INFO FLASH
Finabel
The European Land Force Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

OCTOBER 2024

WRITTEN BY
MANUEL DIAS

EDITED BY
DIMITRA PATERAKI

SUPERVISED BY
BELÉN PADRÓN SALINAS

Introduction

“The number of hacktivist attacks (against) European infrastructure, threat actors whose main aim is to cause disruption, has doubled from the fourth quarter of 2023 to the first quarter of 2024,” (AP, 2024) - Juhan Lepassaar, head of the European Union Agency for Cybersecurity (ENISA)

The current military context, more aptly viewed as a hybrid environment, has inherently changed the framework of military conduct. The previous multi-domain environment of undersea, surface, land, air and space is now further interlinked by the 6th domain: cyber (Vice Admiral Connor, 2019). The more defence equipment depends on digital software and IoT structures, the more their cyber vulnerabilities increase too. Modern stealth fighters, UAVs, sensor networks, data centres as well as Europe’s very own command and control centres are just some examples of military technologies that are, to a great extent, vulnerable to cyberattacks. Additionally, critical infrastructures such as hospitals, banks, common transportation and communication systems all rely heavily on various digital structures that are inevitably largely susceptible to cyber-attacks. In this sense, these public structures are even more vulnerable because the defence mechanisms are often less complex than those in the military sphere. Consequently, the need for a European platform that can adapt to these growing threats becomes irrefutable.

On January 26, 2024, the European Defence Fund launched a new cyber project with the acronym FACT, which stands for Federated Advanced Cyber Physical Test Range. This date marked the inaugural kick-off meeting in Oslo under the leadership of Norwegian military contractor Kongsberg Defence & Aerospace (Kongsberg Defence & Aerospace, 2024). In total, 15 European countries are involved along with their military contractors and entities, amounting to a total of 19 (European Union, 2022, European Defence Fund), which will take over the practical integration of the project. The goal, according to Kongsberg, is to “pave the way for the EU's autonomy and ability to create and integrate a federated cyber-physical test bed” or “a common toolbox for cyber-physical testing with a common architecture and environment” (Kongsberg Defence & Aerospace, 2024).

In recent attempts to integrate European defence, one of the common challenges has been the discrepancies in military technology and strategic complexity across EU countries (Bergmann et al., 2022). This is why the coordinating role of the respective military contractors in the FACT consortium is so relevant since- it inherently implies the transparent sharing of cutting-edge military technology. Beyond informing cyber strategy, FACT can shed light on each EU member state’s strengths and weaknesses in the cyber domain and how they can create a joint cyber framework that enables a mutualist symbiosis that improves

collective long-term cyber-resilience and adaptability independent from NATO infrastructures. To address these issues, this article will look at the current FACT consortium structure and what potential barriers exist, including its current member participation. Secondly, it will explore the basic concept of a cyber range and its pertinence in the current context of foreign adversarial cyber capabilities. Additionally, a summary of FACT's concept of operations will be presented. To conclude, the importance of future European cyber autonomy and resilience will be analysed taking into account lessons learned as well as the potential for a renewed EU cyber framework. If anything, FACT promises to be the first step in the right direction.

I. FACT Consortium

The FACT consortium comprises 15 EU member countries and 19 respective military contractors or entities (European Commission, 2023). With a grant of about 26.9 € million over a three-year period by the European Defence Fund (EDF), the project is set to last from December 2023 to November 2026. Additionally, it is commensurate with the PESCO project "Cyber Threats and Incident Response Information Sharing Platform" (CTIRISP) and the European Defence Industrial Development Programme (EDIDP) project "PANDORA" (EDIDP, 2022).

However, the total amount provided by the EU Defence Fund will not cover the total expected amount of the project, which ranges around € 29,687,302.49 as per EU estimates (European Union, 2022, European Defence Fund). Out of more than 100 different EDF projects, FACT is one of only three currently being coordinated by Norwegian entities (FACT Consortium, 2024) and co-funded by the Norwegian MOD and by Kongsberg D&A. FACT is meant to create the conditions for the shared testing of cyber-vulnerability of European military equipment, a critical capability to be fostered in the current context of hybrid warfare.

The project will deliver an "unprecedented European capability for cyber-physical testing and verification of equipment", based on the test range itself and a common EU-wide approach (European Commission, 2023).

Below, it is worth enlisting the participating EU members and their respective collaborative subject matter experts (SME's). As follows, Austria is represented by the *Austrian Institute of Technology*, Belgium by *Approach*, Bulgaria by *BIANOR*, Denmark by *Terma*, Estonia by *SIHATSUTUS CR14*, and Finland by *Crosshill*. Additionally, Germany is represented by *Rheinmetall Electronics GMBH*, Greece by *Space Hellas*, Hungary by *Nokia Bell Labs**, Italy by University of Genoa *& LEONARDO*, and Latvia by *Latvijas Mobilais Telefons SIA*. Lastly,

Lithuania is represented by *BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS*, the Netherlands by *Emproof*, Norway by *Kongsberg Defence & Aerospace* and *Thales Norway**, and Romania by *CertSIGN*.

Notably, although the United States and France are not technically involved in the programme, they are passively participating through two military contractors, in particular through Nokia Bell Labs (US) and THALES Norway (France). Why these two countries chose to remain technically isolated from the project but effectively integrated all the same is noteworthy. This question also underscores the challenges of fully integrating European military structures, particularly as France, a leading European military power that advocates for more European collective defence, remains unwilling to fully integrate its own cyber domains in this particular context. At least, not yet.

This passive participation illustrates the difficulty of separating European military structures from US control both in the private and military sectors, where we find a strictly European-based cyber consortium that is still integrating US-owned military contractors. This effective separation will eventually involve an industry-based shift in sourcing military contractors, but ultimately, the political will to detach from US influence. European countries could also be reluctant to fully integrate their cyber domains because this would entail a shared risk should a successful cyber-attack occur, as sensitive information infrastructure hubs would necessarily be connected to allow for joint cyber development in the context of a cyber range. In any case, the FACT consortium shows not only a step in the right direction for European cyber- interoperability but also true hope for authentic collective political willingness moving forward.

II. Cyber Ranges - An Overview

As per the *European Cyber Security Organization*, a cyber range is defined as follows: "A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases" (European Cyber Security Organization, 2020).

Simultaneously a physical platform and a complex simulation environment, cyber ranges test the capabilities and vulnerabilities of cyber-physical systems (CPS) of both the hardware and

software components of a given piece of equipment in simulated environments. Tests are often designed to target offensive attacks on the specific CPS defence structures to determine their key vulnerabilities, where Artificial Intelligence, and particularly its subcomponent machine learning, has become a vital resource for the aggregation and analysis of information (FACT Consortium, 2024).

These tests can also be invaluable sources for understanding and anticipating how an enemy might specifically target military CPSs based on previous cyber modus operandi (MO) and how to best prepare for such attacks. Although classified military matrices will likely be more extensive, specific data matrices on adversarial MOs can be used for this purpose, namely the more commercial MITRE & ATT&CK dataset (European Cyber Security Organization, 2020). In turn, the specific data that is initially fed into the cyber range must be highly pertinent to the given CPS. This will enable both a comprehensive determination of vulnerability but also a more insightful post-test recommendation for enhanced resilience.

Overall, as increasingly more of our military equipment relies in some way, shape or form on structures exposed to cyber threats, the importance of such ranges has grown exponentially. In fact, the rise of complex computer network operations, with new embedded functions like shared cloud and 5G services augments the threat and risk of cyber-attacks (European Cyber Security Organization, 2020).

Foreign Cyber Parity

Considering the current cyber capabilities developed by China, Russia, and Iran, the importance of a platform like FACT becomes evident. In 2010, the Chinese Academy of Sciences established the first Chinese national cyber range, trailing DARPA's national cyber range, created in 2008, by only two years (Cary, 2023). The Chinese government has recently invested considerable resources in developing a renewed national cyber-range initiative that integrates the public (civilians and academia), private (industry and military contractors) and governmental sectors (with particular emphasis on critical infrastructure operators) (Cary, 2023).

This initiative includes annual competitions to emulate NATO's Locked Shields Exercise (an annual cyber- resilience exercise) as well as employing supercomputing power to determine AI's applicability in cyber security (Cary, 2023). Developing this type of intricate relationship between different social sectors will allow for better Chinese interoperability between the civilian, private and governmental sectors in the case of a cyber-attack while at the same time raising collective awareness of the issue nationwide. China's Cyber Advanced Persistent Threat Units (APTs), codenamed "Pandas" (APT 31, for example) have traditionally

demonstrated specific interest in targeting critical urban infrastructure networks (CISA, n.d.). In contrast, Russian APTs, codenamed "Bears" (APT 28, CyberBerkut, Sandworm), FSB (Turla APT), SVR (APT29) are known to employ their varied cyber-portfolio to engage in espionage and seek influence over political elections (Hakkala & Melnychuk, 2021).

Nonetheless, Russia has focused on critical infrastructure and equipment, recently forcing Ukraine to build a makeshift cyber range of its own in Kyiv to counter Russian attacks (Antoniuk, 2024). Iranian APTs (APT 33, for example), codenamed "Kittens", have consistently employed their progressively complex cyber capabilities (Shample, 2023) to suppress internal political dialogue (CISA, n.d.). However, their recent military coalescence with Chinese and Russian groups has demonstrated a capacity to employ these cyber means on more strategic targets (Kendall-Taylor, 2024).

In light of recent joint cyber attacks on US infrastructure (Jockims, 2024), joint military exercises (Al Jazeera, 2024) and military technology (know-how) transfer by China, Russia, and Iran (Kendall-Taylor, 2024), it is evident that a strategic military partnership exists between these nations. Although the particulars on Russian and Iranian cyber ranges are unclear, one can only prudently assume that this triad shares a similar cyber test platform and infrastructure for conducting joint tactical military operations, as the nature of hybrid warfare inherently implies a level of interoperability in multi-domain operations, including cyber.

If not just for their shared geopolitical interests (FBI National Press Office, 2024), testing new military technology in real operational environments is always in the interest of two opposing military blocs, in this case, the Western bloc and the triad. This is an opportunity that NATO is certainly exploring in Ukraine against the triad's technology and vice-versa. Under recent developments in the war in Ukraine, targeting specific EU infrastructures would be the logical next step as it presents a perfect strategic opening to continue to test the triad's military technology against the Western blocs. Regardless, joint operations already aim at European targets, as most recently observed by some EU parliamentarians (Sabanadze et al., 2024). Therefore, such events further highlight the need for solidified European cyber-resilience strategies.

The EU cyber community largely focuses on assessing and enhancing the cyber capabilities of individual member countries and their industries while ensuring a growing cyber maturity status at the European level. They operate within the existing framework of the European Union Agency for Cybersecurity (ENISA) and the European Cyber Security Organization (ECSO). These two cyber domain organisations, particularly ENISA, provide Europe with different cyber-cooperation tools, such as National Cybersecurity Information Response

teams (CSIRTs), Information Sharing and Analysis Centers (ISACs) (ENISA, 2022), and most recently through the Joint Cyber Unit, a platform for coordinated responses to larger cyber issues (Bertuzzi, 2021). Moreover, Project PANDORA (EDIDP, 2022) constitutes an EDF project that also shows promise in this regard. However, none of these platforms provide Europe with a coordinated and collective platform for testing military equipment and their cyber vulnerabilities in real-world simulation scenarios.

In this context, only NATO's infrastructure currently provides cyber parity for the EU through the CR14 "Estonian Cyber Security Training and Exercise Center" which includes various cyber ranges (Open Cyber Range, NATO Cyber Range, Estonian Cyber Range and the Classified Cyber Range) (CR14, n.d.), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the NATO Science and Technology Organisation. Through multi-national exercises like Locked Shields, APEX (The NATO Cooperative Cyber Defence Centre of Excellence, n.d.), CIWX (CR14, n.d.), and Crossed Swords (NATO's Strategic Warfare Development Command, 2024), these joint institutions have effectively validated the importance of cyber ranges in fostering interoperability and cyber-resilience (NATO's Strategic Warfare Development Command, 2024).

This existing framework perhaps also explains why collective European interoperability in various domains, independent of NATO, has been so hard to achieve. Primarily, effective proof of concept has been validated solely at the NATO level. Following, the scale of investment already pledged towards the NATO framework makes it less relevant to do so again purely for the EU. Then again, the goal should not be to detach EU capabilities from NATO solely for doing so.

Assuredly, Europe has the potential to foster effective interoperability in the cyber domain and achieve international cyber parity, should pertinent infrastructure, industry, know-how and full EU membership be mobilised towards this goal. A truly federated collective cybersecurity consortium in Europe would pool together EU resources and know-how on a consistent, continuous fundament to bring about not only cyber autonomy and cyber prevention capabilities but, most importantly, cyber interoperability and cyber resilience, a kind that could be independent from the NATO framework.

Undeniably, cyber-attacks will take place one way or another and continuously increase in complexity, considering the advent of quantum computing being used for this purpose (Scanlon, 2023) and the Sino- Russian cooperation in the quantum field (Weber, 2024). The objective then should not be to find a holy grail solution that prevents attacks altogether, which is quite impossible given that technology can be a double-edged sword. The FACT framework allows for the acceptance of this daily risk and prepares for this possibility. The

first step in this direction is to have the capacity to test European technology against state-of-the-art cyber structures in an immersive environment. Indeed, FACT embodies this capacity.

III. Concept of Operations

In June 2024, the General Assembly of the FACT Consortium held a meeting to present recent developments and the overall concept of operations (CONOPS) for the joint programme. This set the basis for the collective use of FACT as a shared, interoperable range to be used as a common European asset moving forward. Regarding the interoperability of the European structures, FACT encourages and demands improved European coordination and cooperation to tackle current and future cyber threats efficiently. As stated in Kongsberg's announcement on FACT, this kind of cooperation is what Europe needs to "prevent, detect, defend against, recover from and deter cyber-attacks on military systems" (Kongsberg Defence & Aerospace, 2024).

The term cyber-resilience is perhaps what best describes the desired outcome of FACT for European militaries overall. This notion is best exemplified by Jon Leistad, the Kongsberg project coordinator for FACT, in his panel lecture at EUROSATORY 2024: "During my military years, if I sent a drone, I would have liked to know for certain that there were no cyber back doors, now we can anticipate this, FACT is that cyber resilience and mitigation answer – all to complete the mission." (Leistad, 2024). As of September 2024, the consortium is building towards the working prototype stage and expects to have reached a value of 6/9 in its overall Technology Readiness Level (TRL) at the end of the project, meaning the prototype cyber-range will be demonstrable in an operational environment.

Currently, the specific types of military equipment within the parameters for testing are those in the "domains of surveillance, data communication and tactical communication, and commercial unmanned vehicles." (FACT - Federated Advanced Cyber Physical Test range, 2024). The cyber range test-bed practical framework will focus on Hardware in the Loop (HIL) type testing, which refers to the integration of the specific embedded software and hardware components of a given system (Bogdanov, 2023) under real-world conditions. This technique is used industry-wide for complex system testing and is one of Kongsberg's know-how specialisations (Leistad, 2024, September).

At the onset, testing the cyber-physical system to be investigated can be connected directly in the range or indirectly by remote connection. This feature is also conducive to enhancing interoperability (FACT Consortium, 2024) and made possible by the shared architecture and toolset that FACT enables. Therefore, new technologies designed by individual countries can

immediately access the cyber range remotely, allowing for more efficient logistics and less time delay in testing.

Four key components constitute the framework that makes up the cyber-range and feeds the central "hybrid" hub: the installed military systems (operational technology), the IT-system infrastructure (information technology), the environment, which "generates traffic, emulation & simulation in the network" (depending on the specific operational parameters required) and AI (Machine Learning) (FACT Consortium, 2024). Artificial Intelligence and Machine Learning form the backbone for two separate AI systems which work against each other (the Red and Blue teams). The Red team is designed to stimulate offensive attacks, and the Blue team for dynamic defences, where the operational and information technologies are the object of interest (FACT Consortium, 2024). These four components work in tandem to feed the necessary information to the central "hybrid" Cyber Range Hub, which creates the simulation conditions for testing, aggregates the results and provides feedback on vulnerabilities for the specific CPS.

Conclusion

Through the analysis of FACT's basic structure, the concept of cyber ranges and the current international cyber context, some key lessons can be taken away. FACT's positioning in the current hybrid context of warfare, particularly in multi-domain military operations, makes it an undeniable resource for cyber- interoperability which will be vital to long-term adaptability and resilience. Although the incomplete FACT membership reveals a lack of comprehensive European dedication, also in investment scale, as it will take time to reach a higher TRL, the potential exists for increased autonomy and cyber-parity. One of the issues with hybrid warfare is the blurred line between military and public infrastructure, especially when both can serve the same level of military efficacy or damage when vulnerable to a cyber-attack.

The Chinese and Russian cases can allow for lessons learned and applied to a future FACT framework. In particular, it would be beneficial for an advanced FACT framework to integrate large-scale critical infrastructure systems for testing as well as those of pertinent entities dealing with classified information, not just smaller-scale military systems and equipment. Similarly, lessons learned from operations under NATO can be applied to the EU context, namely complex annual cyber exercises and multiple dedicated cyber ranges. Assessing which current EU-owned infrastructure is currently employed in the NATO framework that can be appropriated for EU use, namely Estonia's CR14 and integrating these with pertinent EDF, EDIDP and PESCO projects could also be highly impactful. An additional tool that could be useful is to combine a joint data matrix set on adversarial cyber MOs within FACT's

database that can be regularly updated by the public, private and governmental sectors. Finally, the application of quantum computing in the cyber domain, in addition to AI, could allow for even more resilient cyber systems, given its ability to compromise encryption.

When technology is seen as a double-edged sword, one must logically assume that the best anti-cyber systems will always have to counter next-generation cyber threats. Thus, it becomes imperative that Europe tests (and develops the capacity to test) the newest military equipment, systems, and infrastructures not only against the next-generation cyber threats but that it does so together using a shared platform that demands unavoidable cyber-interoperability.

It is in this context that the FACT consortium stands out. It marks not only the start of a different European structure in the cyber domain but perhaps most importantly, a different European attitude, one that embodies the political will necessary for true change and autonomy in the long term.

Bibliography

Al Jazeera. (2024, March 12). China, Iran and Russia hold Joint War Games in Gulf of Oman. https://www.aljazeera.com/news/2024/3/12/china-iran-and-russia-stage-joint-naval-drills-in-gulf-of-oman

Antoniuk, D. (2024, August 26). In a kyiv hangar, Ukraine launches a cyber range for everyone. Cyber Security News | The Record. https://therecord.media/ukraine-cyber-range-kyiv-hangar

Bergmann, M., Wall, C., Monaghan, S., & Morcos, P. (2022, August 18). Transforming european defense. CSIS. https://www.csis.org/analysis/transforming-european-defense

Bertuzzi, L. (2021, October 20). EU countries to "explore the potential" of a joint cyber unit. www.euractiv.com. https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-explore-the- potential-of-a-joint-cyber-unit/

Bogdanov, V. (2023, May 22). The ultimate guide to hardware-in-the-loop testing: What, when, and how. rinf.tech. https://www.rinf.tech/the-ultimate-guide-to-hardware-in-the-loop-testing/¨

CISA. (n.d.). Nation-state cyber actors. Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber- actors

CR14. (n.d.). Multiverse of cyber ranges. CR14 homepage RSS. https://www.cr14.ee/

EDIDP. (2022, December 8). EU-funded Cyber Defence Platform (PANDORA) successfully demonstrated. Defence Industry and Space. https://defence-industry-space.ec.europa.eu/edidp-eu-funded- cyber-defence-platform-successfully-demonstrated-2022-12-08_en

ENISA. (2022, January 24). Tools. https://www.enisa.europa.eu/tools

European Commission. (2023). Federated Advanced Cyber Physical Test Range. EU funding & tenders portal. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/968727943/project/101121335/program/44181033/details

European Commission. (n.d.). Joint Cyber Unit. Shaping Europe's digital future. https://digital- strategy.ec.europa.eu/en/policies/joint-cyber-unit

European Cyber Security Organization. (2020, March). Understanding cyber ranges: From hype to reality. ecs-org.eu. https://ecs-org.eu/ecso-uploads/2023/05/2020_SWG-5.1_paper_UnderstandingCyberRanges_final_v1.0-update.p

EUROMIL. (2021, June). Cybersecurity and defence info sheet June 2021 EU's ... https://euromil.org/wp-content/uploads/2021/06/2106_cybersecurity_and_defence_info_sheet.pdf

Euronews with AP. (2024, May 29). Disruptive attacks double in EU in recent months, cybersecurity chief says | Euronews. Euronews. https://www.euronews.com/next/2024/05/29/disruptive-attacks-double- in-eu-in-recent-months-cybersecurity-chief-says

European Union. (2022). Europa. European Defence Fund. https://defence-industry-space.ec.europa.eu/document/download/2a10a36d-5e42-432e-bb06-ebc690797abe_en?filename=FACT+- +Factsheet_EDF22.pdf

FACT - Federated Advanced Cyber physical Test range. (2024, September 17). Fact - Federated Advanced Cyber Physical Test Range on linkedin: #fact #cybersecurity #eudefenceindustry #strongertogether. FACT - Federated Advanced Cyber physical Test range on LinkedIn: #fact #cybersecurity #eudefenceindustry #strongertogether. https://www.linkedin.com/posts/fact-federated-advanced-cyber-physical-test-range_fact-cybersecurity-eudefenceindustry-activity- 7241715731728318464-RVg7?utm_source=share&utm_medium=member_desktop

FACT Consortium. (2024, September 20).

FBI National Press Office. (2024, September 18). Joint Odni, FBI, and Cisa statement. FBI. https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-091824

Hakkala, J., & Melnychuk, J. (2021, June). Russia's strategy in Cyberspace. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

Jockims, T. L. (2024, June 26). America's drinking water is facing attack, with links back to China, Russia and Iran. CNBC. https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china- russia-and-iran.html

Kendall-Taylor, A. (2024, May 29). The axis of upheaval: How the convergence of Russia, China, Iran, and North Korea will challenge the US and Europe. ICDS . https://icds.ee/en/the-axis-of-upheaval-how- the-convergence-of-russia-china-iran-and-north-korea-will-challenge-the-us-and-europe/

Kongsberg Defence & Aerospace. (2024, January 26). Official launch of the European Defence Fund Project Fact. Kongsberg Defence & Aerospace. https://www.kongsberg.com/kda/news/news- archive/2024/official-launch-of-the-european-defence-fund-project-fact/

Langner, G. (2023). Fact - ait austrian institute of technology. ait.ac.at. https://www.ait.ac.at/en/research- topics/cyber-security/projects/fact

Lazarov, G. (2024, January 5). Bianor commences work on three new defense projects. Bianor. https://bianor.com/blog/new-defense-projects/

Leistad, J. (2024, June 21). An Executive Summary of The Cybersecurity Challenges for Defence Industries. EUROSATORY . Paris; Villepinte. https://www.linkedin.com/posts/fact-federated-advanced-cyber-physical-test-range_the-fact-project-in-the-spotlight-at eurosatory-activity-7210959882689101824-jR2T utm_source=share&utm_medium=member_desktop

Leistad, J. (2024, August 29). We asked 3 questions to Jon Leistad. Linkedin. other, FACT. Retrieved September 2024,. https://www.linkedin.com/posts/fact-federated-advanced-cyber-physical-test-range_jon-leistad-interview-fact-activity-7234862380076216320-5DQG?utm_source=share&utm_medium=member_desktop

NATO's Strategic Warfare Development Command. (2024, July). Cooperative Cyber Defence Centre of Excellence: Locked … Allied Command Transformation. https://www.act.nato.int/article/ccd-coe-2024

Sabanadze, N., Vasselier, A., & Wiegand, G. (2024, June 26). China-russia alignment: A threat to Europe's security. Merics. https://www.merics.org/de/report/china-russia-alignment-threat-europes- security

Scanlon, T. (2023, April 10). Cybersecurity of Quantum Computing: A new frontier. SEI Blog. https://insights.sei.cmu.edu/blog/cybersecurity-of-quantum-computing-a-new-frontier/

Shample, S. (2023, February). Iranian apts: An overview. Middle East Institute. https://www.mei.edu/publications/iranian-apts-overview

The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and Interdisciplinary Cyber Defence Hub. CCDCOE. https://ccdcoe.org/

Vice Admiral Connor, J. (2019, February 21). Sustaining undersea dominance. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2013/june/sustaining-undersea-dominance

Weber, V. (2024, March 22). The New Quantum Technology Race. Internationale Politik Quarterly. https://ip-quarterly.com/en/new-quantum-technology-race#:~:text=As%20of%202022%20and%20according,Japan%20(%241.8%20billion)%20combined.