DANUBE
INSTITUTE

# Public-Private Cybersecurity Cooperation in Hungary

*Michelle Watson & Logan West*

February 2025

**Index**

## Executive Summary

Over the past several years, Hungary’s infrastructure has significantly grown in cyber-based capabilities. This has been enabled through the effective use of new, innovative technologies successfully implemented by government growth strategies and investments working efficiently with agile business organizations. However, this renaissance has been accompanied by new security risks and dangers inherent with these developments at a time when the world is becoming more chaotic. Following decades of relative geopolitical stability, the world today is marked by increased geopolitical conflicts. In the digital realm, the consequences of this instability are the growing power of cybercriminals, a rise of nation-state adversaries’ attacks on critical infrastructure, increasingly sophisticated cyber threats, rapid advances in emerging technologies, and burgeoning attack surfaces. This has led to a cyberspace that is more dangerous and complex than ever before.[1]

The growth in Hungary’s portfolio of cyber-augmented infrastructure necessitates an upgrade of its cybersecurity structure. To this end, the cooperation of the public and private sectors in this industry plays a foundational role in successfully protecting Hungarian infrastructure and data. The agency and role of the private sector in cybersecurity is one that educates, advises, and equips the cybersecurity forces of governments through innovation that is only possible by an independent organization. Hungary has already had experience in the capabilities of private sector firms augmenting state level infrastructure, notably through Chinese investments. Hungarian firms such as 4iG have also contributed to Hungary’s technological advancement in the space and defense sectors. However, the nation’s modernization also includes new risks and threats for Hungary to content with domestically and internationally.

Hungary faces the conventional issues of cyber threat attacks when it comes to developing its infrastructure with hackers targeting state-level institutions and infrastructure. Additionally, Hungary’s security allies warn of is the infrastructure built by China, with whom NATO and the U.S. face with a high-level of tension, much to the chagrin of Hungary’s leadership. While this situation proves to be a challenge for international cooperation, the private sector offers solutions in advisory service in developing a roadmap towards a solution.

The private sector provides two primary benefits to successful execution of state-level cybersecurity: new tools for the detection and defense against cyber threats, as well as intelligence, analysis, and assessments to support the work of state security services. In the context of international cooperation, these assets are essential in ensuring that multinational partners have a clear threat picture assessment. The rise of disinformation that is spread through the cyber domain by state actors and their proxy agencies has proven to be one of the most dangerous threats faced by both the Hungarian and U.S. authorities in recent years. The threat is made more potent with the increase in global instability and decentralization of cyber capabilities. The private sector's ability to quickly adapt to such issues and maintain a neutral disposition will be critical in support of policymakers and national leaders in mitigation efforts.

When it comes to increasing the cybersecurity of Hungary's critical infrastructure, the country's international relationships need to work close in hand with all aspects of Hungary's security affairs. The nation's current relationships offer both challenges and opportunities when it comes to augmenting its security apparatus to meet the constant and increasingly sophisticated threats that cyber adversaries pose. These concerns are oriented primarily towards infrastructural security issues and the collateral effect on regional security assurance. The private sector provides opportunities to navigate this issue while concurrently supporting the development of Hungary's cybersecurity capabilities. This report will detail current challenges for Hungary's international security relations, the benefits of U.S.-Hungarian cybersecurity cooperation to the country, existing examples of such cooperation, and future recommendations for improving it.

## Cooperation and Contention between the U.S., Hungary, and NATO

Successful international cooperation in cybersecurity requires common platforms in organization as well as application. In the case of the relationship between Hungary and the United States, NATO continues to act as the foremost platform for collective cyber defence and security. Specifically, NATO's Cooperative Cyber Defence Centre of Excellence acts as the hub for strategy, technological development, and collective training for member nations. The institution acts as the center of gravity in terms of capability and knowledge for Europe and the U.S. as well as the primary method for developing and coordinating joint strategy.

Hungary's role in NATO is one that has been critical to the security and stability of the Central and Eastern European region. It will very likely continue to be so in the future. Hungary has taken numerous leadership roles such leading the aerial defence of the Baltic airspace in 2022 after the Russian invasion of Ukraine[2] and being a significant contributor and leader of military forces for the NATO peacekeeping force in Kosovo (KFOR).[3] This history of active participation at the forefront of multinational operations demonstrates both the agency of Hungary as a member of NATO as well as the potential for future platforms of cooperation. In the realm of cybersecurity, Hungary is also part of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), which functions as the fusion center of NATO's collective cybersecurity efforts. As the mission statement of the organization reads: "Our mission is to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defense research, training, and exercises covering the focus areas of technology strategy, operations, and law."[4] Hungary's membership in this forum demonstrates its desire for cooperation in cybersecurity and also presents an opportunity to support such a development of capabilities by the private sector. Such a partnership has already begun to develop.

On 9 December 2024, President-Elect Donald Trump hosted Prime Minister Viktor Orbán at his Mar-a-Lago estate. Among those participating was Hungary's Minister of Foreign Affairs and Trade Péter Szijjártó; Gellért Jászai, Chairman of the 4iG Group; Elon Musk, Founder and CEO of Tesla and SpaceX; and Mike Waltz, incoming National Security Advisor in the Trump administration. Discussions between President-Elect Donald Trump and Prime Minister Viktor Orbán included Hungarian space industry initiatives and opportunities for global technological cooperation. The official talks encompassed the 4iG Group's satellite program, potential SpaceX launch services, and broader avenues for commercial and technological partnerships.[5]

Cybersecurity has highlighted how increasingly interconnected our world has become. The importance for nations and industry organizations to work together to address the growing threats in cyberspace is paramount. As noted by the Interntional Journal of Cybersecurity on trends in 2024, "The United States and Hungary recognized the necessity of international collaborations by formulating several strategic partnerships to enhance their cybersecurity capabilities. These collaborations not only bolster the defense mechanisms of individual organizations but also contribute to global cyber resilience."[6]

**Needs of Hungary's Cybersecurity**

Hungary's cybersecurity needs are based in its growing profile of cyber-augmented infrastructure and the international relations connected to it. Hungary has experienced rapid development in telecommunications, artificial intelligence research and development, manufacturing, and logistics. With this rise in technological capability comes the large-scale production of data as well as rising demands for energy to power this infrastructure. Additionally, Hungary has also been targeted by hostile cyber actors. In November of 2024, the Hungarian government's defence procurement agency had its IT systems hacked by what was described by government officials as "a hostile foreign, non-state hacker group."[7] While the government claimed that no sensitive information was stolen, the case demonstrates Hungary's rising profile as a target for cyber attacks. The national government has taken steps to address cybersecurity needs with the development of the National Cybersecurity Strategy of Hungary in 2013 as well as a national coordinating body responsible for overseeing the nation's efforts: the National Cyber Security Coordinating Council (NCSCC). In its text, the National Cyber Security Strategy details five key objectives:

1) Building response capability: having efficient capabilities to prevent, detect, manage (respond to), address and correct any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage. To achieve these goals, the very first step was to establish the GovCERT-Hungary.

2) Creating a secure environment: providing appropriate protection for its national data assets, to ensure the operational safety of the cyberspace functions of its vital systems and facilities, and to have a sufficiently fast, efficient, loss-minimising correction

system in situations where a compromise occurs, which can also be used at times of a special legal order (i.e. emergency situations).

3) Applying international standards: ensuring that the quality of IT and communication products and services required for a secure operation of the Hungarian cyberspace reaches international standards, with special emphasis on compliance with international security certification standards.

4) Improving education: ensuring that the standard of cyber security education, training and research and development is consistent with international best practices, promoting the establishment of a world-class Hungarian knowledge base. The government declared a significant role for the National University of Public Service in this matter, operating as the main base of education, training and research in the field of information security.

5) Protecting the future generation: ensuring that the establishment of a secure cyberspace for children and future generations is consistent with international best practice.

What these five objectives demonstrate, specifically objectives 1, 3, and 4, is the prominence Hungarian national leadership places on cooperation with international allies such as NATO. These three specific objectives focusing on “capacity building,” “applying international standards,” and “education,” all of which point to a recognition of the necessity of integrating cybersecurity forces with those of their allies. What is also acknowledged in the text is that building the skills needed to confront the challenges that are constantly evolving in the cyber realm is crucial. It is here that the private sector offers the greatest benefit in the context of strengthening Hungary’s cybersecurity capabilities: supporting the standardization among allies that the National Cyber Security Strategy stipulates for Hungary’s security services and assisting in training forces. However, a point of contention with Hungary’s security allies will require addressing in order to fully implement that stronger cooperation between countries and implementing those standards of security: the issue of Hungary’s infrastructure built by China.

## Primary Challenges for U.S.-Hungarian Cooperation

The issues that face U.S.-Hungarian cooperation include those that are both technical and geopolitical in nature. The three most important of these issues are the differing U.S. and Hungarian outlooks on China, the rise of artificial intelligence utilization in cybersecurity, and the role of energy. The reason that three issues are the most paramount is due to the large-scale impact on both nations as well as the wider Center and and Eastern European region in economic and security affairs. These three key factors also impact the level of trust that will be invested in cyber infrastructure in terms of integrity both from a technical perspective as well as from a security perspective. The foundation of such trust will rely on whether U.S. and Hungarian leadership can come to a common vision and a roadmap for reach it.

### 1. *The China Factor*

The first challenge that needs to be overcome is developing a common understanding and approach for the U.S., Hungary, and NATO regarding how to approach China. The current disposition of the United States and most of its NATO allies is that China is a strong potential cybersecurity risk. The justification pointed is Beijing's ventures through proxy forces at hacking both private sector and government institutions as well as its efforts at building critical infrastructure overseas through the private sector.

In December 2024, FBI director Christopher Wray announced that dozens of telecommunications providers in several countries were hit by a hacking campaign led by Salt Typhoon, a well-known cybercrime group with Chinese ties. While in early 2024, an attack from Volt Typhoon, another alleged Chinese state-sponsored group targeting US critical infrastructure was disrupted. In response, the U.S. imposed sanctions as a punishment, however, the effectiveness of sanctions alone in deterring cyber attacks is limited. Sanctions can temporarily disrupt operations and impose financial costs, but they don't address the root causes of cyber threats. Director Wray detailed the situation as such:

*"The fact is, the PRC's targeting of our critical infrastructure is both broad and unrelenting," he said. And, he added, the immense size—and expanding nature—of the CCP's hacking program isn't just aimed at stealing American intellectual property. "It's using that mass, those numbers, to give itself the ability to physically wreak havoc on our critical infrastructure at a time of its choosing," he said.*[8]

Assessments by American leadership such as this one has led the United States to disengage China and its firms such as Huawei and ZTE in terms of building critical infrastructure and push its allies to follow suit.[9] However, Hungarian leadership has a different perspective regarding China's presence in Hungary.

Currently, China is the largest foreign director investor in Hungary, overtaking South Korea, Germany, and the United States. Much of this investment has been focused into state-level infrastructure as well as manufacturing ventures, specifically in the automotive industry. The rapid development and deployment of next generation ICT infrastructure, such as the 5G telecommunications network, cyber-augmented and artificial intelligence (AI)-enabled manufacturing, logistics assets, and research centers are the result of significant Chinese-provided technologies and investments.[10] Notable achievements of these investments in the country have included the development of the nation's 5G telecommunications network as well as emergency management communications infrastructure. Logistical infrastructure has also made major advancements with cases such as the East-West Intermodal Terminal in eastern Hungarian village of Fényeslitke,[11] which is a newly completed freight terminal that utilizes artificial intelligence for executing operations. Along with Chinese investments, Hungary's recent signing of numerous memorandums of understanding with Beijing has raised concerns among U.S. and European leaders. Subjects of the memorandums include nuclear energy affairs[12] as well as joint policing efforts.[13]

Such developments have made U.S. and European leadership concerned over security issues, but Hungarian leadership has stated that they see no such risk from infrastructure built by Huawei and other Chinese firms. Foreign Minister Peter Szijjarto also states that Hungary does not wish to see NATO become an "anti-China bloc" and that European efforts to "de-risk and de-couple" from China would be "economic suicide."[14] The impasse over how to approach Chinese investments will remain a continued challenge that Hungarian, U.S., and NATO leadership will need to resolve in order to pursue stronger security relations and cooperation.

### 2. *The Rise of Artificial Intelligence in Cybersecurity*

Artificial Intelligence (AI) and Machine Learning (ML) have been at the forefront of technological advancements for years, and their impact on cybersecurity is profound. Yet, the rise of AI also presents compelling challenges, such as the following:

- The rapid adoption of AI introduces new vulnerabilities and lack of oversight. While there are numerous and growing AI tools being widely implemented across all aspects of organizations today, many of these AI tools are ungoverned. Governing AI is emerging as a new risk that needs to be better managed and tailored according to an organization's needs and risk appetite.

- AI-enabled automated hacking tools, AI-driven phishing campaigns, GenAI and deepfake technologies are becoming common, making it imperative for cybersecurity professionals to recognize, repel and respond to these attacks sooner.

- In 2025, AI-driven proactive and defensive cybersecurity solutions will be more prevalent and effective, enabling increased real-time threat detection and response. AI systems can analyze vast amounts of data, identify patterns, and predict potential threats with remarkable accuracy. These AI tools are crucial to countering sophisticated AI-enabled cyber attacks that traditional methods might miss.

Cyber criminals are leveraging AI tools to develop more advanced attack vectors. For example, in 2024, there was an exponential increase in cyber adversaries' use of AI in social engineering based cyber attack campaigns to interfere with elections. Nation-states took advantage of generative AI to level up influence operations. As voters in over 70 countries went to the polls, influence operations from China, Russia, and Iran used generative AI tools to expand content production and reach. All three nations continue investing in GenAI research.[15] Meanwhile, approximately 66% of organizations expect AI to have the most significant impact on cybersecurity in 2025 but only 37% report having processes in place to assess the security of AI tools before deployment. This reveals the paradox of the gap between the recognition of AI-driven cybersecurity risks and the rapid implementation of AI without the necessary security safeguards to ensure cyber resilience.[16]

### 3. *The Role of Energy*

Energy strategy and management will be a key element of security that will concern the public-private cooperation in Hungary and the wider Central and Eastern European region. The technological advancements in cyber-augmented infrastructure such as telecommunications and logistics, as well as manufacturing ventures in Hungary's growing automotive and military industry sectors, are the assets that will be most concerned with energy assurance. As 4iG details, the push for Hungary's industrial sectors to modernize is due to the technical and informational needs of their international clients and partners. This effort is made in order to interface with global systems and meet international standards.[17] As a result, energy prices rise due to the higher demand that comes with modern technology. Consequently, the function of energy management rises in prioritization as a cornerstone element of national security.

Currently, Hungary's energy infrastructure and relationships are in transition. Russia has a long history of providing energy resources, mostly non-renewables such as oil and gas, to Hungary and the wider region with low prices thanks to its geographic proximity and resulting simpler logistics. However, the Russo-Ukraine War has turned the vast majority of Europeans against continued business with Moscow, prompting political leadership to pursue new resources and relationships. While Hungary has taken a less-than-popular position of continuing energy relations with Russia to a certain level, the nation's leadership has actively pursued alternative energy infrastructure platforms such as as the Black Sea Electric Project as well as signed an MOU with China for potential nuclear energy cooperation. These new initiatives, and the accompanying new infrastructure, are ones that will utilize newer technology that takes advantage of cyber capabilities for the purposes of energy management and security.

An example of the cybersecurity challenge concerning energy infrastructure at hand is the recent effort to upgrade the infrastructure of the Paks nuclear station. Hungary's Paks station is a Russian-built reactor, the nation's only one, which is currently undergoing an expansion project called Paks II so that the facility may meet the nation's rising energy demands. With the Russo-Ukraine War ongoing at the time of this upgrade, concerns from NATO began to grow over the security of the facility given the tensions between Russia and the West over the war. The fear was that given the energy facility was Russian-built it could act as a Trojan Horse for potential hostile action on the part of Moscow. However, given no viable alternative existed for Hungary to take in place of Paks II, Budapest still sought to pursue its construction. Given both the security and energy needs, a compromise was sought and found in the form of the facility's control systems. It is here that the public-private cooperation offered a solution. The French firm Framatome provided new control systems for the facility, which would negate security concerns, given that firms was from a fellow NATO member state.

As explained by the Warsaw based Centre for Eastern Studies (OSW), "France's role in the implementation of the Paks II project has grown since 24 February 2022. It has been assumed since 2019 that the automated process control systems (ACS TP) will be supplied by Framatome. This German-French consortium provided this type of equipment for the needs of Paks I, which has four operating reactors. However, it turned out in January this year that Berlin had refused to grant permission to Siemens Energy to supply components for the new power plant; politicians from the Green Party insisted on this due to the Russian invasion of Ukraine. Hungary therefore sought to give the French part of the company a greater role in the project. Orbán and Macron discussed this in Paris in March this year while Szijjártó was visiting the Flamanville Nuclear Power Plant; one month later the French government approved of Framatome's participation in the joint project with Rosatom."[18] In this scenario, a public-private partnership was able to navigate the political complexities of the situation and provide the technical solutions needed to support Hungary's energy infrastructure needs while also providing a solution to security concerns. Such an example demonstrates the utility of the public and private cooperation in meeting both technical needs and political and security concerns.

**Existing Collaborations of U.S.-Hungarian Public-Private Organizations**

When it comes to meeting the joint challenges to both the U.S. and Hungary in cyber affairs, a number of potential collaboration platforms already exist. These organizations focus their cooperation around elements such as training, monitoring and threat detection, enhanced security software, and other related services. These efforts between American and Hungarian firms can potentially serve as the foundation to build future cooperation in cybersecurity. Below are the current platforms that exist for such cooperation:

- Balabit and Palo Alto Networks — Balabit, a Hungarian company known for its privileged access management solutions, has joined forces with Palo Alto Networks, a renowned American corporation and currently the largest cybersecurity company in the world. This partnership focuses on integrating Balabit's session monitoring and analytics with Palo Alto Networks' next-generation firewall technology. The combined solution offers comprehensive security for enterprises, ensuring that privileged accounts are monitored and protected from unauthorized access.[20]

- Kurtis & Co. and CrowdStrike — Kurtis & Co. is a leading Hungarian cybersecurity firm which first partnered with the American security giant CrowdStrike in early 2024. This collaboration aims to leverage CrowdStrike's advanced threat intelligence platform to enhance Kurtis & Co.'s ability to detect and mitigate cyber threats. Through this partnership, the companies have developed a joint threat intelligence-sharing system that provides real-time alerts and analysis, significantly improving their clients' security postures.[21]

- Avatao and IBM Security — Avatao is a Budapest-based cybersecurity training platform that collaborates with IBM Security to deliver state-of-the-art training programs for cybersecurity professionals. The partnership leverages Avatao's interactive training modules and IBM's extensive security expertise to provide tailored training solutions for organizations worldwide. In 2024, they launched a series of joint webinars and workshops aimed at upskilling cybersecurity teams and enhancing their ability to respond to sophisticated cyber threats.[22]

- VirusBuster Ltd. and Symantec — VirusBuster Ltd., a Hungarian antivirus software company, has entered into a strategic alliance with Symantec, a global leader in cybersecurity software and services. This collaboration focuses on integrating VirusBuster's malware detection algorithms with Symantec's endpoint security solutions. The result is a robust defense mechanism that offers enhanced protection against the latest malware and ransomware attacks. Together, they have also established a joint research and development center in Budapest to innovate and develop new cybersecurity technologies.[23]

## Recommendations

What must be recognized is that cybersecurity is much more than a set of technical challenges, it is a fundamental issue of national security, economic security, resilience, and global leadership. Cybersecurity requires a whole-of nation approach and falls under the authority and responsibility of governments and industry organizations to realize. Through a cooperative approach between the U.S. and Hungary focusing on joint security and benefits, such needs can be realized.

The following recommendations are a compilation from various U.S. sources, with a special endorsement of the Cyberspace Solarium Commission and the report by the McCrary Institute for Cyber and Critical Infrastructure 2024.[19]

1. *Create Global Solutions* — International leadership will be crucial. The United States must not only secure its own digital assets but also work to shape a global cyberspace that reflects our shared values and interests. Engage internationally to build a coalition of like-minded nations committed to a free, open and secure cyberspace.

2. *Establish a multi-agency commission or task force to streamline and coordinate cyberspace regulations* — Diplomatic, Economic, Military, Industry Resources; enable seamless coordination across all levels of government and private sector.

3. *Skilled Workforce Development and Readiness* — The shortage of skilled cybersecurity professionals is a critical vulnerability and we must invest in developing a highly skilled cyber workforce to meet the challenges of 2025 and beyond.

4. *Critical and Emerging Technologies* — Innovation and technologies like AI, quantum computing, 5/6G are reshaping our digital landscape and we must ensure that cybersecurity is built into these systems.

5. *Chain Supply Assurance* — Enhance supply chain security for all critical infrastructure industries

6. *Strengthen Public-Private Partnerships to leverage the full spectrum of a nation's capabilities* — Create a summit of industry leaders to support the public-private partnerships and develop concrete plans for enhancing the security of critical infrastructures.

Each of these sectors offer opportunity for U.S.-Hungarian collaboration in the interest of security current and future assets and critical infrastructure. In order these tenets to be realized, cooperation will be needed not only at the policy level for both countries, but also for private industry. While the national government of the United States and Hungary are now better positioned for a cooperative relationship with the inauguration of President Trump's second term, a number of cooperative platforms already exist in the private sector that can be utilized in international cyber affairs.

**Conclusion**

The rise of cyber-augmented infrastructure provides a multitude of opportunities to Hungary, the United States, and the wider region in terms of join prosperity and strategic security cooperation. However, should the geopolitical and technical challenges not be addressed in both policy and practice, such benefits may never come to fruition. With the newly elected Trump administration in Washington D.C. and the currently Orban administration in Budapest on such familiar terms, the opportunity for such a collaboration is ripe. What political outlook divergences may exist, such as those over how to approach China, are more likely to be overcome with such administrations currently in place thanks to their friendly disposition. Additionally, focusing on joining ventures such as energy, artificial intelligence development, and regional security ensure that the work of the relationship has an outcome in which both nations share profit and other benefits. Through a clear vision being developed and pursued by cordial American and Hungarian political leadership, both nations will position themselves as leaders of the developing world of cyber affairs rather than be at its mercy.

**Endnotes**

[1] World Economic Forum, (2025) "*Global Cybersecurity Outlook 2025*," https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 03 January 2025).

[2] NATO, (2022) "*Germany, Hungary, Italy take up NATO's Baltic Air Policing (2022)*," https://www.nato.int/cps/en/natohq/news_198102.htm (Accessed: 31 January 2025).

[3] NATO, (2023) "*Meet Lieutenant General Ferenc Kajári, the First Hungarian KFOR Commander*," https://www.nato.int/cps/ge/natohq/news_225746.htm?selectedLocale=en (Accessed: 31 January 2025).

[4] NATO, "*CCDCOE-About Us*," https://ccdcoe.org/about-us/ (Accessed: 31 January 2025).

[5] 4iG, (2024) "*A New Era of Hungarian-American Innovation Collaboration, Press Release*," https://www.4ig.hu/sw/static/file/press-release-12-10-24.pdf (Accessed: 11 January 2025).

[6] International Journal of Cybersecurity, (2024) *"Global Cybersecurity Trends 2024,"* vol. 9, no. 1, pp. 15-29.

[7] Komuves, A. (2024) *"Hungary's Defence Procurement Agency Hacked, Government says,"* Reuters. https://www.reuters.com/technology/cybersecurity/hungarys-defence-procurement-agency-hacked-government-says-2024-11-14/ (Accessed: 31 January 2025).

[8] Federal Bureau of Investigation, *"Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says"*, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says (Accessed: 01 January 2025).

[9] Cerulus, L. and Wheaton, S. (2022) *"How Washington chased Huawei out of Europe,"* POLITICO. Available at: https://www.politico.eu/article/us-china-huawei-europe-market/ (Accessed: 31 January 2025).

[10] West, L. (2023) *"Cyber Winds: The East Asian investments that fill Hungary's infrastructural sails,"* Hungarian Conservative. https://www.hungarianconservative.com/articles/politics/energy_infrastructure_independence_digitalization_automotive-industry_opening-to-the-east_5g/ (Accessed: 31 January 2025).

[11] Huawei. (2023) *"The world's first smart 5G railyard"* https://www.huawei.com/en/media-center/our-value/the-world-first-smart-rail-logistics-terminal (Accessed: 31 January 2025).

[12] Szandelszky, B. (2024) *"Hungary and China sign strategic cooperation agreement during visit by Chinese President Xi,"* AP News. https://apnews.com/article/chinas-xi-welcomed-hungary-talks-orban-0719880a351a5ef0763ae6a623a7798b (Accessed: 31 January 2025).

[13] Lee, L. and Woo, R. (2024) *"In unusual move, China offers to back Hungary in security matters,"* Reuters. https://www.reuters.com/world/unusual-move-china-offers-back-hungary-security-matters-2024-02-19/ (Accessed: 01 February 2025).

[14] Gilchrist, K. (2023) *"China decoupling would be an act of 'suicide' for Europe, Hungary's foreign minister says,"* CNBC. Available at: https://www.cnbc.com/2023/06/27/china-decoupling-would-be-suicide-for-europe-hungarys-pter-szijjrt.html (Accessed: 31 January 2025).

[15] Recorded Future, *"2024 Annual Report,"* https://go.recordedfuture.com/hubfs/reports/cta-2025-0128.pdf (Accessed: 01 Dec 2024).

[16] World Economic Forum, (2025) *"Global Cybersecurity Outlook 2025,"* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 11 January 2025)

[17] 4iG, (2024) *Industrial Challenges in Hungary*, *How to keep up with domestic and international developments?"* https://www.4ig.hu/it/how-to-keep-up-with-domestic-and-international-developments_ (Accessed: 03 February 2025).

[18] Gizińkska, I. and Sadecki, A. (2023) Russia's nuclear project in Hungary: France's growing role, OSW Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-07-04/russias-nuclear-project-hungary-frances-growing-role (Accessed: 31 January 2025).

[19] Cilluffo, F. *et al.* (2024) *Securing America's Digital Future: A Bipartisan Cybersecurity Roadmap for the Next Administration*, *Cyber Solarium Commission 2.0*. Available at: https://www.fdd.org/wp-content/uploads/2024/10/20241003-PTTF-Report.pdf (Accessed: 03 January 2025).

[20] Security Today Magazine, *"Balabit and Palo Alto Networks: A Strategic Alliance,"* April 2024.

[21] Cybersecurity News, "Kurtis & Co. and CrowdStrike Join Forces," March 2024.

[22] IBM Security Blog, "Avatao and IBM Security Collaboration Announcement," February 2024.

[23] Antivirus Weekly, "VirusBuster Ltd. and Symantec Partnership," January 2024.

## Bibliography

Cerulus, L. and Wheaton, S. (2022) How Washington chased Huawei out of Europe, POLITICO. Available at: https://www.politico.eu/article/us-china-huawei-europe-market/ (Accessed: 31 January 2025).

Cilluffo, F. *et al*. (2024) *Securing America's Digital Future: A Bipartisan Cybersecurity Roadmap for the Next Administration*, *Cyber Solarium Commission 2.0*. Available at: https://www.fdd.org/wp-content/uploads/2024/10/20241003-PTTF-Report.pdf (Accessed: 03 January 2025).

Government of Hungary. National Cyber Security Strategy of Hungary (2013) National Security Archive. Available at: https://nsarchive.gwu.edu/document/16333-government-hungary-national-cyber-security (Accessed: 31 January 2025).

Kaska, K. (ed.) (2015) National Cyber Security Organization: Hungary, NATO Cooperation Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2018/10/CS_organisation_HUNGARY_2015-10-12.pdf (Accessed: 01 February 2025).