
## About the Article

Main Question: How can AI be used safely in NATO and EU cyber operations? Argument: AI boosts cyber defence but needs oversight, security, and coordination. Conclusion: Combining AI with regulation and collaboration strengthens defence and accountability

## About the Author

**João Pedro Souza Gohla** is a Master's student in Law and Security at NOVA School of Law in Lisbon. He holds a Bachelor's degree in Political Science with a focus on International Relations and History from Goethe University Frankfurt. His current research examines security policy, migration, and state fragility within contemporary global governance frameworks.

## 1. Introduction

Artificial intelligence (AI) has transitioned from an emerging technology in the cyber realm to an omnipresent aspect of operational reality. Its ability to analyse large datasets, identify anomalies instantly, and even automate specific decision-making tasks presents unparalleled chances for enhancing cyber defence. However, the same abilities that render AI beneficial also introduce new dangers, especially when used in delicate military situations. These dangers are heightened in cyberspace, where activities can occur rapidly, transcending borders, and often lacking immediate identification. For NATO and the European Union (EU), cyber capabilities enhanced by AI present a twofold challenge. On one side, they can greatly improve group resilience against advanced cyber threats. While, simultaneously posing intricate legal, ethical, and political dilemmas concerning autonomy, accountability, and control. In contrast to traditional weapon systems, AI employed in cyber operations is typically hidden from public view and can be used secretly, complicating oversight efforts. At present, NATO does not carry out offensive cyber operations these are solely the responsibility of individual member nations. These abilities are regarded as „national resources" that can be utilized for alliance operations on a voluntary basis (Shape n.d.). Although this setup honours national sovereignty, it leads to coordination issues. Sensitive data regarding the extent, techniques, and preparedness of national assets is frequently kept under strict control, hindering NATO's capacity to organize and execute genuinely coordinated cyber operations. This issue of „secrecy" can obstruct trust and delay decision-making in times of crisis. The EU encounters a distinct structural situation. It lacks a military command structure similar to NATO but wields significant influence via its regulatory capabilities, research financing, and coordination tools such as the EU Agency for Cybersecurity (ENISA). EU cybersecurity efforts typically emphasize standardization, strengthening resilience, and enhancing capabilities, which can support NATO's operational functions (Trimintzios et al., 2017). Nevertheless, the absence of a direct operational mandate implies that EU-level actions must depend on the implementation by member states. Considering these variations, the subsequent suggestions aim to enhance AI-driven cyber defence at the national, NATO, and EU tiers. Every suggestion tackles both operational and governance aspects, guaranteeing that technological progress is accompanied by strong policy structures.

## 2. Clarify NATO's Role and Capabilities in Cyber Operations

***Why it matters:***

NATO's existing cyber defence strategy is based on the idea that member nations maintain authority over offensive abilities (Shea, 2025). Though politically essential, this setup may hinder prompt collective reactions to rapidly evolving cyber threats especially those driven by AI. In situations where an opponent launches AI-based assaults on several NATO nations at the same time, lags in the coordination of national resources may enable the attacks to intensify without restraint. The categorization of national capabilities introduces an additional layer of complexity alliance planners might remain unaware of available tools until a crisis arises.

***Recommendation:***

NATO ought to expand the mandate of its Cyber Operations Centre to strengthen the operational integration of AI-driven tools, while still maintaining national authority over their usage. This may require. The creation of a protected, classified database of AI-driven cyber capabilities possessed by member countries, available solely to approved NATO strategists. Establishing interoperability standards for AI technologies, guaranteeing that national systems operate cohesively during collaborative missions. Developing pre-approved operational playbooks for specific types of cyber defence measures, minimizing the necessity for prolonged political discussions in critical situations.

***Supporting platform:***

The NATO Cyber Operations Centre provides a central hub for alliance cyber activities, while the CCDCOE supports joint exercises and training (NATO CCDCOE, 2023). These institutions could serve as the operational and conceptual anchors for AI integration.

## 3. Develop International Rules for AI in Cyber Warfare

***Why it matters:***

Artificial intelligence in cyber warfare presents distinct regulatory issues. In contrast to kinetic weapons, AI cyber tools can be created and utilized with minimal physical infrastructure, making them more challenging to oversee within current arms control systems (Dykstra, Inglis, & Walcott, 2020, p. 116-118). The lack of global regulations leads to a strategic void where nations might feel compelled to create and implement offensive AI technologies proactively.

***Recommendation:***

Engage with multilateral platforms such as the United Nations Group of Governmental Experts (UN GGE), NATO, the EU, and the G7 to develop practical, enforceable standards for AI applications in military cyber activities. These must, outline banned applications of AI, especially fully autonomous offensive cyber tools that can operate independently without human supervision. Set up essential transparency standards, including mechanisms for reporting before and after operations. Steer clear of impractical universal bans that might unfairly impact liberal democracies, prioritizing practical protections instead.

***Supporting example:***

The Tallinn Manual 2.0 (Schmitt, 2017) offers a general starting point but is a non binding resource for legal advisers and policy experts dealing with cyber issues. Updating this framework to include AI-specific scenarios would bridge a critical gap (NATO Cooperative Cyber Defence Centre of Excellence, n.d.).

## 4. Require Human Oversight and Explain ability in Military AI

***Why it matters:***

Lack of transparency in AI decision-making poses a major risk for governance. In military cyber operations, where immediate decisions can have significant strategic impacts, the lack of clarity in an AI system's actions diminishes both operational trust and democratic responsibility. This is especially pronounced in the EU, where the regulatory environment highlights transparency and rights safeguards, and in NATO, where political agreement necessitates that member countries have confidence in each other's systems

***Recommendation:***

Enforce legal and policy standards that require AI utilized in cyber defence to be understandable to operators and policymakers. Creates a record of choices and measures implemented. Is subject to significant human supervision at critical decision moments. NATO might integrate these demands into its procurement criteria for shared initiatives, and the EU could broaden the reach of the Artificial Intelligence Act to specifically include military AI, ensuring uniform oversight processes among member states (European Commission, 2021).

**Artificial Intelligence (AI):**
**Machines performing tasks that normally require human intelligence**

***Supporting model:***

The European Union's Artificial Intelligence Act (AI Act) explicitly excludes applications used solely for military, defence, or national security purposes, as set out in Article 2(3) and Recital 12. In the civilian sphere, however, the Act establishes stringent requirements for high-risk systems, including those that process biometric data. Extending comparable oversight mechanisms to military AI could help bring defence technologies into line with established civilian standards. Alongside this, the European Parliament has adopted policy resolutions encouraging the development of AI-driven cyber defence capabilities, encompassing both defensive and offensive measures

provided they comply with international law. These initiatives, however, remain political guidance rather than binding provisions of the Act itself (European Parliament, 2022; European Parliament, 2023; Sierra-Tango, 2023).

## 5. Build AI Tools That Are Secure by Design

***Why it matters:***

AI systems are naturally susceptible to threats like adversarial inputs, data poisoning, and model inversion (Federal Office for Information Security, 2023, p.5-11). Within a NATO framework, a breached AI defence mechanism might generate weaknesses among various member nations if interoperability functions are misused. In the EU, insecure AI solutions created in the private sector might be incorporated into defence supply chains, bringing systemic risks.

**AI enhances cyber defence but requires strict human oversight to prevent misuse**

***Recommendation:***

Implement secure-by-design principles as a mandatory criterion for all AI systems employed in defence (Cybersecurity and Infrastructure Security Agency, n.d.). This involves, strict adversarial testing throughout development. Incorporating cybersecurity protocols into the AI framework from the beginning. Implementing ongoing surveillance to identify and address emerging risks. Although this might raise upfront expenses, savings over time will be achieved by lowering the necessity for expensive retrofits and minimizing the chances of major failures.

***Supporting example:***

Ukraine's Delta situational awareness system demonstrates the practical importance of secure-by-design architecture in contested settings (Bondar, 2024, p.7-12).

## 6. Promote International AI-Cyber Threat Intelligence Sharing

***Why it matters:***

Cyber threats powered by AI function at machine speed, allowing minimal time for human detection and response. In the absence of real-time intelligence sharing, even the most proficient individual state can become overwhelmed. Intelligence-sharing mechanisms are present in NATO but may be hindered by classification obstacles. The EU has put resources into civilian cyber threat-sharing systems, yet these frequently lack connection to military networks.

***Recommendation:***

Create cohesive, AI-focused threat intelligence networks at NATO and EU levels, connected via secure gateways. They ought to provide not just threat information but also AI-generated analytical results. Utilize standardized taxonomies for AI-driven threats to enhance interoperability. Perform collaborative NATO–EU training drills that replicate AI-assisted assaults on essential infrastructure. As AI-enabled cyber threats move at machine speed, integrated threat-intelligence channels are critical for both NATO and EU cyber resilience. Figure 1 illustrates a conceptual NATO–EU intelligence-sharing network, highlighting how existing military and civilian channels could be linked through AI-driven analytical hubs. This proposed structure aims to reduce classification bottlenecks, standardise threat taxonomies, and enable near real-time data exchange during cyber incidents. This diagram shows military (NATO), civilian (EU), member state, and AI analysis nodes, along with proposed secure gateway links for AI-driven cyber threat intelligence exchange.

## Integrated NATO-EU AI Threat Intelligence Sharing Network

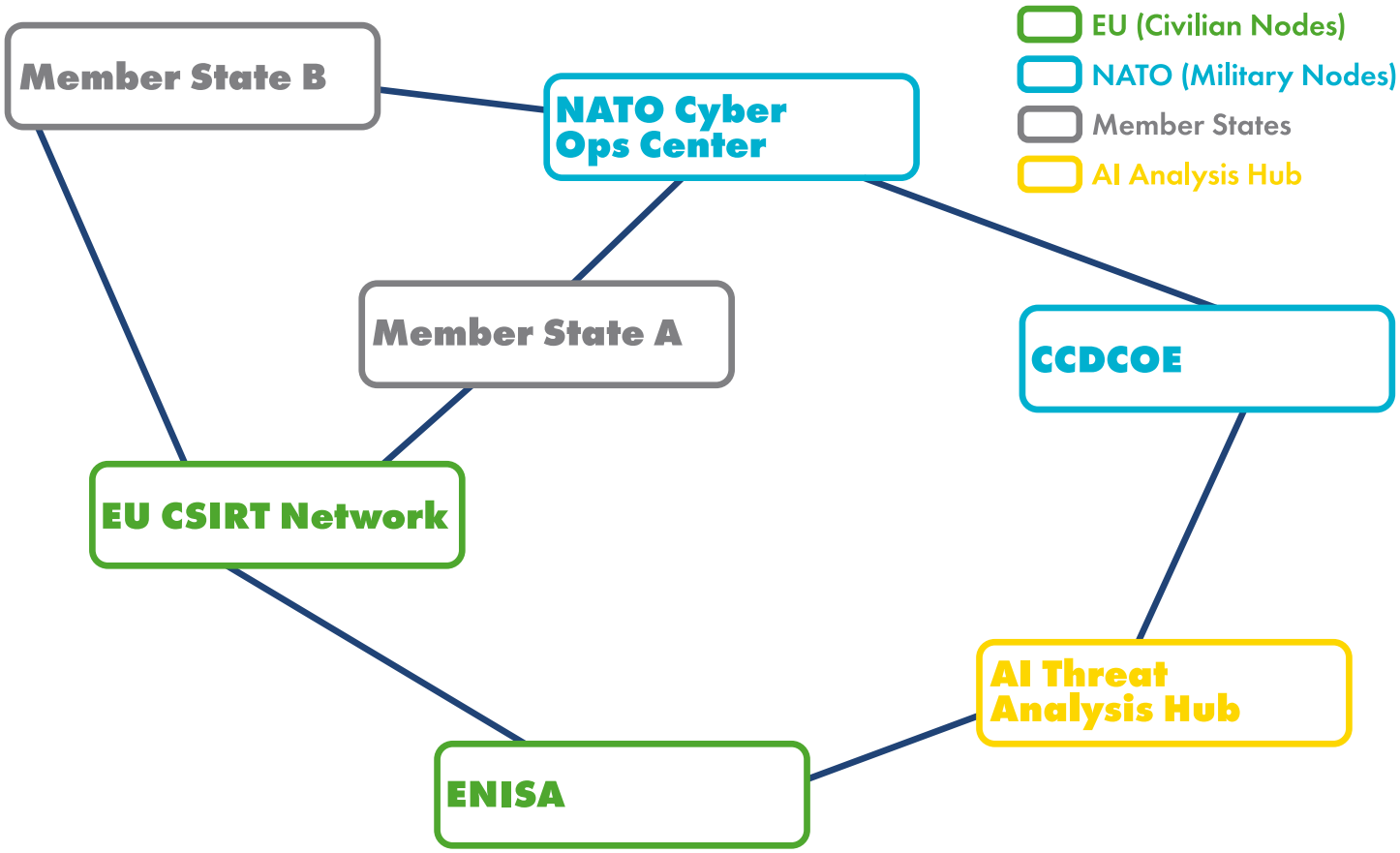


Figure 1. Integrated NATO–EU AI Threat Intelligence Sharing Network.

***Supporting platform:***

The NATO CCDCOE's Locked Shields exercise is a prime venue for testing these capabilities, and the EU's CSIRT Network could serve as the civilian counterpart.

### 7. Close the Skills Gap in AI and Cybersecurity

***Why it matters:***

NATO and the EU both encounter a lack of experts skilled in the convergence of AI, cybersecurity, and defence strategy. Lacking adequate expertise, even the most sophisticated policy frameworks will be ineffective in real-world application. NATO's power is rooted in its operational training framework, whereas the EU possesses more sway in educational policies and research financing.

***Recommendation:***

Initiate collaborative NATO–EU talent programs that create unified curricula addressing AI, cybersecurity, and military uses. Provide shared scholarships and exchange initiatives for professionals from partner countries. Encourage collaboration between public and private sectors to train and keep specialists in the defence industry. Even the most advanced AI-enabled cyber capabilities will falter without a sufficiently trained workforce. The EU currently employs approximately 9.37 million ICT specialists (Eurostat, 2024), but is on track to reach only 12 million by 2030—far below the EU's target of 20 million. Figure 2 visualises this projected shortfall, illustrating the urgent need for joint NATO–EU talent development programmes. Data source: Eurostat (2024) and European Commission (2023). The EU faces an estimated shortfall of approximately 8 million ICT specialists by 2030, underscoring the urgency of coordinated training and recruitment initiatives.

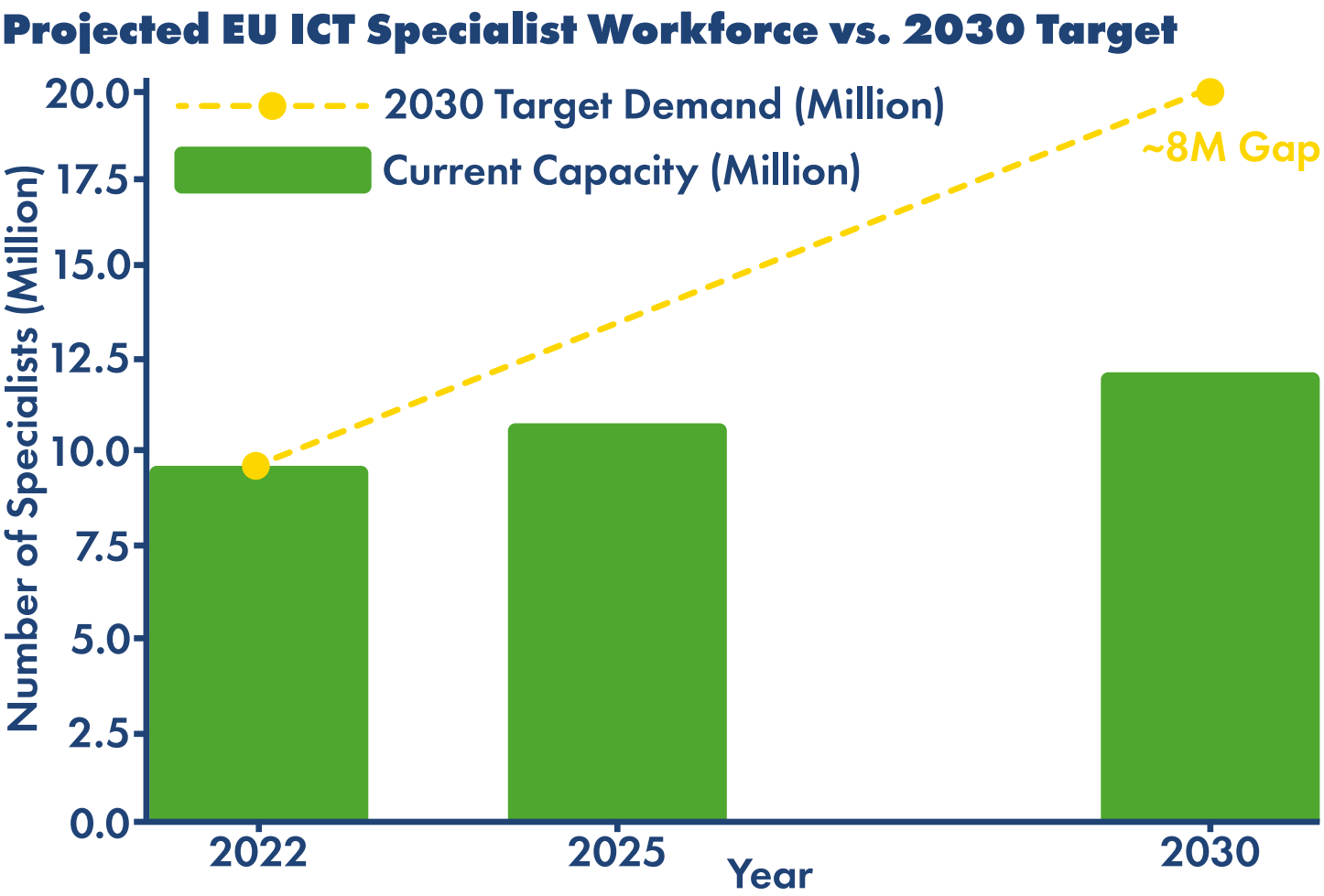


Figure 2. Projected EU ICT Specialist Workforce vs. 2030 Target.

***Supporting example:***

India's post-crisis investment in AI-cybersecurity training offers a model that could be scaled for multinational application (Bharadwaj, 2025).

## 8. Regulate Offensive AI Use with Political Oversight

***Why it matters:***

Offensive AI in cyber warfare represents a highly sensitive political aspect of military technology policy. In NATO, where consensus is essential for decision-making, any ambiguity regarding the use of offensive AI may lead to tension among member states. Within the EU, the lack of a direct military mandate does not eliminate the ability to exert influence especially via export regulations, procurement policies, and industrial strategies.

***Recommendation:***

At the national level, establish explicit criteria for parliamentary or legislative consent prior to utilizing offensive AI in cyber operations. At the NATO level, establish common definitions and political oversight processes that promote transparency among allies while maintaining operational security. At the EU level, create export regulations for offensive AI systems, in line with wider international standards.

***Supporting framework:***

NATO's Responsible AI principles already emphasise accountability and chain of command these could be formalised into binding political oversight structures (NATO Innovation Hub, 2021).

## 9. Conclusion

The incorporation of AI into military cyber operations presents significant strategic benefits as well as serious governance issues. For NATO, the main focus is operational integration making sure that national assets can be aligned swiftly and efficiently without compromising sovereignty. For the EU, the main focus is on regulatory consistency establishing elevated benchmarks for transparency, security, and accountability that member nations and industries are required to uphold. NATO and the EU can enhance their collective defence strategy and maintain the democratic values they aim to safeguard by defining roles, establishing practical global standards, ensuring human oversight, integrating security into AI technologies, exchanging threat intelligence, addressing the skills gap, and regulating offensive AI with political supervision.

## References


Bondar, K. (2024). Understanding the military AI ecosystem of Ukraine. https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

Cybersecurity and Infrastructure Security Agency. (n.d.). Secure by design. CISA. Retrieved August 19, 2025, from https://www.cisa.gov/securebydesign

Dykstra, J., Inglis, C., & Walcott, T. S. (2020). Differentiating kinetic and cyber weapons. Joint Force Quarterly, 99, 116–123. National Defense University Press.

European Commission. (2021). Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

European Parliament. (2022). Artificial intelligence in a digital age [Resolution 2022/2040(INI)]. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52022IP0140

European Parliament. (2023). European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

Eurostat. (2024). ICT specialists—statistics on hard-to-fill vacancies in enterprises. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=679049

Federal Office for Information Security. (2023). AI security concerns in a nutshell: Practical AI-Security Guide 2023. BSI. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Practical_AI-Security_Guide_2023.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2023). About CCDCOE. https://ccdcoe.org/about-us/

NATO Innovation Hub. (2021). Responsible AI in the military: A framework. https://innovationhub-act.org

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Shea, J. (2025). Non-traditional security threats. In J. Sperling & M. Webber (Eds.), The Oxford handbook of NATO (Oxford Handbooks). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198851196.013.29

Sierra-Tango. (2023). AI Act: What impact for defence? https://sierra-tango.eu/en/ai-act-what-impact-for-defence/

Supreme Headquarters Allied Powers Europe. (n.d.). Cyber defence. NATO. Retrieved August 15, 2025, from https://shape.nato.int/about/aco-capabilities2/cyber-defence

Bharadwaj, S. (2025, May 25). How pro-India hackers defended country during cross-border cyberattacks amid Op Sindoor. The Times of India. https://timesofindia.indiatimes.com/city/hyderabad/how-pro-india-hackers-defended-country-during-cross-border-cyberattacks-amid-op-sindoor/articleshow/121385229.cms

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU (STOA Study PE 603.175). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

United Nations Group of Governmental Experts (UN GGE). (2021). Reports on responsible state behavior in cyberspace.
World Economic Forum. (2024). Strategic Cybersecurity Talent Framework. Retrieved from https://www.weforum.org/publications/strategic-cybersecurity-talent-framework