# THE ROLE OF CIVILIAN CYBERSECURITY COMPANIES IN MILITARY CYBER OPERATIONS

**Csaba KRASZNAY**
*Ludovika University of Public Service, Budapest, Hungary*
krasznay.csaba@uni-nke.hu

**ABSTRACT**

*The Russia-Ukraine war has clearly shown that critical infrastructures are prime targets for cyber operations in addition to the physical domain. In practice, in many cases, these critical infrastructures are protected by civilian cybersecurity companies in the context of a managed security service, so their defense operations must necessarily be coordinated with military defense activities. This includes among others the sharing of information classified under different classification systems (national, EU, NATO) between different actors in national cyber defense, the inclusion of appropriate civilian experts in the armed forces, and the usage of cutting-edge cybersecurity technologies (e.g. AI-enabled solutions) that are first introduced for civilian use, with military organizations only having access to them later or possibly not encountering them at all due to procurement difficulties. The main goal of this paper is to introduce the existing opportunities and obstacles to civilians' involvement in military cyber operations in the areas of legislation, technology, and human resources from the European perspective. Moreover, the paper deals with the actual questions of cybersecurity intelligence sharing between civilian and military entities and the European Union's actions in order to improve the overall cybersecurity posture of the region.*

**KEYWORDS**: cyberspace operations, cyber warfare, European Union, security operation center, managed security service provider

## 1. Introduction

One of the most important questions of Russia's aggression against Ukraine in the first months of 2022 was how the cyber operations that have been affecting the country for years, and which have been an important pillar of Russian hybrid warfare, would work and develop in real combat conditions. Indeed, a significant number of military experts expected that land, air, and sea operations would be supported by significant and devastating cyber operations. But cyber operations were not decisive. Cyber-attacks against Ukrainian critical infrastructures were launched, but their modus operandi was not new compared to previous attacks and their impact was less than expected (Giles, 2023). Rob Joyce, Director of Cybersecurity for the US National Security Agency, in his State of the Hack 2023 presentation at the RSA 2023 Conference, summarized the first year of the Russia-Ukraine war, confirming that Russia had indeed conducted significant operations in Ukrainian cyberspace, launching more than 400 attacks against civilian critical infrastructure in sectors such as energy and finance in 2022 alone. However, these failed

DOI: 10.2478/raft-2024-0001

to achieve their objectives, mainly because the Russian military failed to properly integrate cyber operations capabilities into its overall military activities and because the intelligence services behind the operations, in particular the military intelligence organization GU GSh (Main Directorate of the General Staff of the Armed Forces of the Russian Federation), still commonly referred to both in Russia and abroad by its Soviet era acronym as GRU, were not prepared for large-scale warfare. Meanwhile, the U.S. private companies, who are involved in the supply chain of military aid to Ukraine, are prime targets for Russian cyber operations (Joyce, 2023).

Sir Jeremy Fleming, Director of the British Electronic Intelligence Organization, GCHQ (Government Communications Headquarters), in his lecture “If China is the Question, What is the Answer?” at the RUSI Annual Security Lecture 2022, highlighted three other aspects that underpin the relative failure of Russian cyber operations: the preparedness of Ukrainian cyber defense, the support of allied states, and the assistance of private companies through access to the latest technologies and cyber intelligence data: *“Ukraine’s resistance to the illegal Russian invasion is a result of their national unity. But that resistance also depends on their access to, and mastery of, advanced technology. The alliances and trust that enable that supply. And, of course, impressive and agile cyber security. That’s a government-to-government thing. But it’s reinforced by incredible and deep support from the private sector, especially, from the big technology companies. We’re very proud of the role the UK has played in Ukraine’s defense: that’s over a decade of UK and allied investment in cyber technologies and advanced equipment, together with a willingness to share intelligence to drive operations. It’s enhancing Ukraine’s security in real time. And it’s redefining how cyber can be responsibly used”* (Fleming, 2022).

My hypothesis is that the involvement of private companies in national military cyber defense and offensive cyber operations is essential in modern cyber warfare, however there are some practical barriers resulted from legal and trust issues. In that context, I use the U.S. Joint Publication 3-12 definition for cyberspace operations that is *“the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace”*, carried out by the national militaries (Joint Chiefs of Staff, 2018). Drawing on the experience of the Russian-Ukrainian war to date, I will show that private sector actors have access to high-quality cyberspace information and possess the human and technological capabilities that military integration is essential to successful cyberspace operational capabilities. I support my hypothesis by using a literature review and case studies as research methods. I will also describe the European Union’s legislative activity on cybersecurity and use this legal analysis as a research method that could pave the way for the development of military-civilian cooperation in Member States.

## 2. Opportunities and Barriers to Private Involvement in National Cyber Defense

The above reflections highlight the paradigm shift that military strategists must make with the emergence of cyberspace as an operational space. While in other operational spaces, military capability development is typically state-invested, tightly controlled, and there is a centuries-old tradition and legal order on how to use the resources of market companies in wartime, in cyber operational space, private sector innovation and capabilities are far ahead of those of national militaries. There are many reasons for this, such as the fact that the salaries of cybersecurity professionals far exceed those offered by the military, or the fact that, mainly due to the development of artificial intelligence, the solutions of large companies are evolving at a speed that national armies cannot keep up with, neither doctrinally nor in terms of training. Last but not least, global cybersecurity companies have the ability to collect CTI (cyber threat intelligence) from around the world through their extensive sensor networks, which perhaps no other country except the United States has the capability to do at the state level.

For this reason, it is not surprising that private domestic and global cybersecurity companies have also played a prominent role in Ukraine's cyber defense. The following points were highlighted in a study by Anushka Kaushik, analyst at GlobeSec Slovakia and also confirmed by Keir Giles from Chatham House (Giles, 2023):

– Private sector contributions have built upon and complemented the extensive cyber resilience campaign of Ukraine.

– A critical function of recruits and volunteers has been building trust between the Ukrainian government and the private sector.

– Ukraine has leveraged the private sector to protect and build the cyber defense of privately owned critical infrastructure companies.

– Private sector involvement in Ukraine's cyber defense, the cooperation between CERTs, technology companies, and security agencies suggests that ad-hoc collective cyber defense efforts are already underway.

– Governments are no longer the only prominent stakeholders in intelligence services in the information sphere given the private sector's unparalleled data and telemetry for understanding cyber-attacks and the threat landscape.

– The private sector is emerging as a reliable source of information on understanding threats in cyberspace and is contributing to shaping the public perception of conflict in this domain.

– The application of norms governing private sectors' actions in cyber war, the need for limitations on a cyber attacker's ability to target private cyber defense firms, like the restrictions imposed on attacks on civilians in general, and whether firms could be regarded as combatants are issues that require further study.

– The impact on small companies that do not possess enough information on cyber threats and are not part of existing partnerships that would enable access to such intelligence is questionable.

– Establishing a mechanism to monitor technological aid extended to Ukraine is a crucial area where public-private collaboration is necessary (Kaushik, 2023).

### *2.1. Involvement of Experts in National Cyber Defense*

The Ukrainian government has therefore involved the private sector in military preparations at an early stage. This is not surprising in light of the cyber-attacks on private IT infrastructures in the context of Russian hybrid operations since 2014 (Fabian, 2019). However, in most countries, this type of cooperation is far from trivial, as there are often constitutional obstacles to the national army carrying out internal defense activities in times of non-war. Countering hybrid operations is typically the responsibility of domestic organizations, in particular, intelligence services and often national CSIRTs (Computer Security Incident and Response Teams) operating within them.

A further difficulty for the involvement of civil companies in military cooperation in peacetime is the involvement of volunteers and the strengthening of their cooperation with professionals. As Conti and Raymond (2011) eloquently put it in their article on the leadership of cyber warriors: *"From our experience, cyber warriors are often independent and expect that their leaders are at least as bright and technically skilled as they. Many will have college degrees and professional certifications and take part in alternative hobbies and lifestyles. Contrast this with the physical prowess-centric kinetic* *warfare environment, where being the biggest caveman in the tribe is often enough to earn the respect of the led”.*

Because of the differences in mentality, therefore, only years of mutual trust-building can help to ensure that cybersecurity experts are present in the volunteer reserve system and that their skills can be used by the national army. In the case of Ukraine, this has taken many years since the beginning of the conflict in 2014. Mandatory conscription, including the appropriate use of the skills of conscripts, mutual interdependence in countering hybrid operations, and the adoption of Western command and control best practices all played a role in ensuring that there was a working relationship of trust between the Ukrainian army and the cyber security community at the outbreak of the war (Sosento, 2022).

### *2.2. Issues with Vital Cyber Intelligence Sharing*

Our national experience with national cyber defense also confirms that critical infrastructure is generally operated by private sector actors. Typically, their direct cyber protection is self-provided, with maximum reporting and cooperation obligations to national authorities, but without deep, operational-level knowledge of the critical information infrastructures operating in the state CSIRT or, in particular, the national army. Operational cyber defense is provided by in-house SOCs (Security Operations Centers) or external MSSPs (Managed Security Service Providers), possibly a hybrid of the two. Consequently, without the involvement of private sector actors, such critical information infrastructures cannot be protected. As pointed out by Davydiuk and Zubok (2023), the sharing of detailed cyber security information between critical infrastructure operators and public authorities is still only partially solved in war-torn Ukraine, where the legal framework is adequate, but there are practical difficulties at the technological and operational levels.

In addition to national cooperation, building links with global corporations is essential. In the case of Ukraine, there is documented involvement of several global IT corporations in the implementation of cyber defense from 2022, including active support from Amazon, Microsoft, and Google (Amazon, 2023; Google, 2023; Microsoft, 2022). This support is evident in two very important areas, which would not be possible without global players. Firstly, our experience shows that more and more global IT companies are building security operations centers with very high-quality cyber threat intelligence, typically better than that available in the nation-states. This CTI information can be purchased, but it is truly accurate when tailored to the needs of the specific country. It is this tailored cyber threat intelligence information that has helped enormously in preparing for Russian cyber operations. Second, as the Tallinn Manual 2.0 (2017) puts it, in Rule 103, *“means of cyber warfare are cyber weapons and their associated cyber systems”* (Schmitt, 2017). The defeat of cyber warfare thus depends to a large extent on the control of the infrastructures that the belligerents use. In today’s world, these are typically cloud-based systems, the largest global operators of which are the companies mentioned above. Thanks to their active defense activities, the infrastructural background of Russian cyber operations has thus been reduced, their attempts have become detectable and, by sharing CTI information and the modus operandi observed, detailed TTP (tools, techniques, procedures) have been made available to Ukrainian cyber defense.

### *2.3. Information Sharing with Non-Cybersecurity Parties*

The private sector is therefore emerging as a trusted source of information and a partner in understanding and addressing threats in cyberspace. However, they can also make a significant contribution to public perceptions of the conflict in this area, given that the information they produce is not necessarily classified and can be made public. This is particularly true of the OSINT (Open-Source Intelligence) community, which is playing a much more prominent role in the Russia-Ukraine war than before, and whose shares on social networks are even taken into account by official intelligence organizations. This is highly unusual in a war situation, where classical state information operations have a prominent role in strategic communication through which the state can shape the narrative of the war. There is thus a conflict of interest between the communication between states and private actors, which is also reflected in the cyber operational space. Indeed, an actor may not necessarily know which state cyber operation is being disrupted by the CTI or OSINT information it discloses. Therefore, the question is how to involve private actors, often operating in other countries, in the sharing of classified information and how to control the online disclosures of non-state actors? (Schmuki, 2023). This has not been addressed at the national or European level and is a serious obstacle to the expansion of military-civil cooperation in the field of cyber defense.

The issue of sharing classified information also arises for companies that generally do not have sufficient information on cyber threats and are not part of existing partnerships that would allow access to such information. In particular, private companies with low cybersecurity preparedness because they have not previously been forced to build protection for their systems, either because of the lack of legal compliance or real cyber threats. Specifically, we should think about the fact that supply chains have become very extended during wartime, as many small and medium-sized companies provide products and services to the military. These European and American companies are significantly exposed to Russian cyber operations during the war, which they have not had to face before (Joint Cyber Advisory, 2022).

Finally, we must not forget that a significant part of the technologies used in cyberspace can also be considered dual use. Today, we see a breakthrough in artificial intelligence-enabled cyber defense products that can also help militaries, which, without the latest advances in cyber security, find it harder to defend themselves and less able to sustain successful offensive operations in cyberspace. However, understanding the potential and limitations of these technologies requires strengthening the civil-military dialogue. Defense innovation is very important, but in many cases, there are cultural barriers to companies, primarily in the civilian domain, being able to work closely with military experts and mutually recognize the potential of technological advances.

These are just a few examples of the prominent role of civil actors in cyber operations. It is therefore essential to consider how international military law should relate to non-state actors in cyberspace. Of course, it is well known that international law applies in cyberspace, as highlighted in the 2014 NATO Wales Summit Declaration and the Tallinn Manual 2.0, which deals in detail with most of the issues raised above, but the reality of the Russia-Ukraine war shows that what is clear in theory can be questionable in practice, for example, the issue of cyber operations on neutral territory, which is prohibited by Tallinn Manual Rule 151 but is still frequently used in practice due to the proliferation of cloud technology (Schmitt, 2017). As the revision of the Tallinn Manual has already started within the NATO CCDCOE, it is hoped that version 3.0 will also propose a reassuring resolution of the practical issues of international law of war in the context of the Russia-Ukraine war.

## 3. EU Actions to Involve the Private Sector in Cyber Defense

There is no state of war in the Europe Union, so national constitutions do not currently allow armies to force cooperation from private sector actors in the EU member states. There are also limited possibilities to encourage voluntary cooperation. This is why the legislative steps taken by the European Union in the field of cybersecurity are very important and could create the appropriate basis and obligation for the involvement of market players in national cyber defense, as the need for the involvement of civilian entities in the national and European cyber defense can be derived from European and national security and cybersecurity strategies. The key regulators and initiatives of the European Union are the following:

– **The Strategic Compass for Security and Defense**: The Strategic Compass requires the EU member states to boost their intelligence analysis capacities and help to substantially enhance their defense expenditures to match the EU's collective ambition to reduce critical military and civilian capability gaps and strengthen the European Defense Technological and Industrial Base (European Union External Action, 2022).

– **The EU Cybersecurity Strategy**: One of the main objectives of the Strategy is to strengthen cooperation between national military and civilian Security Operation Centers and to test the adaptation of the latest technologies that will contribute to the creation of the EU network of AI-enabled SOCs, the European Cybersecurity Shield. The widespread adoption of cybersecurity technology objectives is carried out through dedicated support to SMEs under the Digital Innovation Hubs (European Commission 2020).

– **NIS2 Directive**: Although the issue of critical infrastructure protection in a wartime situation is not mentioned in this Directive, with the implementation of NIS2, a central forum for discussion among the relevant organizations will be established and there will be an opportunity for a wider discussion of the national and European cyber defense. Specifically, the establishment of National cyber crisis management frameworks as described in Article 9 of the Directive and Article 13 Cooperation at a national level will actively support the preparedness. Article 29 Cybersecurity information-sharing arrangements also reflect a vital element of cooperation between the states and private entities. Mutual assistance under Article 37 can strengthen the wider cooperation of EU member states (European Parliament and the Council, 2022).

– **The EU Cybersecurity Act**: One of the main objectives of this Act is to strengthen national and regional cooperation and share relevant information through ENISA (European Union Agency for Cybersecurity). As there is a Proposed Regulation on 'managed security services' amendment of this Act, the public-private cooperation is also relevant here (European Parliament and the Council, 2019).

– **The EU Cyber Solidarity Act**: the proposed legislation specifically addresses many of the issues described above, i.e. how a country should respond to a large-scale cyber security crisis and how to create cooperation between public and private SOCs and CSIRTs. The national and regional view of this Act can be easily complemented with military defense options, so that it can contribute greatly to the national adaptation of the legislation and the building of the European Cybersecurity Shield. The Cybersecurity Incident Review Mechanism described within the legislation will also be important in the context of the national de-barring of information sharing (European Commission 2023a).

– **Horizon Europe and European Cyber Security Organization**: There are plenty of completed or ongoing Horizon Europe research projects whose technical results can assess as dual-use cybersecurity products. Although the military usage of Horizon Europe results is not a key goal, in such a situation an extended usage can be acceptable. Through ECSO members, which are private companies, the existing European cybersecurity solutions can also be analyzed in this context (European Commission 2024).

– **EU Cybersecurity Skills Academy**: The Academy was set up to support cybersecurity skill development in Europe. Therefore, direct cyber-military training can be initiated to involve cybersecurity professionals in the national cyber defense (European Union, 2023).

– **Cybersecurity Competence Centre and Network**: In cooperation with the National Contact Points, member states can make a significant contribution to the networking of the European cybersecurity stakeholders in line with European objectives and to the use of the experience of other Member States, including military-related issues (ECCC, 2024).

It is not easy to finance pan-European defense either in a way that gives private actors direct access to resources to develop their capabilities and, through them, an interest in cooperating with public actors. This is particularly difficult to achieve in the field of military defense. This is why the Digital Europe Program is of particular importance, as it offers a particularly interesting financial solution to support the private sector and to cooperate with government bodies. The need for national cyber defense involving private actors is even clearer from the Digital Europe Program 2023-2024 overall work program, as follows:

– **Strengthen the preparedness of the key sectors and response actions across the EU to cyber threats.** By removing legal, technical, and human resource barriers in national cyber defense, Europe's preparedness for both military and critical infrastructure cyber defense perspective will be strengthened, and the response capability will be improved both within and outside its borders.

– **Further support the excellence of EU education and training institutions in digital areas to improve the capacity to nurture and attract digital talent through specialized education programs in advanced digital technologies, and, for example, in areas of cybersecurity and semiconductors.** The results of the relevant projects can make a significant contribution to the further development of the already existing cybersecurity master programs, to help overcome the cybersecurity workforce shortage, especially in the civil service in European countries, and to be in line with European initiatives such as the European Cyberskills Framework.

– **Further invest in the uptake of blockchain in Europe and in building of efficient and interoperable digital public services, as well as in building confidence in digital transformation and developing reference framework addressing urgent needs in energy consumption.** The goal of sharing CTI information securely and reliably between stakeholders is essential. With the review of previous EU-funded developments, interoperable digital public services can be developed for efficient CTI sharing.

Some key objectives of the Digital Europe Program 2023-2024 cybersecurity-specific work program also have a supportive effect on cooperation between civil companies and the military.

– **Support joint actions in order to create an advanced (state of the art) threat detection and cyber incident analysis ecosystem by building capacities of Security Operation Centers (SOCs).** Such projects allow for strengthening cooperation between civil and defense SOCs, including the sharing of CTI information and the use of the latest technologies.

– **Contribute to improving the prevention, detection, analysis, and capability to learn and respond to cyber threats and incidents by providing additional means and better interplay amongst cyber communities to support preparedness (ex-ante), and response (ex-post) to large-scale cybersecurity**

**incidents via Cybersecurity Emergency Mechanism.** This objective allows the identification of legislative and technological options to enable deeper prevention, detection, and analysis cooperation between military and law enforcement organizations and civil critical infrastructure operators at national and European levels.

– **Support cybersecurity capacity building at national and, where relevant, regional and local levels through National Coordination Centers which will aim at fostering cross-border cooperation and at the preparation of joint actions as defined in the Regulation (EU) 2021/887.** Such projects can strengthen the non-military but governmental national and European capacities, which can serve as a base for military cooperation as well.

– **Support the industry with a strong focus on helping SMEs and start-ups in complying with regulatory requirements, especially the NIS2 implementation or requirements concerning the proposed Cyber Resilience Act (Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020).** The strategic goal of the EU is to involve local SMEs and start-ups in defense developments, which enables the potential to understand the relevant products' dual-use nature (European Commission 2023b).

Overall, the European Union offers European Member States and private actors with an interest in cybersecurity a legal and funding framework that can provide a good basis for effective military and civilian cooperation. At both the national and NATO levels, it is worthwhile to take note of this particular situation and to exploit the synergies that the experience of the Russia-Ukraine war in cyber operations has demonstrated.

## 4. Conclusion

My hypothesis is backed up by a wealth of research and practical case studies. It is no coincidence that European policy has also recognized the importance of civilian-military cooperation. However, as a conclusion to my study, to launch an academic debate and to support the detailed implementation of policy objectives, I would like to identify five key challenges that need to be addressed to enable private actors to cooperate effectively with the military. These are the following:

– Challenge 1: The cyber defense of critical infrastructures is typically provided by civilian service providers that are not closely linked to military or civilian governmental cyber defense organizations, and therefore in specific situations, such as war, practical cyber defense of these critical infrastructures is not sufficiently effective.

– Challenge 2: The majority of the best cybersecurity experts and the civilian companies that employ them have no connection to the military, which means that in a war situation, the protection of national cyberspace and potentially the effectiveness of active operations is not the most effective.

– Challenge 3: Today's information technology revolution, e.g. the emergence of artificial intelligence, opens up new perspectives in cyber security, but the application of these technologies in national cyber defense, whether military or civilian, will only become feasible after a longer period in medium-sized countries, which are therefore more exposed to cyber-attacks than other, larger and richer powers.

– Challenge 4: Information sharing on incidents is not only not working smoothly at the European level, but also at the national level, which is an obstacle to more effective national and European cyber defense.

– Challenge 5: Only a fraction of the potential of bilateral and regional cybersecurity cooperation is exploited, and national cyber capability development typically does not take into account the experience of other countries.

Over the past decade, there have been many studies and research to address these challenges, but very few real good practices can be found. In addition, these resources are not typically focused on the situation in medium and small countries, so they are certainly not fully adaptable to these regions. Therefore, as a continuation of my research, my objective is to examine how the private sector can effectively contribute to the implementation of national military cyber defense and offensive capability development at the national and central European regional level.

**Acknowledgments**

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

## REFERENCES

Amazon. (2023). *Amazon's cybersecurity assistance for Ukraine*. Amazon. Available at: https://www.aboutamazon.com/news/community/amazons-cybersecurity-assistance-for-ukraine.

Conti, G., & Raymond, D. (2011). *Leadership of Cyber Warriors: Enduring Principles and New Directions*. Small Wars Journal. Available at: https://smallwarsjournal.com/blog/journal/docs-temp/811-contiraymond.pdf.

Davydiuk, A, & Zubok, V. (2023). Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War. *15th International Conference on Cyber Conflict: Meeting Reality,* 121-140. DOI:10.23919/CyCon58705.2023.10181813.

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Commission. (2023). *The EU Cyber Solidarity Act.* European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

European Commission. (2023). *The DIGITAL Europe Programme – Work Programmes*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital.

European Commission. (2024). *Shaping Europe's digital future*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

European Cybersecurity Competence Centre. (2024). *The European Cybersecurity Competence Centre*. ECCC. Available at: https://cybersecurity-centre.europa.eu/index_en.

European Parliament and the Council. (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*. European Parliament and the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881.

European Parliament and the Council. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148*. European Parliament and the Council. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555.

European Union External Action. (2022). *A Strategic Compass for Security and Defence.* European Union External Action. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en.

European Union. (2023). *Cybersecurity Skills Academy: a coordinated approach to boost the EU cyber workforce*. European Union. Available at: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.

Fabian, S. (2019). The Russian hybrid warfare strategy – neither Russian nor strategy. *Defense & Security Analysis, Vol. 35, Issue 3*, 308-325. DOI: 10.1080/14751798.2019.1640424.

Fleming, J. (2022). *RUSI Annual Security Lecture 2022*. GCHQ. Available at: https://www.gchq.gov.uk/speech/rusi-asl.

Giles, K. (2023). *Russian cyber and information warfare in practice*. London: Chatham House. ISBN: 978 1 78413 589 8. DOI: 10.55317/9781784135898.

Google. (2023, February 24). *Updates on our support for Ukraine*. Google. Available at: https://blog.google/outreach-initiatives/public-policy/updates-google-support-for-ukraine/.

Joint Cyber Advisory. (2022, April 20). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. U.S. Department of Defense. Available at: https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF.

Joyce, R. (2023, April 23). *State of the Hack 2023*. RSA Conference 2023. Available at: https://www.rsaconference.com/library/presentation/usa/2023/state%20of%20the%20hack%202023%20%20nsas%20perspective.

Kaushik, A. (2023). *Ukraine's cyber defence: Insights on private sector contributions since the Russian invasion*. GlobSec. Available at: https://www.globsec.org/what-we-do/publications/ukraines-cyber-defence-insights-private-sector-contributions-russian.

Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. ISBN: ISBN 978-1-107-17722-2.

Schmuki, Y. (2023). The Law of Neutrality and the Sharing of Cyber-Enabled Data During International Armed Conflict. In T. Jančárková, D. Giovannelli, K. Podiņš & I. Winther (Eds.), *15th International Conference on Cyber Conflict: Meeting Reality,* 25-38. CCDCOE Publications. ISBN: 978-9916-9789-3-1

Smith, B. (2022, June 22). *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Sosento, S. (2022). *The IT Army of Ukraine. Structure, Tasking, and Eco-System.* Center for Security Studies (CSS), ETH Zürich. DOI: 10.3929/ethz-b-000552293.