NEW TECH IN REVIEW

The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach

Raluca Csernatoni and Katerina Mavrona

EU CYBER DIRECT

September 2022

Contents

Disclaimer

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Introduction

Digital technologies increasingly complicate and transform present-day conflicts. The current war between Russia and Ukraine, for instance, is also played out in cyberspace, involving multiple public and private actors. This ranges from the formation of an IT army of Ukrainian volunteers, to the intensification of Kremlin-backed malicious cyber operations, to Western allied nations offering Ukraine assistance across "the full spectrum; offensive, defensive, [and] information operations."[1]

Such developments matter as they are consistent with a longer history of cyber conflicts[2] running alongside and feeding into kinetic operations. Even if the conflict's cyber dimension is, as noted by experts,[3] presently limited, there are serious concerns about the destabilisation of the international security environment, including high risks of escalation. These risks are also exacerbated by the potential spillover of cyberattacks targeting Ukraine into other countries, which could cause systemic ripples in cyberspace and beyond. It was such cross-border effects that led the European Union (EU) to issue a declaration[4] on May 10, strongly condemning the malicious cyber activity conducted by the Russian Federation, which targeted the satellite KA-SAT network owned by VIASAT and facilitated the military invasion of Ukraine.

Among actors amplifying the cyber dimension of the conflict are tech companies, which have supported the Ukrainian effort by deploying state-of- the-art cyber capabilities. These include the use of emerging disruptive technologies (EDTs) and in particular artificial intelligence (AI) in cyber operations. For example, it has been made known that Ukraine is using Clearview AI's facial recognition software[5] to identify Russian soldiers and Ukrainians killed on the battlefield. In response to the expanding Ukraine-Russia conflict, Vectra AI, a leader in AI-driven threat detection[6] and response for hybrid and multi-cloud enterprises, is offering a slate of free cybersecurity tools and services to organisations that believe they may be targeted as a result of this conflict. Use of these cyber tools in the context of an ongoing war is both a novelty and an added complication insofar as these may tamper with or potentially generate new conflict dynamics.

Indeed, in the bigger picture of day-to-day cybersecurity practice, already many complex challenges are mitigated by applying AI tools and intelligent solutions,[7] as new advanced capabilities are developing at a fast pace. Developments have grasped the attention of experts[8] globally who analyse the potential effects of the AI-cybersecurity[9] convergence on themes including surveillance, national security, and geopolitical competition for technological development.

---

[1] Kaminska, Monica, and James Shires, and Max Smeets (2022) Cyber operations during the 2022 Russian invasion of Ukraine: Lessons learned (so far). ECCRI Tallin Workshop Report, European Cyber Conflict Research Initiative, July 2022. Available from https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.

[2] See above.

[3] Heinl, Caitriona, *et al.* (2022) Is War in Ukraine the End of Cyber Diplomacy. Directions, 18 March. Available from: https://directionsblog.eu/is-war-in-ukraine-the-end-of-cyber-diplomacy/.

[4] Council of the European Union (2022b) Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, 10 May. Available from: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

[5] The New York Times (2022) Facial Recognition Goes to War. Available from: https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html.

[6] Vectra (2022) As the War in Ukraine Spirals, Vectra AI Announces Free Cybersecurity Services. Available from: https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services.

[7] Heinl, Caitríona H. (2014) Artificial (intelligent) agents and active cyber defence: Policy implications. 6th International Conference On Cyber Conflict (CyCon 2014) 53-66. 3 June. Available from: https://ieeexplore.ieee.org/abstract/document/6916395/authors#authors.

[8] CSET (2022) Publications. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/publications/?fwp_topic=cyberai.

[9] Kangas, Santeri (2022) Why AI is the key to cutting-edge cybersecurity. World Economic Forum, 21 July. Available from: https://www.weforum.org/agenda/2022/07/why-ai-is-the-key-to-cutting-edge-cybersecurity/.

Less attention has however been given to understanding how the EU and its various institutions and agencies engage with the many technical, operational, and policy-related questions surrounding this burgeoning nexus between AI and cybersecurity. Accounting for the lack of analytical attention, this article aims to examine the EU's approach to potential challenges and opportunities emanating in this policy field and corresponding policy solutions put forward.

For instance, as a dual-use technology defined by the European Commission as "disruptive,"[10] AI is starting to play a vital role in the EU's digital transformation and cybersecurity planning in both civil and military domains. Already in December 2020, the European Union Agency for Cybersecurity (ENISA) warned in a report[11] on artificial intelligence cybersecurity challenges that AI could provide both opportunities and challenges. These range from cybersecurity for AI to AI in support of cybersecurity to malicious and adversarial uses of AI. The latter category involves sophisticated attacks such as AI-powered malware, AI-enhanced *distributed denial-of-service* (DDoS) attacks, and AI-enabled advanced disinformation campaigns.

Indeed, the EU recognises the countless possible ways the cyber-related uses of EDTs could fundamentally impact the threat landscape in Europe. The EU's Cybersecurity Strategy for the Digital Decade[12] from December 2020 already identified key technologies like AI, encryptions, quantum computing, and future generation networks as essential to cybersecurity. The strategy notes that cybersecurity considerations must be integrated into all digital investments related to the above technological fields and the integrity of their supply chains. The council's conclusions[13] on the development of the European Union's cyber posture from May 2022 also stress "the importance to make intensive use of new technologies, notably quantum computing, Artificial Intelligence and Big Data, to achieve comparative advantages, including in terms of cyber responsive operations."

To examine the range of relevant initiatives, the article will first highlight several areas of possible interest and examine the implications of rapidly evolving AI systems in relation to cyber-related policy. Second, the article continues by tracing EU policy initiatives in both domains of interest (the EU's AI and cybersecurity policies) in an attempt to carve out possible connections between the two domains in existing policy planning, as well as explore whether interconnections between the two fields figure in EU policy thinking. Lastly the article zooms in on a range of promising initiatives spanning from regulatory approaches to research and innovation projects. The latter could potentially further sync the two areas into producing innovative policy and practices within the EU's evolving AI-cyber policy nexus.

AI and Cyber: A Multidimensional Relation

The fast-growing field of AI is considered one of the most important developments for the so-called Fourth Industrial Revolution.[14] As the European Commission highlights in its Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence[15] (AI Act) of 2021, "by improving prediction, optimising operations and resource allocation […] the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy."

---

[10] European Commission (2021a) Action Plan on synergies between civil, defence and space industries, 22 February. Available from: https://ec.europa.eu/info/sites/default/files/action_plan_on_synergies_en.pdf.

[11] ENISA (2020) Artificial Intelligence Cybersecurity Challenges, 15 December. Available from: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

[12] European Commission (2020c) Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[13] Council of the European Union (2022a) Council conclusions on the Development of the European Union's Cyber Posture, 23 May. Available from: https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

[14] Schäfer, Matthias (2018). The fourth industrial revolution: How the EU can lead it. European View, 17(1): 5-12. Available from: https://www.martenscentre.eu/wp-content/uploads/2020/10/1781685818768125-1.pdf.

[15] European Commission (2021b) Proposal for a Regulation laying down harmonised rules on artificial intelligence, 21 April. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

This potential however makes cybersecurity a necessary precondition for the secure deployment of these systems for all other social and economic purposes. Indeed, the EU does not fail to stress[16] that "cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so by within the assurance that they will be shielded from cyber threats." And at the same time, cybersecurity is itself a domain that could arguably harness the power of AI systems.

Innovative AI-based solutions,[17] from new techniques and algorithms helping to speed up mundane yet time-consuming tasks, to AI-supported cyber capabilities with potential strategic significance,[18] all presently deployed applications, and those at earlier stages of development, display features that may revolutionise cybersecurity capabilities and operations. Compared to conventional cybersecurity methods, they are expected to operate at greater scale and speed,[19] be more adaptable, and stealthier. They could thus help improve security performance and strengthen the protection of digital systems from an increasing number of sophisticated cyber threats. For instance, Pillsbury - a global law firm focusing on technology - and The Economist Intelligence Unit have noted in a report[20] that 49 percent of world leaders think AI is the best tool to counter nation-state cyberattacks. Widespread machine learning and AI-powered systems across cybersecurity[21] range from anomaly detection algorithms to detect malicious traffic or user behaviors in real time to algorithms for zero-day malware and spam detection to AI systems prioritising threats and taking automated remediation actions. Research focus is globally devoted to up-and-coming systems able to deliver sophisticated cyber campaigns with novel characteristics, ranging from malware "capable of tactical adaptation"[22] to "value calculations vis-à-vis strategic objectives."

There are also risks and concerns related to the complexities of AI and human agents' interactions: the potential technical glitches of still evolving systems, not to mention the challenges of transparency related to understanding the "black box" of intelligent systems' behavior.

Nevertheless, there are also emerging risks and concerns related to the complexities of AI and human agents' interactions: the potential technical glitches of still evolving and not yet mature systems, not to mention the challenges of transparency related to understanding the so-called "black box"[23] of intelligent systems' behavior. This leads to a series of important considerations regarding the security of AI systems already deployed in a range of sectors such as industry, health, finance, law enforcement and border security, and defense. These systems equally need cybersecurity protections and defenses against potential adversarial attacks to the AI itself. They need to be secured not only

[16] European Commission (2020c) Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[17] Li, Jian-hua (2018) Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering 19(12):1462-1474. Available from: https://link.springer.com/article/10.1631/FITEE.1800573.

[18] Johnson, James (2019) The AI-cyber nexus: implications for military escalation, deterrence and strategic stability. Journal of Cyber Policy, 4(3): 442-460. Available from: https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1701693.

[19] Whyte, Christopher (2020) Poison, Persistence, and Cascade Effects. Strategic Studies Quarterly, 14(4): 18-46. Available from: https://www.jstor.org/stable/26956151#metadata_info_tab_contents.

[20] Pillsbury & The Economist Intelligence Unit (2021) AI & Cybersecurity: Balancing Innovation, Execution & Risk, 9 September. Available from: https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

[21] Korolov, Maria (2022) Top Three Use Cases for AI in Cybersecurity. Data Centre Knowledge, 3 February. Available from: https://www.datacenterknowledge.com/security/top-three-use-cases-ai-cybersecurity.

[22] Whyte, Christopher (2022) Machine Expertise in the Loop: Artificial Intelligence Decision-Making Inputs and Cyber Conflict. In *2022 14th International Conference on Cyber Conflict: Keep Moving!* 700: 135-154. Available from: https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf.

[23] Castelvecchi, Davide (2016) Can we open the black box of AI?. *Nature News* 538(7623): 20. Available from: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731.

from conventional threats but also from new AI-targeting attacks[24] such as poisoning - a type of attack where intruders feed an algorithm with altered data to modify its behaviour according to their own aims.

ENISA describes these dynamics in its recent report on artificial intelligence cybersecurity challenges,[25] distinguishing between AI-targeting and AI-supported cyberattacks. This multidirectional linkage between cybersecurity and AI systems defines an increasingly relevant policy nexus, which should be of high concern to the EU. Interestingly the report recommends that the EU needs to dedicate more attention to how the AI and cyber nexus plays out in the context of an evolving threat landscape and in the case of both cybersecurity and cyber defense capabilities and operations. ENISA's report[26] further highlights the agency's effort to actively map the AI ecosystem and corresponding cybersecurity challenges by considering such challenges at various stages of the AI lifecycles. In particular, the report underlines the need to prioritise the security of supply chains, innovation, and capacity-building when it comes to all the elements of a secure, robust, and trustworthy European AI ecosystem.

We argue that these key dimensions should potentially be further reflected in the upcoming 2022 EU Cyber Defence Policy[27] in order for the EU to be better prepared "to protect, detect, defend, and deter against cyberattacks," as well as in the new 2022 European Cyber Resilience Act and the work of the Joint Cyber Unit (JCU).[28] Given evidence of recognition by the EU that AI can be both a friend and a foe to cybersecurity, the next section asks about the stage of development of various EU initiatives and instruments and the coherence of current EU efforts.

The AI-Cyber Nexus: New Governance Challenges

The EU seems to acknowledge the need to explore the operational use of AI systems in support of broader cybersecurity aims and interests. For instance, in its 2020 EU Cybersecurity Strategy, the European Commission proposes to build a network of security operation centers (SOCs) for threat intelligence powered by AI in the form of the EU Cyber Shield.[29] The AI-cybersecurity nexus can be roughly divided within the EU between two functional but interconnected areas of operational and regulatory interest.

As noted above, AI systems are increasingly embedded into the daily operations of cybersecurity teams in the private and public sectors, aiding in the effort to protect firms and organisations. Vendors claim that systems at the current level of technological development are able to perform tasks such as intrusion and threat detection,[30] curation of intelligence, or vulnerability discovery[31] while providing unprecedented levels of time and resource efficiency. It is these types of functionalities that EU actors seem to have taken notice of when drafting plans for the European Cyber Shield and SOCs referenced above. The work of these SOCs is "highly demanding and fast-paced, which is why AI and in particular machine learning techniques can provide invaluable support to

[24] Lohn, Andrew and Wyatt Hoffman (2022) Securing AI How Traditional Vulnerability Disclosure Must Adapt. Center for Security and Emerging Technology (CSET): Washington, DC, USA.. Available from: https://cset.georgetown.edu/publication/securing-ai-how-traditional-vulnerability-disclosure-must-adapt/.

[25] ENISA (2020) Artificial Intelligence Cybersecurity Challenges, 15 December. Available from: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

[26] See above.

[27] Cyber Risk GmbH (2022) Pillar 2: Secure - Strategic Compass of the European Union, Available from: https://www.strategic-compass-european-union.com/2_Secure_Strategic_Compass.html#:~:text=In%202022%2C%20we%20will%20further,Joint%20Cyber%20Unit%20will%20continue.&text=By%20the%20end%20of%202023,Strategy%20for%20security%20and%20defence.

[28] European Commission (2021e) Joint Cyber Unit. Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit.

[29] Prucková, Michaela (2021) New EU's cybersecurity package: ambitious proposals, daring tasks and deeper cooperation. CCDCOE. Available from: https://ccdcoe.org/library/publications/new-eus-cybersecurity-package-ambitious-proposals-daring-tasks-and-deeper-cooperation/.

[30] Microsoft (2021) Microsoft Digital Defense Report. Available from: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report.

[31] IBM (2022) Artificial intelligence (AI) for cybersecurity. IMB Solutions. Available from: https://www.ibm.com/security/artificial-intelligence.

practitioners" when it comes to speedily detecting, analysing, and responding to cybersecurity incidents. The aim of the SOCs is "to improve incident detection, analysis and response speeds through state-of-the-art AI and machine learning capabilities."

AI systems are poised to support operations in cyberspace that move beyond purely defensive activity. Reliance - even if partial - on AI capabilities in offensive cyber operations is considered the next level of development for the cybersecurity-AI domain.[32] Since DARPA's 2016 Cyber Grand Challenge[33] competition to create automatic defensive systems capable of self-patching, many relatively ambitious estimates anticipate future systems capable of "fighting dynamically against attackers."[34] It is not expected that such systems will materialise in the short term, as the current research focus is more on improving human-machine teaming,[35] as exemplified in recent DARPA projects. The EU has a keen interest in keeping an eye on developments. This is especially so as China and Russia are working to develop relevant capabilities, including software "capable of running their cyber offensives more autonomously."[36]

Reliance - even if partial - on AI capabilities in offensive cyber operations is considered the next level of development for the cybersecurity-AI domain.

It is worth noting that AI is not always built with cyber defense or offense specifically in mind. Rather, AI is a "general purpose technology," a generic technology that over time "comes to be widely used, to have many uses, and to have many spillover effects."[37] Such spillover effects are hard for policymakers to predict, let alone regulate, and demand adaptive forms of governance capable of accounting for the expanded and unpredictable use cases, as well as significant degrees of organisational adaptability.[38] In security terms, this equates to a continuous broadening and deepening of the vulnerabilities surface, far beyond what was experienced by conventional digitalisation processes of previous decades.

One such instance is given by the opening of many algorithms for public use, and often for entertainment or commercial purposes. Social media have recently been filled with images from public use of DALL-E mini,[39] with the model having been made available to the public for use with fun and sometimes bizarre outcomes. Despite the output of public experimentation, dangers of popularisation exist especially as commercialisation takes place in an environment where disinformation[40] has long been elevated to a public threat and even to a threat to

[32] Hoffman, Wyatt (2021) AI and the Future of Cyber Competition. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/publication/ai-and-the-future-of-cyber-competition/.

[33] Fraze, Dustin (2016) Cyber Grand Challenge (CGC). Defense Advanced Research Projects Agency (DARPA). Available from: https://www.darpa.mil/program/cyber-grand-challenge.

[34] Muser, Micah and Ashton Carriott (2021) Machine Learning and Cybersecurity - Hype and Reality. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf.

[35] DARPA (2022) AI Next Campaign. Defense Advanced Research Projects Agency (DARPA). Available from: https://www.darpa.mil/work-with-us/ai-next-campaign.

[36] Lohn, Andrew (2022) Testimony before the Senate Armed Services Subcommittee on Cybersecurity. Center for Security and Emerging Technology (CSET): Washington, DC, USA, 3 May. Available from: https://cset.georgetown.edu/publication/andrew-lohns-testimony-before-the-senate-armed-services-subcommittee-on-cybersecurity/.

[37] Crafts, Nicholas (2021) Artificial intelligence as a general-purpose technology: an historical perspective, *Oxford Review of Economic Policy*, 37(3): 521–536. Available from: https://academic.oup.com/oxrep/article/37/3/521/6374675?login=true.

[38] Horowitz, Michael (2020) AI and the Diffusion of Global Power. In *Modern Conflict and Artificial Intelligence*. A CIGI essay series. Centre for International Governance Innovation (CIGI). Available from: https://www.cigionline.org/sites/default/files/documents/Modern%20Conflict%20and%20AI_web.pdf#page=36.

[39] Knight, Will (2022) DALL-E Mini Is the Internet's Favorite AI Meme Machine. WIRED, 27 June. Available from: https://www.wired.com/story/dalle-ai-meme-machine/.

[40] Helmus, Todd C. (2022) Artificial Intelligence, Deepfakes, and Disinformation: A Primer. Santa Monica, CA: Rand Corporation. Available from: https://www.rand.org/pubs/perspectives/PEA1043-1.html.

democratic systems. In addition, it is worth wondering what implications the democratisation of access and use of off-the-shelf AI systems could have for cybersecurity and defense, especially given the expansion of the vulnerability surface accompanying the widespread deployment of AI for civilian and military purposes as described above.

Is the EU ready to respond to and counter current and future opportunities and threats emanating from the AI-cybersecurity nexus? And what actions should be taken concerning products safety and security, investments, innovation, and geopolitical competition for systems deployment and more?

The EU's Responses: Connecting the Dots?

The EU has undertaken regulatory, policy, and operational initiatives with heightened relevance for the AI-cybersecurity nexus. They are part of recent efforts toward the overall consolidation of the EU's technological leadership and sovereignty[41] in critical technological areas, as well as its economic competitiveness and strategic autonomy in security and defense.

Regulatory and Policy Interventions

The EU views cybersecurity as both a precondition and a means for achieving the aims of resilience, technological autonomy, and leadership: the 2020 Cybersecurity Strategy [42] noted that "the upcoming decade is the EU's opportunity to lead in the development of secure technologies across the whole supply chain."

The strategy further flags the need for new technological innovation and industrial policies to achieve such goals. This forward-looking technological and industrial approach, however, will need to be matched by (geo)strategic thinking and concrete actions. What is more, the strategy promises to integrate cybersecurity into digital investments and the development of "key technologies like Artificial Intelligence (AI), encryption and quantum computing" by using incentives, obligations, and benchmarks. Not surprisingly, the EU's 2022 Strategic Compass for Security and Defence[43] reinforces such ideas by flagging the importance of EDTs in the cyber domain and for cyber defense, noting the development and "intensive" use of new technologies such as AI, big data, and quantum computing to "achieve comparative advantages in terms of cyber responsive operations and information superiority."

These aspirations are accompanied by an emerging EU regulatory architecture, including the Commission's proposed draft AI Act,[44] the Data Act,[45] the move from the Network and Information Security (NIS)[46] Directive to its follow-up, the proposal for the NIS 2 Directive[47] (currently under negotiation); the recently tabled Digital

---

[41] Csernatoni, Raluca (2021) The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty. Carnegie Europe Program. Available from: https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.

[42] European Commission (2020d) New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Press Release, 16 December. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

[43] European Union External Action Service (EEAS) (2022) A Strategic Compass for Security and Defence. European Union External Action Service (EEAS), 23 March. Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

[44] European Commission (2021c) Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 21 April. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[45] European Commission (2022b) Data Act: Commission proposes measures for a fair and innovative data economy. Press Release, 23 February. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[46] European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, July 6. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148.

[47] European Commission (2020e) Proposal for directive on measures for high common level of cybersecurity across the Union. Policy and Legislation, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

Services Package, consisting of the Digital Services Act (DSA)[48] and the Digital Markets Act (DMA),[49] and the forthcoming Cyber Resilience Act (CRA).[50] These are complemented by a range of operational elements focused on capability generation and deployment.

Nevertheless, the above regulatory architecture is also characterised by a sometimes-clashing division of competences among EU actors, namely the European Commission, the European External Action Services, the member states, and EU agencies entrusted with developing domain specific policies, first and foremost ENISA. The EU's security and defense policy field is an illustrative example. As defined by the Treaty on European Union and the Treaty on the Functioning of the European Union, the EU has no competence in defense, and relevant security fields are the sole purview of EU member states. This creates rifts in overall regulatory and policy outcomes, which are often colored by different rationales in approaching civil, security and defense issues and especially the military uses of these systems. However, it is promising that attempts at bridging siloed thinking and imbuing envisioned policy initiatives with degrees of coherence are now strongly supported.

In this regard, several AI-focused civil-military projects merit further scrutiny. Case in point, the Commission's Action Plan on Synergies between Civil, Defence, and Space Industries[51] defines disruptive technologies, including AI, as inducing paradigm shifts in both civil and military domains: "The term 'disruptive technology' refers to a technology inducing a disruption or a paradigm shift, i.e. a radical rather than an incremental change. Development of such a technology is 'high risk, high potential impact', and the concept applies equally to the civil, defence and space sectors."

At the same time, as the European Commission controls various instruments including innovation funds such as the Horizon Europe and DigitalEurope programs, cleavages in this rather rigid division of competences have started to emerge, while efforts of coordination and the movement toward greater coherence go forward even if in incremental fashion.

For example, EU institutions and especially the European Commission have taken important steps to upgrade the bloc's ambitions for AI leadership. The Commission has emerged as a key driver and agenda setter for a more coherent approach to AI industrial and technological policies. Its plan, set out in the White Paper on AI[52] released in February 2020, has been to boost the EU's research and innovation, as well as its technological and industrial capabilities in this key strategic sector. While it specifically excludes a security and defense focus, the white paper is indicative of the EU's goal to build up a solid technological and industrial base for the research and development of AI. The paper suggests that the EU could merge its "technological and industrial strengths with a high-quality digital infrastructure and a regulatory framework," paying close attention to fundamental values. The main building blocks proposed in the white paper are an "ecosystem of excellence" and an "ecosystem of trust."

To achieve an ecosystem of excellence, the European Commission proposes to streamline research, foster collaboration between member states, and increase investment in AI development and deployment. These actions build on the Coordinated Plan on Artificial Intelligence[53] from December 2018 (updated in 2021). To achieve an ecosystem of trust, the European Commission presents options on creating a legal framework that

[48] European Commission (2020a) Proposal on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December. Available from: https://eur-lex.europa.eu/legal-content/en/HIS/?uri=COM:2020:825:FIN.

[49] European Commission (2020b) The Digital Markets Act: ensuring fair and open digital markets, 15 December Available from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

[50] European Commission (2022a) Cyber resilience act – new cybersecurity rules for digital products and ancillary services. Published Initiatives. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

[51] European Commission (2021a) Action Plan on synergies between civil, defence and space industries, 22 February. Available from: https://ec.europa.eu/info/sites/default/files/action_plan_on_synergies_en.pdf.

[52] European Commission (2020f) White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 February. Available from: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[53] European Commission (2021d) Coordinated Plan on Artificial Intelligence 2021 Review. Policies, 21 April. Available from: https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

addresses the risks for fundamental rights and safety. This follows the work of the High-Level Expert Group on Artificial Intelligence set up in June 2018 and the group's Ethics Guidelines for Trustworthy AI; the "trustworthy AI" approach has now materialised in the AI Act.

Importantly, the white paper only mentions cybersecurity twice in the main body of the text and once very curtly in a footnote regarding potential malicious uses. The AI-cybersecurity nexus is mainly and briefly addressed in relation to safety- and product liability–related issues and "issues associated with AI application in critical infrastructures, or malicious uses of AI." When it comes to the concept of safety, the white paper highlights the fact that the use of AI in products and services can engender risks that the EU legislation currently fails to address, including risks liked to cyber threats. The experience of ENISA for assessing the AI threat landscape is also glossed over in one short sentence.

Hence, different priorities and attributes associated with discrete technological and digital domains - cybersecurity and emerging technologies in this instance - are reflected in corresponding fragmentation among proposed policy solutions. For this reason, oftentimes different logics saturate distinct policy initiatives, and interdependencies between sectors are ignored. One such instance is the interdependence between security, cybersecurity in particular, and the safety of systems. And yet such points of functional interdependence between the two fields increasingly emerge and the question for the EU becomes one of connecting the dots.

Different priorities and attributes associated with discrete technological and digital domains - cybersecurity and emerging technologies in this instance - are reflected in corresponding fragmentation among proposed policy solutions.

On the AI-targeting cybersecurity front, an example of this difference between rationales can be illustrated in the examination of currently debated regulatory proposals in the cybersecurity domain and in AI regulation, namely the NIS 2 Directive[54] and the AI Act. The former attempts to clarify conditions for the cybersecurity of entities the operation of which is considered critical for the smooth functioning of the political and socioeconomic system by imposing incidence reporting obligations. These cover a wide range of areas including electricity, banking, transport, digital infrastructure, and public administration. Most sectors falling within the scope of critical infrastructure are potential targets to malicious activity emanating in cyberspace by virtue of their increasing dependence on cyber-physical systems[55] for their continued operations. Such industrial control systems[56] running critical infrastructures increasingly rely on automation for efficient operation,[57] and therefore become part of the expanded AI-relevant vulnerability surface. Yet, no reference to AI-backed systems or relevant provisions exists in the draft proposal of the European Commission.

The draft AI Act makes explicit reference to critical infrastructure systems as well as systems deployed in the administration of justice and in democratic processes, including elections. It also makes repeated references to the cybersecurity of products at high risk from malicious activity including data poisoning or adversarial attacks, with references usually grouped together with requirements for accuracy and robustness. The act places responsibility for the fulfillment of such requirements - upon which the safety of deployed products is contingent - on manufacturers as well as those placing systems on the market. While the text lacks explicit references to

[54] European Commission (2020e) Proposal for directive on measures for high common level of cybersecurity across the Union. Policy and Legislation, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[55] ENISA (2022) IoT and Smart Infrastructures. Available from: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot?tab=details.

[56] ENISA (2017) Communication network dependencies for ICS/SCADA Systems. Publications, 1 February. Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies.

[57] Siemens (2022) Artificial intelligence in industry: intelligent production. Available from: https://new.siemens.com/global/en/company/stories/industry/ai-in-industries.html.

cybersecurity-by-design considerations, it does clarify that products complying with EU cybersecurity processes, as delineated under the Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification of 2019 (Cybersecurity Act),[58] may be considered to fulfill requirements under the AI Act.

Overall, the NIS 2 includes no provisions for the cybersecurity of AI systems deployed for the functioning of critical infrastructures, despite the fact that the cybersecurity requirements of these systems are distinct from conventional cybersecurity operations due to the different nature of threats facing said systems. However, the AI Act draws some connections between safety failures and the permanent danger of cyberattacks.[59] Therefore, via conjecture we can discern that the AI Act would confer a degree of cyber protection in the event of cyberattacks on AI-dependent large-scale systems. In this sense, the AI Act seems to move a step further in the direction of cyber protecting AI systems. Liability for cybersecurity operates primarily ex ante, although provisions for post-market monitoring and reporting on "any serious incident or any malfunctioning"[60] are included in the proposal. Yet it remains unclear where responsibility for response to and recovery from such potentialities - especially those generated by malicious activity - lies between private vendors and public authorities at the national or EU level.

Operational Capabilities and Structures

The EU has also embarked on a process to shape the development of a European cybersecurity ecosystem, as indicated by the recent proliferation of institutional structures and processes. The latest members of the EU institutional family in the cyber field - the newly established European Cybersecurity Industrial, Technology, and Research Competence Centre and the Network of National Coordination Centres[61] (or Competence Centre and Network), and the Commission-proposed JCU - all include to some extent the research or use of AI-supported capabilities.

The regulation establishing the Competence Centre acknowledges that "the Union still lacks sufficient technological and industrial capacities and capabilities to autonomously make its economy and critical infrastructures secure and become a global leader in the area of cybersecurity." Notably, and beyond highlighting the need for further strategic autonomy in cyber-related domains, the center identified the insufficient level of strategic and sustainable coordination and cooperation between various stakeholders, including industries, cybersecurity research communities, and governments. For this reason, the center sets out to become the EU's "main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives."

Among other coordination tasks, the center will make strategic investment[62] decisions and pool resources from the EU, its member states and, indirectly, industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. This includes supporting projects by

---

[58] European Union (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 17 April. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881.

[59] Imbrie, Andrew and Elsa Kania (2019) AI Safety, Security, and Stability Among Great Powers: Options, Challenges, and Lessons Learned for Pragmatic Engagement. Publications, Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/publication/ai-safety-security-and-stability-among-great-powers-options-challenges-and-lessons-learned-for-pragmatic-engagement/.

[60] European Commission (2021c) Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 21 April. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[61] European Cybersecurity Competence Centre and Network (ECCC) (2022) The European Cybersecurity Competence Centre, Home. Available from: https://cybersecurity-centre.europa.eu/index_en.

[62] European Commission (2018) European Cybersecurity Competence Network and Centre. Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

implementing the cybersecurity parts of Horizon Europe, the Digital Europe Program, and other EU funds, and establishing strategic recommendations for research, innovation, and deployment in cybersecurity.

The center is accompanied by the Network of National Coordination Centres, tasked with supporting the cybersecurity community at the national level and managing portions of available funding under certain conditions. What is interesting is that the setup of the Competence Centre and Network follows the development of four innovative EU-funded pilot projects[63] aiming to tackle different facets of coordination problems among cybersecurity communities such as the private sector, small and medium-sized enterprises, research, and academia.

For example, while CyberSec4Europe[64] experiments with novel governance structures, its fellow project SPARTA[65] works on developing capabilities within the AI-cybersecurity nexus, and in particular capabilities such as autonomous self-protected systems. Given the privileged position of relevant projects in designing and implementing the Competence Centre and Network, more attention could be devoted to mainstreaming AI as well as other EDTs in EU cybersecurity research and innovation efforts.

One further capability worth noting is found in the 2021 Commission Recommendation[66] - followed by the Council's tacit approval[67] - for establishing the JCU[68] to coordinate all existing EU cybersecurity agencies and EU-level capabilities, in order to support potential responses to cyber incidents. Indeed, the following list of the entities the recommended structure[69] seeks to coordinate is impressive, further showcasing the highly fragmented AI-cybersecurity ecosystem across the EU and the urgent need to connect the dots:

> This existing architecture includes, on the operational side, the Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises (the Blueprint), the CSIRTs network and the European Cyber Crises Liaison Organisation (EU CyCLONe) network, as well as the European Cybercrime Centre (EC3) and the Joint Cybercrime Taskforce (J-CAT) at the European Union Agency for Law Enforcement Cooperation (Europol), and the EU Law Enforcement Emergency Response Protocol (EU LE ERP). The NIS Cooperation Group, the EU Intelligence and Situation Centre (EU INTCEN), and the Cyber Diplomacy Toolbox and cyber defence-related projects launched under the Permanent Structured Cooperation (PESCO) also contribute to policy and operational cooperation in different cybersecurity communities. The European Agency for Cybersecurity (ENISA), by virtue of its reinforced mandate, is tasked with supporting operational cooperation with regard to the cybersecurity of network and information systems, the users of such systems, and other persons affected by cyber threats and incidents.

Accordingly, the extent of information and intelligence accumulated but not efficiently shared across entities has for a long time troubled EU entities and officials, and it is this gap in intra-EU information-sharing that the JCU would help mitigate. Among other things, the recommendation seeks to establish the previously-mentioned network of SOCs in order to facilitate information exchange across this vast stakeholder ecosystem: "contributing to the Joint Cyber Unit should enable participants to strengthen existing networks, such as the CSIRTs Network and EU CyCLONe, providing them with secure information exchange tools and better detection

---

[63] European Cyber Competence Network (2019) Four EU pilot projects prepare the way for the European Cybersecurity Centre and Competence Network. About. Available from: https://cybercompetencenetwork.eu/about/.

[64] Cybersecurity for Europe (2022) Our Community. About. Available from: https://cybersec4europe.eu/our-community/.

[65] SPARTA (2022). Available from: https://www.sparta.eu/.

[66] European Commission (2021g) EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents, Press Release, 23 June. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088.

[67] Council of the European Union (2021) Cybersecurity: Council adopts conclusions on exploring the potential of a joint cyber unit. Press Release, 19 October. Available from: https://www.consilium.europa.eu/en/press/press-releases/2021/10/19/cybersecurity-council-adopts-conclusions-on-exploring-the-potential-of-a-joint-cyber-unit/.

[68] European Commission (2021g) Commission Recommendation on Building a Joint Cyber Unit. Policies, 23 June. Available from: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit.

[69] See above. Also available from: https://www.stradalex.com/en/sl_src_publ_leg_eur_jo/toc/leg_eur_jo_3_20210705_237/doc/ojeu_2021.237.01.0001.01.

capabilities (i.e. Security Operation Centres, 'SOCs') and allowing them to tap into available EU operational capabilities."

The text also describes the creation of "a virtual platform composed of collaboration and secure information sharing tools." Those tools will leverage the wealth of information gathered through the European Cyber Shield, including SOCs and Information Sharing and Analysis Centres (ISACs). It is through this envisaged network of SOCs and ISACs that the EU seeks to tap into the latest advances of AI use for anomaly and threat detection and embed these tools into EU-level capabilities developed in the future.

Conclusion

The EU is pursuing the twin goals of establishing a robust cybersecurity architecture across the bloc and harnessing the benefits of AI for broader societal and economic (cyber) security and defence purposes. Yet, if the goal is to ensure the cybersecure rollout of AI systems and services, and that both the dimensions of AI for cybersecurity and cybersecure AI feature prominently on the EU's policy and operational agendas, connecting the dots between various initiatives, processes, and stakeholders is paramount. A holistic view on the AI-cybersecurity nexus is required.

This can be achieved via new cross-institutional and strategic thinking to pave the way for concrete actions in the AI-cybersecurity nexus, particularly in terms of better understanding and mitigating the risks of progressively using AI systems and services in key domains like healthcare, transportation, critical infrastructures, security, and defense. It is imperative to strengthen the cybersecurity of AI and preserve accountability across intelligent systems. Also, as AI-powered cyberattacks are increasingly on the rise, the EU and its member states, in partnership with the private sector, need to be ready to respond to the growing range of AI-driven cybersecurity risks and threats, as well as possess the capabilities and expertise required to mitigate such challenges.

References

Castelvecchi, Davide (2016) Can we open the black box of AI?. Nature News 538(7623): 20. Available from: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731.

Council of the European Union (2021) Cybersecurity: Council adopts conclusions on exploring the potential of a joint cyber unit. Press Release, 19 October. Available from: https://www.consilium.europa.eu/en/press/press-releases/2021/10/19/cybersecurity-council-adopts-conclusions-on-exploring-the-potential-of-a-joint-cyber-unit/.

Council of the European Union (2022a) Council conclusions on the Development of the European Union's Cyber Posture, 23 May. Available from: https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

Council of the European Union (2022b) Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, 10 May. Available from: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

Crafts, Nicholas (2021) Artificial intelligence as a general-purpose technology: an historical perspective, Oxford Review of Economic Policy, 37(3): 521–536. Available from: https://academic.oup.com/oxrep/article/37/3/521/6374675?login=true.

Csernatoni, Raluca (2021) The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty. Carnegie Europe Program. Available from: https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.

CSET (2022) Publications. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/publications/?fwp_topic=cyberai.

Cyber Risk GmbH (2022) Pillar 2: Secure - Strategic Compass of the European Union, Available from: https://www.strategic-compass-european-union.com/2_Secure_Strategic_Compass.html#:~:text=In%202022%2C%20we%20will%20further,Joint%20Cyber%20Unit%20will%20continue.&text=By%20the%20end%20of%202023,Strategy%20for%20security%20and%20defence.

Cybersecurity for Europe (2022) Our Community. About. Available from: https://cybersec4europe.eu/our-community/.

DARPA (2022) AI Next Campaign. Defense Advanced Research Projects Agency (DARPA). Available from: https://www.darpa.mil/work-with-us/ai-next-campaign.

ENISA (2017) Communication network dependencies for ICS/SCADA Systems. Publications, 1 February. Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies.

ENISA (2020) Artificial Intelligence Cybersecurity Challenges, 15 December. Available from: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

ENISA (2022) IoT and Smart Infrastructures. Available from: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot?tab=details.

European Commission (2018) European Cybersecurity Competence Network and Centre. Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

European Commission (2020a) Proposal on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December. Available from: https://eur-lex.europa.eu/legal-content/en/HIS/?uri=COM:2020:825:FIN.

European Commission (2020b) The Digital Markets Act: ensuring fair and open digital markets, 15 December Available from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

European Commission (2020c) Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Commission (2020d) New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Press Release, 16 December. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

European Commission (2020e) Proposal for directive on measures for high common level of cybersecurity across the Union. Policy and Legislation, 16 December. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

European Commission (2020f) White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 February. Available from: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission (2021a) Action Plan on synergies between civil, defence and space industries, 22 February. Available from: https://ec.europa.eu/info/sites/default/files/action_plan_on_synergies_en.pdf.

European Commission (2021b) Proposal for a Regulation laying down harmonised rules on artificial intelligence, 21 April. Available from: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

European Commission (2021c) Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 21 April. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission (2021d) Coordinated Plan on Artificial Intelligence 2021 Review. Policies, 21 April. Available from: https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

European Commission (2021e) Joint Cyber Unit. Policies. Available from: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit.

European Commission (2021f) Commission Recommendation on Building a Joint Cyber Unit. Policies, 23 June. Available from: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit.

European Commission (2021g) EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents, Press Release, 23 June. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088.

European Commission (2022a) Cyber resilience act – new cybersecurity rules for digital products and ancillary services. Published Initiatives. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

European Commission (2022b) Data Act: Commission proposes measures for a fair and innovative data economy. Press Release, 23 February. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

European Cyber Competence Network (2019) Four EU pilot projects prepare the way for the European Cybersecurity Centre and Competence Network. About. Available from: https://cybercompetencenetwork.eu/about/.

European Cybersecurity Competence Centre and Network (ECCC) (ND) The European Cybersecurity Competence Centre, Home. Available from: https://cybersecurity-centre.europa.eu/index_en.

European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, July 6. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148.

European Union (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 17 April. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881.

European Union External Action Service (EEAS) (2022) A Strategic Compass for Security and Defence. European Union External Action Service (EEAS), 23 March. Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

Fraze, Dustin (2016) Cyber Grand Challenge (CGC). Defense Advanced Research Projects Agency (DARPA). Available from: https://www.darpa.mil/program/cyber-grand-challenge.

Heinl, Caitríona H. (2014) Artificial (intelligent) agents and active cyber defence: Policy implications. 6th International Conference On Cyber Conflict (CyCon 2014) 53-66. 3 June. Available from: https://ieeexplore.ieee.org/abstract/document/6916395/authors#authors.

Heinl, Caitriona, et al. (2022) Is War in Ukraine the End of Cyber Diplomacy. Directions, 18 March. Available from: https://directionsblog.eu/is-war-in-ukraine-the-end-of-cyber-diplomacy/.

Helmus, Todd C. (2022) Artificial Intelligence, Deepfakes, and Disinformation: A Primer. Santa Monica, CA: Rand Corporation. Available from: https://www.rand.org/pubs/perspectives/PEA1043-1.html.

Hoffman, Wyatt (2021) AI and the Future of Cyber Competition. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/publication/ai-and-the-future-of-cyber-competition/.

Horowitz, Michael (2020) AI and the Diffusion of Global Power. In Modern Conflict and Artificial Intelligence. A CIGI essay series. Centre for International Governance Innovation (CIGI). Available from: https://www.cigionline.org/sites/default/files/documents/Modern%20Conflict%20and%20AI_web.pdf#page=36.

IBM (2022) Artificial intelligence (AI) for cybersecurity. IMB Solutions. Available from: https://www.ibm.com/security/artificial-intelligence.

Imbrie, Andrew and Elsa Kania (2019) AI Safety, Security, and Stability Among Great Powers: Options, Challenges, and Lessons Learned for Pragmatic Engagement. Publications, Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from:

https://cset.georgetown.edu/publication/ai-safety-security-and-stability-among-great-powers-options-challenges-and-lessons-learned-for-pragmatic-engagement/.

Johnson, James (2019) The AI-cyber nexus: implications for military escalation, deterrence and strategic stability. Journal of Cyber Policy, 4(3): 442-460. Available from: https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1701693.

Kaminska, Monica, and James Shires, and Max Smeets (2022) Cyber operations during the 2022 Russian invasion of Ukraine: Lessons learned (so far). ECCRI Tallin Workshop Report, European Cyber Conflict Research Initiative, July 2022. Available from https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.

Kangas, Santeri (2022) Why AI is the key to cutting-edge cybersecurity. World Economic Forum, 21 July. Available from: https://www.weforum.org/agenda/2022/07/why-ai-is-the-key-to-cutting-edge-cybersecurity/.

Knight, Will (2022) DALL-E Mini Is the Internet's Favorite AI Meme Machine. WIRED, 27 June. Available from: https://www.wired.com/story/dalle-ai-meme-machine/.

Korolov, Maria (2022) Top Three Use Cases for AI in Cybersecurity. Data Centre Knowledge, 3 February. Available from: https://www.datacenterknowledge.com/security/top-three-use-cases-ai-cybersecurity.

Li, Jian-hua (2018) Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering 19(12):1462-1474. Available from: https://link.springer.com/article/10.1631/FITEE.1800573.

Lohn, Andrew (2022) Testimony before the Senate Armed Services Subcommittee on Cybersecurity. Center for Security and Emerging Technology (CSET): Washington, DC, USA, 3 May. Available from: https://cset.georgetown.edu/publication/andrew-lohns-testimony-before-the-senate-armed-services-subcommittee-on-cybersecurity/.

Lohn, Andrew and Wyatt Hoffman (2022) Securing AI How Traditional Vulnerability Disclosure Must Adapt. Center for Security and Emerging Technology (CSET): Washington, DC, USA.. Available from: https://cset.georgetown.edu/publication/securing-ai-how-traditional-vulnerability-disclosure-must-adapt/.

Microsoft (2021) Microsoft Digital Defense Report. Available from: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report.

Muser, Micah and Ashton Carriott (2021) Machine Learning and Cybersecurity - Hype and Reality. Center for Security and Emerging Technology (CSET): Washington, DC, USA. Available from: https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf.

Pillsbury & The Economist Intelligence Unit (2021) AI & Cybersecurity: Balancing Innovation, Execution & Risk, 9 September. Available from: https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html.

Prucková, Michaela (2021) New EU's cybersecurity package: ambitious proposals, daring tasks and deeper cooperation. CCDCOE. Available from: https://ccdcoe.org/library/publications/new-eus-cybersecurity-package-ambitious-proposals-daring-tasks-and-deeper-cooperation/.

Schäfer, Matthias (2018). The fourth industrial revolution: How the EU can lead it. European View, 17(1): 5-12. Available from: https://www.martenscentre.eu/wp-content/uploads/2020/10/17816858187768125-1.pdf.

Siemens (2022) Artificial intelligence in industry: intelligent production. Available from: https://new.siemens.com/global/en/company/stories/industry/ai-in-industries.html.

SPARTA (2022). Available from: https://www.sparta.eu/.

The New York Times (2022) Facial Recognition Goes to War. Available from: https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html.

Vectra (2022) As the War in Ukraine Spirals, Vectra AI Announces Free Cybersecurity Services. Available from: https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services.

Whyte, Christopher (2020) Poison, Persistence, and Cascade Effects. Strategic Studies Quarterly, 14(4): 18-46. Available from: https://www.jstor.org/stable/26956151#metadata_info_tab_contents.

Whyte, Christopher (2022) Machine Expertise in the Loop: Artificial Intelligence Decision-Making Inputs and Cyber Conflict. In 2022 14th International Conference on Cyber Conflict: Keep Moving! 700: 135-154. Available from: https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf.

About the authors

Raluca Csernatoni is Visiting Scholar at Carnegie Europe in Brussels, where she leads the European security and defence, as well as the emerging and disruptive technologies workstreams. She is also Guest Professor at the Centre for Security, Diplomacy and Strategy of Vrije Universiteit Brussel, her research exploring topics at the intersection of International Relations and Science and Technology Studies. Her newest co-edited book, Emerging Security Technologies and EU Governance: Actors, Practices and Processes, was published with the Routledge Studies in Conflict, Security and Technology (2020).

Katerina Mavrona is a policy analyst focusing on EU digital policies, cybersecurity, and the governance of emerging technologies.

About EU Cyber Direct – EU Cyber Diplomacy Initiative

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

New Tech in Review is a collection of commentaries, highlighting key issues at the intersection of emerging technologies, (cyber)security, defence, and norms.

IMPLEMENTING ORGANISATIONS

euiss European Union Institute for Security Studies

Universiteit Leiden Institute of Security and Global Affairs

CARNEGIE EUROPE

FUNDED BY THE EUROPEAN UNION