EUROPEAN POLICY CENTRE

POLICY BRIEF

TRANSNATIONALISATION PROGRAMME

EUROPE IN THE WORLD PROGRAMME

26 JULY 2024

# Russia's war against Ukraine: Lessons on infrastructure security and new technologies

Maria Martisiute
Auriane Técourt

## INTRODUCTION

In 2022, Russia hit Ukraine with a major cyberattack and unleashed a full-scale war of aggression. This includes new technologies[1] and AI-enabled capabilities such as the Bylina electronic-warfare command-and-control system.[2] Nord Stream[3] and the Balticconnector[4] also fell victim to sabotage attacks by hostile actors. The EU has stepped up the resilience and cybersecurity of critical infrastructure. However, the capacity to leverage innovative technologies and defensive AI remains underdeveloped. Worrying is also the fact that protection of industrial control systems (ICS)[5] remains unaddressed. As Russia upgrades[6] its 2030 National AI Development Strategy,[7] there is an urgency to integrate the security of industrial controls into the EU's approach to the cybersecurity of critical infrastructure, before Moscow strikes with deadlier offensives. It is also time to start building a measured, albeit scalable, deployment plan for new technologies that may be AI-enabled for European critical infrastructure in connectivity with Ukraine and Moldova.

## BACKGROUND: RUSSIA'S CYBER-MILITARY THREAT

While the world was focused on the 200,000 Russian troops on the Ukrainian border, on 23 February 2022, Russia hit Ukraine with some of the most impactful cyberattacks[8] to date. They rendered much of Ukraine's infrastructure inoperative, deactivated the US satellite provider[9] (Viasat Inc's KA-SAT) used by Ukraine's military, and spilled over into Germany, France, Poland, Hungary, Greece, and Italy.[10] A day later, Russia began a full-scale ground invasion, including airstrikes. The integration of cyber capabilities into Russia's military strategy aimed to facilitate the military takeover by destabilising Ukraine internally and cutting it off externally.

Even though the cyberattacks did not provide the expected military advantage, it created significant damage and revealed Russia's expanding capabilities. This may be used elsewhere, for example, against Moldova and Georgia ahead of national elections in autumn 2024.[11] It also exposed the unpreparedness of the West and gave a sense of urgency to bolster cybersecurity. After all, neither Ukrainian nor Euro-Atlantic state security structures deterred the attack. In response to Kyiv's request, the EU activated the cyber rapid-response team[12] (CRRT) to assist Ukraine, and cyber non-profits such as the IT Army of Ukraine consisting of 300,000 international volunteers also helped.[13] But to a high degree it was the US technology companies who provided the tools that allowed Ukraine to defend itself from the Russian cyberattack.[14] The reliance on volunteers, and foreign private entities based 10,000 kilometers away, reflects a worrying state of European cybersecurity and a shortage of experts.

> **The reliance on volunteers, and foreign private entities based 10,000 kilometers away, reflects a worrying state of European cybersecurity and a shortage of experts.**

**Russia's AI strategy**

Russia's threat must be understood in the context of Moscow's AI strategy, which started with President Vladimir Putin's 2017 statement that whoever dominates AI "will rule the world".[15] Russia's first 10-point military AI initiative[16] and National AI Development Strategy[17] followed in 2018-19 through 2030 led by Sberbank (financing sector), Rostec (military sector) and Gazprom Neft (oil/gas sector). In 2023, Putin announced its review:[18] He highlighted generative AI, partnerships build-up, and a need to counterbalance Western algorithms, which Putin called "monopolistic" and "biased."

Russia's innovation capabilities remain limited, ranking 51/132 according to the Global Innovation Index 2023. But Moscow does not need to be among the world's top 10 tech giants to launch a lethal attack.

Despite these priorities, Russia's innovation capabilities remain limited, ranking 51/132 according to the Global Innovation Index 2023.[19] But Moscow does not need to be among the world's top 10 tech giants to launch a lethal attack.[20] It has developed and employed advanced technologies against Ukraine through unmanned vehicles, robotics and, electronic weapons such as AI-enabled Bylina.[21] Russia is also deepening cybersecurity cooperation with Tehran,[22] Beijing[23] and Pyongyang,[24] which demonstrates their alignment in opposition to the West. Thus far, cyberattacks on the infrastructure of the EU and NATO have not been attributed to the axis of Russia, China, Iran, and the Democratic People's Republic of Korea (DPRK). Still there should be no surprise if their cooperation in cybersecurity through combined training and technology transfer became more menacing.

## STATE OF PLAY: CATCHING UP ON CYBERSECURITY BUT MISSING OUT ON AI

Russia's cyber capabilities highlight the need for better preparedness and robust measures in the Euro-Atlantic area. The EU is starting to catch up, but the approach remains slow and haphazard.

The EU started with achievable goals: the expansion[25] of the EU's NIS2 to public administration, space, and electronic communication networks. As well as the obligation to establish a registry for entities providing cross-border services by the European Union Agency for Cybersecurity (ENISA) to help speed up and coordinate the EU's response to large scale cyber-attacks.[26] The Directive on the Resilience of Critical Entities[27] is also welcome because it sets some ground rules for all member states. Such rules relate to the requirement to carry out risk assessments on a regular basis and the development of national strategies for the cybersecurity of critical infrastructure. The Directive also foresees additional support to the entities who provide services to six or more member states. This is a vital step in mitigating the effects of large-scale cyberattacks with cross-border dimensions.

In addition, the political agreement reached[28] in March 2024 on the EU Cyber Solidarity Act[29] (Act) provides the EU with new capabilities (European Cybersecurity Shield, Alert System, Emergency Mechanism and Incident Review Mechanism) to detect, prepare and respond to cyberattacks across the EU. However, this development has four significant shortcomings:

- **The Act would be more effective if it foresaw scenarios of worst-case attacks on infrastructure as well as procedures to deal with liability in situations where, for example, important data was lost, and the neighbouring country's network was also damaged.** Moreover, reducing the time needed to detect a large cyberattack from 190 days to a few hours will be a struggle unless the EU adopts significantly higher cybersecurity measures. Indeed, the provision for the EU Cybersecurity Reserve aims to support the Cyber Emergency Mechanism by creating a list of reliable providers who can respond to major cyberattacks or incidents in the EU. This provision promotes stronger collaboration between the public and private sectors. However, there are some shortcomings in the nature of the reserve. There are no provisions regarding the reserve's size, diversity, or accountability, nor are there attack scenarios. If the provider does not meet the expectations, the Act fails to specify if another provider would intervene.[30]
- **Ukraine and Moldova are not associated with the reserve nor with the Act given that they do not have cybersecurity enshrined as a strategic objective within the Digital Europe Programme (DEP). A lack of coordination with NATO is also problematic.** Associating and including Ukraine and Moldova would provide a substantial safeguard for the Euro-Atlantic security considering that Russia's attacks on Ukraine can spill over into the territory of the EU and NATO. For example, in the Baltic States, Denmark, and beyond.[32] Moreover, Russia may attack a non-NATO member of the EU and spill over into the shared EU-NATO area without directly attacking NATO. This is pertinent given the rising number of cyberattacks since Russia's invasion of Ukraine. In 2022, the Google Threat Analysis Group[33] counted over a 300% increase of Russian-state-backed cyberattacks in NATO countries. In Ukraine,[34] 4,748 cyber incidents happened in 2022-2023, of which 1,415 were "major or critical." The Russia-Ukraine cyberwar is projected to be "even harder"[35] in 2024 and beyond, while the global cost of cybercrime may triple by 2027.[36] In this regard, both the EU and NATO would benefit if the Act incorporated channels of coordination and consultation.

- **The third shortcoming of the Act is related to Establishing the European Cybersecurity Shield.** Using cutting-edge technologies such as AI to detect cyber threats through National and Cross-Border Security Operations (SOCs) will enhance intelligence sharing and real-time situational awareness among the member states.[37] In this regard, the deployment of EU pilots for 2024-2026, such as cyber consortiums ATHENA[38] or ENSOC[39] carry the potential for enhanced cross-border coordination among the selected member states. However, the aim of creating an AI-assisted pan-European network of cyber hubs is based on aspiration.[40] The national and cross-border cyber-hubs are non-mandatory, do not cover critical infrastructure and do not include Ukraine or Moldova. Small and regional steps using advanced technologies including AI should not be discounted. However, the proposed approach is not so much the creation of a shield or a network as a fragmented cybersecurity landscape with some countries being better protected than others. For any of this to have a "network effect" across the EU, it would also be important that the proposed cross-border consortiums are interoperable with each other.

- **The Act (and the wider EU's approach to cybersecurity) does not consider protecting the industrial control systems of critical infrastructure.** This is despite evidence that cyberattacks are shifting towards industrial controls (ICs) and away from the more typical IT-related databases.[41] This is important, because ICs are the key vulnerabilities in critical infrastructure due to their monitoring and physical control processes. According to Industrial Cybersecurity Consultant Vytautas Butrimas[42] and Lecturer on hybrid threats, resilience, and global strategy Chris Kremidas-Courtney,[43] there is a need to fundamentally change the approach to the security of critical infrastructure by incorporating the protection of industrial controls.

  The EU should mandate member states and invite neighbouring countries to participate in at least one AI-assisted cross-border cyber hub and SOC, in close coordination with NATO. The EU pilots from 2024-2026 must create synergies with NATO's exercises such as the Cyber Coalition 2022 event[44] (NATO's flagship annual collective cyber defence exercise) and Exercise Dynamic Messenger 23, which have already tested the ability of emerging technologies and AI to protect critical infrastructure.[45] The scope of these exercises should also be extended to include the industrial control defences, Ukraine and Moldova, to maximise standardisation, interoperability and minimise vulnerabilities. Furthermore, findings should be leveraged to design mature and stable specifications for advanced technologies and defensive AI, and feed into the EU-NATO Taskforce on critical infrastructure,[46] NATO's undersea infrastructure cell,[47] and relevant agreements with third countries such as in the scope of the European Network of Transmission System Operators for Electricity (ENTSO-E).[48]

### A deployment plan for new and AI-enabled technologies

AI presents threats and opportunities which the EU and NATO must factor into their approach to infrastructure security. AI can enable cyberattacks to become more targeted and sophisticated through phishing emails, malware or deepfakes of unprecedented quality. It could also be developed to find vulnerabilities in a victim's infrastructure and attack - known as offensive AI. While offensive AI's speedy, accessible and evasive nature, which supersedes conventional security systems,[49] can be counteracted by new technologies enabled by defensive AI. Therefore it is important that the EU work with NATO to move from aspiration to action and start developing stable and mature specifications for new and AI-enabled technologies. Based on those specifications, they should build a measured, albeit scalable, deployment plan along the critical European infrastructure networks. This needs to be done selectively yet speedily before offensive AI becomes ever more mainstream, while simultaneously continuing to research and test breakthrough technologies and future AI.

**It is important that the EU works with NATO to start developing stable and mature specifications for new and AI-enabled technologies, and build a measured, albeit scalable, deployment plan.**

The deployment plan should be developed step by step, with indicative deadlines for its implementation and select as priority several segments of critical infrastructure that are suitable for early deployment (phase 1); based on lessons learned, the plan should progressively extend (phase 2) to those infrastructure segments that connect to phase 1, to turn the segments of infrastructure into a connected network. The connectivity with the infrastructure segments of neighboring countries (phase 3) such as Ukraine and Moldova should also be considered.

As the threatened landscape evolves such an approach requires continuous research, testing and understanding of innovative technologies including how AI could enable defenses against cyberattacks and sabotage. **The following examples illustrate which new technologies could be potentially applied and standardised for early deployment on critical infrastructure in the EU and NATO:**

- **In 2022, Nord Stream, a gas pipeline running from Russia to Germany under the Baltic Sea, was sabotaged by a bomb.**[50] To counter such attacks, technologies including underwater sensors could be deployed for early warning. Autonomous Underwater Vehicles (AUVs) could also be used to mitigate and prevent sabotage by moving, monitoring, analysing data, pre-warning, and enhancing decision-making 24/7. AUVs can also jam signals. NATO has already tested the viability of AUVs on undersea infrastructure through a series of multi-domain exercises in Portugal.[51]

- **In 2023, the Balticconnector, the EU's first gas interconnector[52] between Finland and Estonia, was damaged by an anchor.[53]** Seismometers and acoustic sensors such as distributed acoustic sensors (DAS) could be deployed to monitor, analyse, share data, and pre-warn about seabed activity 24/7. The new technology of DAS is advantageous because it suits linear infrastructure such as long pipelines in a high-density environment.[54] In this regard, lessons can also be drawn from wildlife conservation in sub-Saharan Africa, which relies on the technologies of underwater robots and microcontroller sensors to send notifications about any threats and risks to the environment.[55] Moreover, since the Balticconnector was damaged by a private company, legal and financial measures such as financial fines and barring of the private company from European ports could also serve as a deterrent measure.[56]

- **Telecommunications and electricity grids can be powered by advanced technologies and AI monitoring 24/7, which could detect thousands of failed log-in guesses and prompt defensive measures before it is too late.** Moreover, quantum sensing and quantum encryption technologies carry enormous potential[57] both to enhance threat detection and risk analysis and to protect critical infrastructures even from the most sophisticated cyberattacks.

## PROSPECTS: ENHANCING CRITICAL INFRASTRUCTURE SECURITY

The EU has strengthened cybersecurity and resilience of critical infrastructure. However, there is scope for improvement. Considering the pace at which new technologies and AI-enabled technologies are developing, the following steps would enhance the security of European infrastructure:

**1: Possible attack scenarios.** Consideration of the size, diversity and the liability of EU Cybersecurity Reserve would make the Cyber Emergency Mechanism more resilient, while the development of possible attack scenarios, including the worst possible case, would increase the readiness and response of the emergency mechanism itself.

**2: Mandatory SOCs and cyber hubs.** The Union should mandate member states and invite neighbouring countries such as Ukraine and Moldova to participate in at least one SOC and AI-assisted cross-border cyber hub proposed in the scope of the EU Cyber Solidarity Act to create a "network effect" across the EU.

**3: Industrial control systems (ICS).** Considering the shift of cyberattacks towards ICS and away from more traditional IT databases and communications, the EU must integrate the security of industrial control systems into its cybersecurity approach to critical infrastructure.

**4: Synergies between the EU and NATO.** The EU and NATO should seek synergies in the scope of pilots and exercises dedicated to testing the ability of emerging and AI-enabled technologies to enhance situational awareness and protect critical infrastructure. The pilots and exercises should also cover the defences of industrial controls, include Ukraine, Moldova and relevant agreements with third countries such as in the scope of ENTSO-E. Findings and lessons learned should be leveraged to develop mature and stable technical specifications for innovative technologies and defensive AI.

**5: A deployment plan for new technologies that may include AI.** The EU and NATO should progressively build a measured albeit scalable deployment plan for innovative technologies that may be AI-enabled along the critical European infrastructure networks and connect to Ukraine and Moldova. The process should be developed in phases and select as a priority several segments of critical infrastructure that are suitable for early deployment. The development of stable and mature specifications would help ensure that the deployment plan is scalable and interoperable.

The Euro-Atlantic cybersecurity landscape is only as strong as its weakest link. Russia will continue flexing cyber-military offensives until Putin meets his goals in Ukraine and beyond. Considering that Norwegian,[58] Swedish,[59] German,[60] Polish,[61] and British[62] authorities do not exclude an attack on EU and NATO countries before 2030, the EU must enhance the cybersecurity of critical European infrastructure through the protection of industrial control systems, joint pilots and exercises with NATO, and progressively build a measured yet scalable deployment plan for new technologies in connectivity with Ukraine and Moldova.

*The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute an endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.*

[1] Gordon Corera, "Ukraine war: Cyber-teams fight a high-tech war on front lines (bbc.com)," 6 September 2023.

[2] David Axe, "Russia Sent Its New A.I. Drone-Killer To Ukraine. A Drone Blew It Up. (forbes.com)," 13 January 2023.

[3] Melissa Eddy, "Three Inquiries, but No Answers to Who Blew Holes in Nord Stream Pipelines - The New York Times (nytimes.com)," 25 October 2022.

[4] Jon Henley, "Undersea pipeline damage appears to be deliberate, says Finland," *The Guardian*, 10 October 2023.

[5] Vytautas Butrimas, "Hybrid CoE Working Paper 18: Defending critical infrastructure: The challenge of securing industrial control systems - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats," 2 June 2022.

[6] President of Russia, "Artificial Intelligence Journey 2023 conference • President of Russia (kremlin.ru)," *Official Website*, 23 November 2023.

[7] Artificial Intelligence of the Russian Federation, "National strategy (ai.gov.ru)", *Official Website* (Accessed 17 July 2024).

[8] James Pearson, "Russia downed satellite internet in Ukraine -Western officials | Reuters," 11 March 2022.

[9] Gordon Corera, "Ukraine war: Cyber-teams fight a high-tech war on front lines (bbc.com)," 2 September 2023.

[10] Ministry of National Defence of the Republic of Lithuania, "2022_key-trends-and-statistics-of-cyber-security.pdf (nksc.lt)," 2002.

[11] James Andrew Lewis, "Cyber War and Ukraine (csis.org)," *Centre for Strategic and International Studies*, 16 June 2022.

[12] European Defence Agency, "Activation of first capability developed under PESCO points to strength of cooperation in cyber defence (europa.eu)," *Official Website*, 24 February 2022.

[13] World Economic Forum, "How the cyber world can support Ukraine | World Economic Forum (weforum.org)," Official Website, 19 March 2022.

[14] Ian Bremmer, "The Next Global Superpower Isn't Who You Think | Ian Bremmer | TED (youtube.com)," April 2023 (Accessed 17 July 2024).

[15] Edoardo Maggio, "Putin: Whatever Country Has Best AI Will Be 'Ruler of the World' - Business Insider," *Business Insider*, 4 September 2017.

[16] Samuel Bendett, "Here's How the Russian Military Is Organizing to Develop AI - Defense One," Defence One, 20 July 2018.

[17] Artificial Intelligence of the Russian Federation, "National strategy (ai.gov.ru)", *Official Website* (Accessed 17 July 2024).

[18] President of Russia, "Artificial Intelligence Journey 2023 conference • President of Russia (kremlin.ru)," *Official Website*, 23 November 2023.

[19] World Intellectual Property Organisation, "Global Innovation Index 2023 – Innovation in the face of uncertainty (wipo.int)," 2023 (Accessed 17 July 2024).

[20] Jonathan Ponciano, "The World's Largest Technology Companies In 2023: A New Leader Emerges (forbes.com)," 8 June 2023.

[21] David Axe, "Russia Sent Its New A.I. Drone-Killer To Ukraine. A Drone Blew It Up. (forbes.com)," 13 January 2023.

[22] Omree Wechsler, "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East | Council on Foreign Relations (cfr.org)," *Council on Foreign Relations*, 15 March 2021.

[23] Yuxi Wei, "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty - The Henry M. Jackson School of International Studies (washington.edu)," 21 June 2016.

[24] Benjamin R. Young, "The Emerging North Korean-Russian Cybercrime Partnership | The National Interest," *National Interest*, 31 March 2022.

[25] European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's digital future (europa.eu)," *Official Website*, 29 June 2023.

[26] European Union Agency for Cybersecurity (ENISA), "NIS Directive — ENISA (europa.eu)," *Official Website* (Accessed 17 July 2024).

[27] European Commission, "Critical entities' resilience (europa.eu)," *Official Website*.

[28] European Commission, "Commission welcomes political agreement on Cyber Solidarity Act | Shaping Europe's digital future (europa.eu)" *Official Website*, 6 March 2024.

[29] European Commission, "Cyber solidarity package: Council and Parliament strike deals to strengthen cyber security capacities in the EU - Consilium (europa.eu)," *Press Release*, 6 March 2024.

[30] European Commission, "A European Cyber Shield to step up our collective resilience (europa.eu)," *Official Website*, 5 April 2023.

[31] Laurens Cerulus, "Cyber 'spillover' from Ukraine looms in the Baltics – POLITICO," 22 February 2022.

[32] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED," 22 August 2018.

[33] Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape (blog.google)," 16 February 2023.

[34] The Economist, "The cyberwar in Ukraine is as crucial as the battle in the trenches (economist.com)," 20 March 2024.

[35] *Ibid.*

[36] World Economic Forum, "2023 was a big year for cybercrime – here's how we can make our systems safer | World Economic Forum (weforum.org)," 10 January 2024.

[37] European Commission, "The EU Cyber Solidarity Act | Shaping Europe's digital future (europa.eu)," *Official Website* (Accessed 17 July 2024).

[38] European Commission, "EU Funding & Tenders Portal (europa.eu)", *Official Website* (Accessed 17 July 2024).

[39] *Ibid.*

[40] European Commission, "Political agreement on Cyber Solidarity Act (europa.eu)", *Official Website*, 6 March 2024.

[41] Vytautas Butrimas, "Hybrid CoE Working Paper 18: Defending critical infrastructure: The challenge of securing industrial control systems - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats," 2 June 2022.

[42] *Ibid.*

[43] Chris Kremidas-Courtney, "Closing the cyber gaps in Europe's energy security - Friends of Europe," 18 October 2022.

[44] Michael Hill, "NATO tests AI's ability to protect critical infrastructure against cyberattacks | CSO Online," 5 January 2023.

[45] NATO's Allied Maritime Command, "Allied Maritime Command - NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal," *Official Website*, 4 October 2023.

[46] European Commission, "EU-NATO_Final Assessment Report Digital.pdf (europa.eu)," *Official Website*, June 2023.

[47] NATO, "NATO - News: NATO stands up undersea infrastructure coordination cell, 15-Feb.-2023," *Official Website*, 15 February 2023.

[48] The European Network of Transmission System Operators for Electricity, "220114_NCCS_Legal_Text.pdf (entsoe.eu)," *Official Website*, 14 January 2022.

[49] The Security Science Company, "What is Offensive AI and how to protect from it? | Secure-IC," 17 April 2023.

[50] Nerijus Adomaitis, Johan Ahlander, "Nord Stream: What's known about the mystery pipeline explosions? | Reuters," 7 February 2024.

[51] NATO's Allied Maritime Command, "Allied Maritime Command - NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal," *Official Website*, 4 October 2023.

[52] European Commission, "Balticconnector - European Commission (europa.eu)", *Official Website*.

[53] Andrius Sytas, Anne Kauranen, "Three Baltic pipe and cable incidents 'are related', Estonia says | Reuters," 27 October 2023.

[54] Hong-Hu Zhu, Wei Liu, Tao Wang, Jing-Wen Su, Bin Shi, "Sensors | Free Full-Text | Distributed Acoustic Sensing for Monitoring Linear Infrastructures: Current Status and Trends (mdpi.com)", *Multidisciplinary Digital Publishing Institute*, 5 October 2022.

[55] Jennifer Swanson, "National geographic kids. Everything robotics: all the photos, facts, and fun to make you race for robots: Swanson, Jennifer, author: Free Download, Borrow, and Streaming: Internet Archive," *National Geographic Kids*, 2016.

[56] Aljazeera, "Finland says Chinese vessel's broken anchor caused Balticconnector damage | News | Al Jazeera," 25 October 2023.

[57] Yagmur Yigit, Mohamed Amine Ferrag, Iqbal H. Sarker, Leandros A. Maglaras, Christos Chrysoulas, Naghmeh Moradpoor, Helge Janicke, "[2405.04874] Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities (arxiv.org)", *Cornell University*, 8 May 2024.

[58] James Rothwell, "We are running out of time to build defences against Russia, warns Norway's commander in chief (telegraph.co.uk)", 12 January 2024.

[59] Emma Löfgren, "'There could be war in Sweden': Civil Defence Minister urges Swedes to act (thelocal.se)," 8 January 2024.

[60] Nicolas Camut, "Putin could attack NATO in '5 to 8 years,' German defense minister warns – POLITICO", 19 January 2024.

[61] ERR News, "Polish security chief: NATO Eastern Flank states have 3 years to prepare for Russia attack | News | ERR," 3 December 2023.

[62] Faye Brown, "British citizens should be 'trained and equipped' to fight in a potential war with Russia, military chief says | Politics News | Sky News", 24 January 2024.

With the strategic support of
King Baudouin Foundation
*Working together for a better society*

Co-funded by the European Union