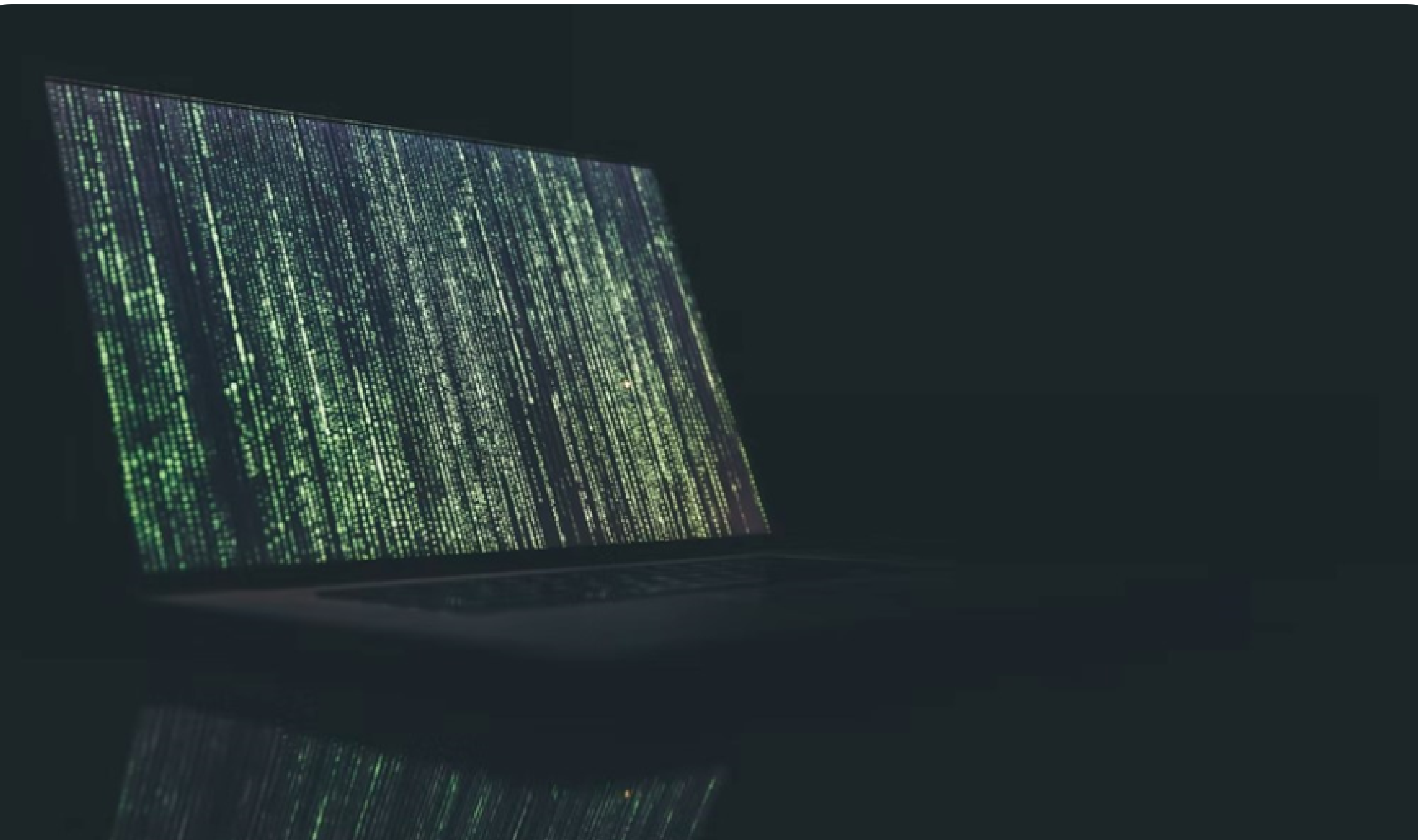
INFO FLASH
Finabel
European Army Interoperability Centre

The EU Deploys a Cyber Defence Team to Support Ukraine

WRITTEN BY CATERINA POZZI

Image credits: https://unsplash.com/photos/FXFz-sW0uwo



The European Union (EU) is mobilising a team of specialists, the Cyber Rapid Response Team (CRRT), to back up Ukrainian cybersecurity efforts during the current conflict. As the country is fighting on many fronts, this measure intends to strengthen the Ukrainian response to cyber-attacks by employing European expertise and capabilities.

The CRRT is a team of cyber specialists that falls under the Permanent Structured Cooperation (PESCO) scope. The team comprises ten national cybersecurity officers from Lithuania, Estonia, Croatia, Poland, the Netherlands, and Romania, and its operational control is on a rotating basis. Currently, it is held by Romania (Sprenger, 2022; PESCO, n.d.). The CRRT was set up in 2019 to assist the European member states and the EU institutions in cooperating and ensuring a higher level of cyber resilience using common toolkits to fight cyber threats. The team aims to strengthen states' capabilities, the capabilities at the European level, and increase cyber defence cooperation. What is peculiar, compared to other multilateral initiatives, is that the project allows not only the exchange of information but also of human resources (Galinec, Steingartner, & Zebic, 2019). The team works on incident response, forensics, and vulnerability assessment to respond to all types of scenarios. More specifically, it researches and develops cyber defence tools and organises cyber crisis simulation exercises (Tidy, 2022).

The EU has decided to deploy the CRRT for the first time in the context of the current conflict in Ukraine. This type of assistance complements the military equipment and humanitarian aid already provided. The decision follows Ukrainian cybersecurity services' warnings for new cyberattacks on the country's infrastructures. The threat was highlighted in a meeting between the Ukrainian Foreign Minister, Dmytro Kuleba, and EU Foreign Policy Chief, Josep Borrell. Kuleba declared that Ukraine would have welcomed the deployment to Kyiv of the team experts to evaluate “vulnerabilities of their key computer networks and systems” (Cerulus, 2022). The Lithuanian Ministry of Defence tweeted: "In response to Ukraine request, [we] are activating [a] Lithuanian-led cyber rapid-response team, which will help Ukrainian institutions to cope with growing cyber-threats. #StandWithUkraine." (Tidy, 2022) Kyiv's request for assistance follows two major cyberattacks that occurred in the last weeks. The first, in January, involved a threat of malware and data wiping, and the second, in February, hit the Ministry of Defence websites (Cerulus, 2022).

Nowadays, cyberspace is considered the fifth battlefield. Thus, strategic success in conflicts largely depends on access to cyber defence governance, determined by a set of tools and norms that protect critical infrastructures and networks (Calcara, Csernatoni, & Lavallée, 2020). The scope of cyber defence is to prevent, detect, and provide an adequate response to attacks, avoid disruption, and safeguard sensitive information and assets. Over the last decade, states and international organisations have become increasingly concerned about cybersecurity and cyber defence issues. In the EU, these started to be relevant in the late 90s. While at first, the scope was protecting citizens' rights and freedoms and did not entail the military dimension, after the cyberattacks in Georgia in 2008, the military, together with the protection of critical infrastructure, became the focus of discussion. As a consequence, regulations became increasingly specific in defining the EU's cybersecurity normative architecture (Calcara, Csernatoni, & Lavallée, 2020). For example, the 2013 EU Cybersecurity Strategy highlights among its core issues the necessity to promote the civil-military dialogue and the dialogue with international partners, the latter being the basis for the EU's decision to deploy the CRRT for the first time.

However, cyberattacks are nothing new in Ukraine. They have been reported in 2014, 2015, 2016, and 2017 and targeted mainly critical infrastructures, such as power grids or weapon systems, de facto weakening their operation (Noguchi & Ueda, 2018). They also affected the functioning of society seeking for its disruption and endangering its core values, for example, through the spread of disinformation or interruption of communications (Galinec, Steingartner, & Zebic, 2019). Consequently, Ukraine and the EU had already started a cyber-dialogue, peaked in June 2021 during a bilateral meeting. They affirmed their commitment towards global and secure cyberspace based on the rule of law. During the talks, the EU and Ukraine provided updates on cyber-related legal and institutional frameworks, addressed coordination and cooperation, digital transformation and capacity building activities, and reaffirmed the importance of the Budapest Convention as a solid basis for national and international legislation (EU4Digital, 2021). Thus, the deployment of the CRRT follows already existing cooperation between the two actors, and the EU's efforts support Ukraine's cybersecurity, which also involves investments and cyber-offensive and espionage tools. With the deployment of CRRTs, the EU will also provide a different kind of support, making its officials' expertise available to help the Ukrainian forces.

In addition, following the latest events, the EU has decided to take a step further by acknowledging the possibility of a spillover effect of the cyberattacks on European networks (Bertuzzi, 2022). The issue was addressed on 8 March 2022 during an informal meeting of the European governments, which drafted a declaration to reinforce the EU's cybersecurity capacities. The provisions also include a new Emergency Response Fund for Cybersecurity and further EU funding to support national capabilities. The meeting was mostly focused on the conflict in Ukraine and represents a promising development in cybersecurity cooperation among the member states.

Bibliography

Bertuzzi, L. (2022, March 8). EU countries to call for the establishment of a cybersecurity emergency fund. Euractiv. Retrieved from https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-call-for-the-establishment-of-a-cybersecurity-emergency-fund/

Calcara, A., Csernatoni, R., & Lavallée, C. (2020). Emerging Security Technologies and EU Governance. Actors, Practices and Processes. London: Routledge.

Cerulus, L. (2022, February 21). EU to mobilise cyber team to help Ukraine fight Russian cyberattacks. Retrieved from: Politico. Retrieved from https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/

EU4Digital. (2021, June 7). Cyberspace: EU and Ukraine launch dialogue on cyber security. Retrieved from EU4Digital: https://eufordigital.eu/cyberspace-eu-and-ukraine-launch-dialogue-on-cyber-security/

Galinec, D., Steingartner, W., & Zebic, V. (2019). Cyber Rapid Response Team: An Option within Hybrid Threats. IEEE 15th International Scientific Conference on Informatics. Retrieved from https://www.researchgate.net/publication/342249458_Cyber_Rapid_Response_Team_An_Option_within_Hybrid_Threats

Noguchi, M., & Ueda, H. (2018). An analysis of the actual status of recent cyberattacks on critical infrastructures. NEC Technical Journal, 12, 19-24. Retrieved from https://dr.nec.com.onenec.net/en/global/techrep/journal/g17/n02/pdf/170204.pdf

PESCO. (n.d.). Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity (CCRT). Retrieved from PESCO: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

Sprenger, S. (2022, February 22). European Union cyber defense team deploys to aid Ukraine. DefenseNews. Retrieved from https://www.defensenews.com/global/europe/2022/02/22/european-union-cyber-defense-team-deploys-to-aid-ukraine/

Tidy, J. (2022, February 22). Ukraine: EU deploys cyber rapid-response team. BBC. Retrieved from https://www.bbc.com/news/technology-60484979

Bibliography

Prem Mahadevan. (2010). The Military Utility of Drones (p. 3). Center for Security Studies (CSS), ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-78.pdf

Zegart, A. (2020). Cheap fights, credible threats: The future of armed drones and coercion. Journal of Strategic Studies, 43(1), 6–46. https://doi.org/10.1080/01402390.2018.1439747