запрете TikTok показывают, насколько сильно социальные сети могут влиять на целое поколение пользователей, продвигая определённые нарративы.[55]

---

[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."

[52] Признанными средами ведения войны являются земля, воздух, море, космос и киберпространство.

[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/busi

Объединение иммерсивных технологий и нейротехнологий создаёт беспрецедентные возможности для оценки воздействия внешних стимулов (например, из метавселенной) на эмоциональную реакцию субъекта. Достижения в области инвазивных нейротехнологий, особенно в интерфейсах мозг-компьютер (BCI), позволяют стимулировать нейроны и изменять их реакции. Можно представить себе будущее, в котором такие технологии потенциально могли бы манипулировать мыслями и моделями мышления с удивительной точностью. Распространение этих технологий может обеспечить уровень манипуляции людьми в глобальном масштабе, никогда не наблюдавшийся в истории манипуляции или убеждения.

Если это станет реальностью, больше не понадобится физическое насилие, чтобы заставить противника изменить свое мнение, что является целью войны, как постулировал Клаузевиц, определявший войну как акт насилия для того, чтобы заставить противника выполнить свою волю.[56] Такие технологические разработки в корне изменят природу самой войны, чего не удавалось достичь ни одной предыдущей технологии. Стоит отметить, что хотя эти технологии ещё недостаточно зрелы для реализации таких возможностей, они уже продемонстрировали впечатляющие результаты. Например, BCI уже используют для лечения таких психиатрических расстройств, как эпилепсия,[57] а сочетание функциональной МРТ с алгоритмами всё больше позволяет машинам читать то, что видят люди.[58] Чтение мыслей уже не является научной фантастикой и вскоре найдёт военное применение. Следующим шагом в этих разработках станет запись в мозг, хотя она все ещё технологически далека.

Тем не менее потенциал этих достижений заставил НАТО серьёзно отнестись к когнитивной войне, опубликовав несколько исследований по этой теме и подчеркнув важность этой новой формы войны, доступной благодаря новым технологиям.[59]

Учитывая темпы развития технологий, при анализе рисков и в политике безопасности следует больше учитывать последствия этих новых технологий. Традиционный набор инструментов безопасности, предназначенный

---

ness/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.

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,” S*TO Technical Report* TR-HFM-ET-356 (Paris: NATO Science and Technology Organization, 2023).

для устранения угроз государству, недостаточен для борьбы с многогранными рисками, создаваемыми злонамеренным и/или военным использованием ИИ, синтетической биологии, квантовых вычислений или нейротехнологий.[60] Кроме того, наличие передовых технологий у негосударственных субъектов и отдельных лиц усложняет анализ рисков. Хакеры, преступные организации и даже отдельные лица теперь способны наносить масштабный вред при помощи кибератак, биотехнологических экспериментов или дезинформации, управляемой ИИ.

Оценка риска

Понятие риска не имеет общепринятого определения с учётом вероятности, ожидаемых результатов, опасностей или неопределённости.[61] С изменениями в международной безопасности традиционные структуры управления рисками должны адаптироваться для решения сложных задач, особенно возникающих из-за технологий искусственного интеллекта и синтетической биологии.[62] Эти технологии создают взаимосвязанные риски, требующие новых подходов для точной оценки и эффективного смягчения последствий.[63] Например, проблема «чёрного ящика»,[64] когда алгоритм принятия решений непрозрачен,[65] создаёт потенциальные комплексные воздействия. Объединение технологий ИИ и синтетической биологии повышает

---

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.

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,” в *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.

сложность из-за усугубляющих эффектов их взаимодействия. Эти риски взаимодействия требуют упреждающих стратегий, включая анализ сценариев и сканирование окружающей среды [66] для более эффективного прогнозирования угроз. Объединение ИИ и биологических систем создаёт проблемы безопасности, выходящие за традиционные рамки,[67] особенно из-за нелинейной эскалации риска,[68] когда последствия нарастают непропорционально относительно первоначальной вероятности или серьёзности. Эту динамику иллюстрирует изменение климата, усугубляющее такие проблемы, как нехватка ресурсов и геополитическая нестабильность, которые усложняют однозначные ответы [69] и указывают на необходимость моделей риска, предназначенных для управления взаимосвязанными системами.

Для лучшей оценки риска нужно учитывать системную взаимосвязь и развивающуюся природу технологий, что позволит оценивать риск более комплексно.[70] Сетевой анализ, доказавший свою эффективность в таких областях, как финансы и кибербезопасность, позволяет понять как риски распространяются по взаимосвязанным системам, выявляя уязвимости в критических точках.[71] Применительно к ИИ и биотехнологиям этот подход может раскрыть зависимости, которые традиционные модели упускают из виду, способствуя более эффективному управлению рисками.

---

[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.

[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.

Прогностическая аналитика и вероятностные модели, такие, как моделирование по методу Монте-Карло,[72] повышают точность, предлагая руководителям эффективные идеи упреждающих действий. Присущая взаимозависимость таких технологий, как ИИ и синтетическая биология, затрудняет их отдельную оценку. Сетевые эффекты, когда отказ или неправильное использование одного компонента влияет на несколько систем, очень часто – каскадно, указывают на необходимость системного анализа рисков. Например, автономные системы с ИИ могут давать неожиданные сетевые эффекты, нарушающие важную инфраструктуру.[73] Теория сложных систем и сетевой анализ[74] позволяют количественно оценить эти взаимозависимости, что даёт возможность создавать комплексные структуры управления рисками, отвечающие требованиям взаимосвязанного мира.

В условиях всё более сложной и изменчивой картины угроз руководители должны отдавать приоритет адаптивности и надёжности своих стратегий. Традиционные прогностические модели часто не срабатывают, сталкиваясь с новыми или неожиданными вызовами. Исходя из этих принципов, можно разрабатывать системы, способные реагировать на сценарии, выходящие за рамки обычных прогнозов, обеспечивая большую устойчивость в условиях неопределённости. Этот подход особенно важен при внедрении передовых технологий, таких как искусственный интеллект, который влечёт не только технические риски, но и глубокие этические и социальные последствия.[75] Например, применение автономных систем порождает вопросы ответственности и контроля, усложняющие традиционное управление рисками. Поэтому комплексный подход на основе рисков должен включать системный анализ, учитывающий взаимозависимость технологических, этических и социальных рисков. Такой подход позволит руководителям предвидеть и управлять последствиями угроз, гарантируя своевременность и эффективность реакции в динамичных условиях.

С усложнением новых технологий эффективное управление рисками требует передового моделирования и межотраслевого взаимодействия для

---

[72] Исследования на основе моделирования Монте-Карло дают более гибкие модели, поскольку переменные можно описать с помощью распределения вероятностей. Этот подход даёт лучшее понимание конкретных результатов и повышает способность идентифицировать наиболее репрезентативные переменные модели.

[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.

понимания их социальных последствий. Включение сетевого анализа в современную оценку рисков имеет важное значение для решения проблемы растущей сложности взаимосвязанных систем, повышения точности прогнозов и упреждающего управления системными рисками.[76] Объединение этих методов позволяет аналитикам лучше понять сложные риски, связанные с комплексным воздействием новых технологий. В следующем разделе мы рассмотрим, как Рабочая группа по новым вызовам безопасности (ESCWG) Консорциума «Партнёрство ради мира» (ПРМ) рассматривает риски военного использования новых технологий.

Как рабочая группа по новым вызовам безопасности Консорциума ПРМ рассматривает эти вопросы?

За последние пять лет рабочая группа Консорциума ПРМ по новым вызовам безопасности детально рассмотрела новые риски, уделяя особое внимание таким критически важным областям, как искусственный интеллект, роевые технологии, кибербезопасность, гибридные угрозы,[77] когнитивная война, нейротехнологии, генеративный ИИ, синтетическая биология [78] и глобальные изменения соотношения сил.

Кибервойна и реакция НАТО

Одной из самых серьёзных проблем, с которыми сталкивается НАТО, является кибервойна. Кибератаки становятся всё более изощрёнными, разрушая критически важную инфраструктуру, военные системы и демократические институты. Согласно отчету НАТО, эти угрозы быстро развиваются, и противники используют передовые методы подрыва национальной безопасности и стабильности стран-участниц.[79] Развитие киберспособностей не только усиливает угрозы, но и меняет глобальную динамику власти, вынуждая НАТО повышать свою киберустойчивость. Конкуренция за техноло-

[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.

гическое доминирование стала определяющей чертой международных отношений, поскольку новые технологии могут усиливать возможности государственных и негосударственных игроков.[80]

На недавнем семинаре, организованном ESCWG, эксперты отметили, что противники превратили в оружие роевые технологии и ИИ, создав новые инструменты для использования уязвимостей в киберзащите НАТО. НАТО отреагировало повышением киберустойчивости, сосредоточившись на улучшении возможностей обнаружения, защиты и восстановления после киберинцидентов.[81]

Инициативы наподобие учений Cyber Coalition иллюстрируют усилия НАТО по укреплению кибербезопасности стран-участниц посредством коллективного обучения.[82] Cyber Coalition – это важные многонациональные учения по проверке и усилению возможностей НАТО и стран-партнёров реагировать на киберугрозы.[83]

НАТО осознаёт необходимость комплексного реагирования, поскольку гибридная война, включающая обычную, кибер- и асимметричную тактику, становится всё более распространённой. Действия России в Украине и её продолжающиеся киберкампании против членов НАТО указывают на срочность устранения угроз, выходящих за традиционные военные рамки.[84] С этой целью Консорциум ПРМ по инициативе ESCWG недавно опубликовал примерную учебную программу по гибридным угрозам и гибридной войне, содержащую основные справочные материалы для преподавания этих тем.[85]

Роевые технологии и ИИ в войне

Использование ИИ и автономных систем создаёт для НАТО как возможности, так и проблемы. Роевая технология, позволяющая беспилотным летательным аппаратам и другим устройствам с ИИ действовать согласованно, существенно изменила баланс наступательных и оборонительных стратегий. Эта технология позволяет подавить традиционные системы обороны,

---

[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, по состоянию на 13 декабря 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.*

координируя множественные атаки одновременно,[86] что снижает эффективность обычных средств защиты.

Например, всё более массовое использование автономных беспилотников в Украине и на Ближнем Востоке, хотя ещё не настоящих роёв,[87] показало их способность преодолевать традиционные системы обороны, демонстрируя новую парадигму ведения войны.[88] Рой дронов включает несколько БПЛА, работающих в иерархических группах, чтобы преодолеть ограничения отдельных БПЛА. Эти системы являются примером многокомпонентных систем, способных выполнять задачи, которые отдельные дроны выполнить не могут. Кроме того, рой дронов может выполнять множество распределённых задач одновременно.[89] Для решения этих задач НАТО следует инвестировать в технологии противодействия роям и оборонительные системы на основе ИИ, способные самостоятельно противодействовать этим угрозам.

На последних семинарах ESCWG была отмечена важность учёта ИИ в военных доктринах. Однако распространение этих технологий означает, что противники, включая негосударственные субъекты, тоже могут использовать их при относительно низких затратах. Использование летального автономного оружия хотя и даёт значительные военные преимущества, но также создаёт риски непредсказуемых неудач и морально-этических дилемм.[90]

Когнитивная война и генеративный ИИ

Касательно когнитивной войны на семинаре ESCWG было отмечено, что генеративный ИИ несёт серьёзные риски, поскольку он может производить высокореалистичный синтетический контент, включая дипфейки и сфабрикованные синтетические медиа. Эти возможности усиливают кампании дезинформации, позволяя противникам подрывать доверие к институтам и ма-

---

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

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/.

нипулировать общественным мнением во время конфликтов. Отчёт корпорации RAND подтверждает это, отмечая пагубное влияние дипфейков на общественное доверие и правдивость информации, что показывает, насколько легко генеративный ИИ может искажать реальность и влиять на восприятие.[91]

Доступность инструментов генеративного ИИ также увеличивает вероятность использования этих технологий государственными и негосударственными субъектами и даже отдельными лица в своих целях, таких, как вымогательство, распространение дезинформации или влияние на демократические процессы, включая выборы.[92] Понимая эти взаимосвязанные угрозы, НАТО поощряет сотрудничество с научными учреждениями и странами-участницами для разработки принципов разрешения когнитивных угроз, включая дезинформацию, усиленную генеративным ИИ. По мере развития этих технологий НАТО должно адаптировать свои стратегии для противодействия когнитивной войне и распространению дезинформации, генерируемой ИИ, тем самым обеспечив устойчивость к этим комплексным вызовам.

Соперничество великих держав

Хотя новые технологии несут новые риски, международная обстановка, в которой эти технологии развиваются, тоже важна для любого анализа глобальных рисков. Геополитическая картина претерпевает значительные изменения, с неравенством сил не только среди стран, но и среди негосударственных субъектов, включая террористические группы и частные компании. Продолжающаяся конкуренция за технологическое превосходство, особенно между США и Китаем, подчёркивает стратегические проблемы, с которыми сталкивается НАТО за пределами своих границ. Как отмечено в докладе Сэмсона с коллегами, взаимосвязь между технологическим прогрессом и изменением соотношения сил усложняет роль НАТО в поддержании стабильности и безопасности в многополярном мире.[93]

Рост Китая как мировой державы, его инициатива «Один пояс, один путь» и напористость в регионе Южно-Китайского моря, в сочетании с размещением военных сил вдали от его территории, представляют новые стратегические вызовы для НАТО. В то время как США сосредоточены на соперничестве великих держав, НАТО необходимо подтвердить свои стратегии для сохранения своих позиций в многополярном мире. Растущее влияние Китая в Европе, особенно за счёт инвестиций в критическую инфраструктуру, включая порты, вызывает обеспокоенность из-за зависимостей в области безопасности, которые могут быть использованы во время кризисов.

---

[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.

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

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

Использование взаимозависимостей в качестве оружия,[94] определяемое как «условие, при котором игрок может использовать своё положение во внедрённой сети, чтобы при торгах получить преимущество над другими в замкнутой системе», становится методом ослабления противника. Использование взаимозависимостей в наших глобализованных сетях в качестве оружия позволяет обнаруживать и использовать уязвимости, принуждать к изменению политики или сдерживать нежелательные действия.[95]

Соперничество великих держав с Россией и Китаем вынуждает НАТО внедрять инновации и включать эти технологии в свои стратегии. Однако глобальные и децентрализованные цепочки поставок и системы производства [96] делают эти технологии уязвимыми в силу взаимозависимостей, превращающих их в оружие.[97] Кроме того, поддержание технологического превосходства и совместимости стран-участниц важно для эффективного противодействия этим новым угрозам. Герцог и Кунертова [98] утверждают, что хотя НАТО имеет потенциал для лидерства в военном применении новых технологий, его реализация потребует глубоких преобразований в бюрократической практике и большего участия европейских союзников в распределении технологического бремени.

Выводы и рекомендации

Третье десятилетие XXI века отмечено традиционным соперничеством великих держав и военным использованием новых технологий. Международную среду безопасности характеризуют традиционная силовая политика и связанные с ней риски. Растущая взаимосвязь геополитики и технологий усилила конкуренцию, причём Китай и США борются за контроль над правилами и институтами, которые будут определять будущие международные отношения.[99]

---

[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.

[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.

Быстрое развитие, распространение и доступность новых технологий, включая искусственный интеллект, синтетическую биологию и кибервозможности, порождают новые виды рисков, которые гораздо сложнее понять и смягчить. Глобальные риски взаимосвязаны, что усложняет проблемы современной безопасности. Понятия глобального катастрофического риска и экзистенциального риска всё больше применимы к таким проблемам, как изменение климата, биотехнологии и ядерная война – проблемам, требующим глобальных, а не национальных решений.

Поэтому политика безопасности должна перейти от угроз к рискам для выявления слабых мест. Эффективное смягчение возникающих рисков будет зависеть от глобального сотрудничества, партнёрства государства с частным сектором и инновационных структур управления, причём НАТО будет играть ведущую роль в содействии эффективному использованию прорывных технологий. Переход от традиционного подхода на основе угроз к структуре, основанной на рисках, имеет решающее значение для НАТО, особенно с учетом того, что Повестка НАТО на период до 2030 года признаёт эти проблемы, хотя необходимы дополнительные усилия.

Примечание

Представленные здесь взгляды принадлежат исключительно авторам и могут не отражать официальную политику Консорциума «Партнёрство ради мира» или его руководства.

Об авторах

Д-р **Жан-Марк Рикли** – руководитель отдела глобальных и новых рисков, директор Полиматической инициативы Женевского центра политики безопасности. Также является сопредседателем рабочей группы по новым вызовам безопасности Консорциума Партнёрства ради мира (ПРМ), одним из кураторов Международной карты безопасности Стратегической информационной платформы Всемирного экономического форума.
Электронная почта: j.rickli@gcsp.ch
https://orcid.org/0000-0003-4459-1802

Д-р **Гёзим Влласи** – старший консультант программы в отделе посредничества и поддержания мира Женевского центра политики безопасности (GCSP) в Женеве, Швейцария. Ранее Влласи был докторантом Университета Граца, Австрия, и докторантом GCSP.
E-mail: G.Vllasi@gcsp.ch; https://orcid.org/0009-0000-2151-6151

Библиография

"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.