

Chapter 6

Cyberthreats to the Science and Research Sector as a Challenge to National Security and Economic Competitiveness¹

IZABELA ALBRYCHT

AGH University of Krakow

Abstract: This chapter argues that escalating cyber-attacks against universities and research organizations have become a strategic challenge affecting national security and economic competitiveness. It links the sector's growing exposure to the industrialization of cybercrime and intensifying geopolitical techno-rivalry, emphasizing risks of disruption, data theft, and cyberespionage targeting intellectual property and dual-use research. The chapter outlines priority response measures, including EU-level research security initiatives, NIS2-driven compliance, stronger institutional governance, SOC capabilities, supply-chain risk management, and systematic cyber-resilience building within academia.

Keywords: cybersecurity; universities; research security; cyberespionage; intellectual property; hybrid threats; NIS2; cyber-resilience; SOC; supply-chain risk²

Introduction

In an era characterized by the widespread digitalization of public institutions and sectors of the economy, including universities and research organizations, the risk of unintentional disruption associated with the operation of a heavily interconnected and networked digital infrastructure is increasing, as is the

¹ Translated with the support of DeepL.com (free version).

² The keywords and abstract of this report is based on the text provided by the Author, but was generated by the Editors.

number of intentional malicious cyber-attacks. The latest statistics indicate an alarming surge in cyber-attacks targeting the academic sector. These incidents are becoming increasingly sophisticated, comparable with those targeting other critical infrastructure sectors, such as financial services and healthcare.

The Expanding Scope of Cyberthreats

The latest records indicate that in Q3 of 2024, the number of cyber-attacks worldwide has reached an all-time high, with a 75% increase compared to the same period in 2023.³ Data from the same report paints an alarming picture: “The Education/Research sector was the most targeted, with an average of 3,828 weekly attacks, followed by the Government/Military and Healthcare sectors, with 2,553 and 2,434 attacks, respectively.”⁴ These findings are corroborated by the 2024 Data Breach Investigations Report, which highlights that the education sector “was by far the most impacted, accounting for more than 50% of breached organizations.”⁵ The report analyzed 30,458 real-world security incidents and confirmed a record-high number of 10,626 data breaches, with 1,537 cases of confirmed data disclosure in educational services.⁶

For these reasons, cybersecurity has become a critical challenge for academic institutions, including universities, which are increasingly falling victim to cyber threats. In 2024, institutions such as the University of Cambridge, Università di Siena, Université Paris-Saclay, Reykjavik University, Berliner Hochschule für Technik, University of Winnipeg, Heinrich-Heine-Universität, Universitätsklinikum Brandenburg, Sveriges lantbruksuniversitet, Kansas State University, and South East Technological University Waterford Campus were among many affected by cyber-attacks.⁷ The types of cyber-attacks are varying but among the most wi-

³ Check Point Team, “A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide,” Check Point, October 18, 2024, <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/>.

⁴ Ibid.

⁵ Verizon, “2024 Data Breach Investigations Report,” 2024, <https://bakotech.pl/upload/file-uploads/files/2024-dbir-data-breach-investigations-report.pdf>.

⁶ Ibid.

⁷ Bert Kondruss, “Cyber attacks on universities,” <https://konbriefing.com/en-topics/cyber-attacks-universities.html>.

despread are ransomware attacks, password compromise, theft of email accounts, and phishing attacks.⁸

The rise in the number and sophistication of cyber-attacks poses significant threats to the confidentiality and integrity of sensitive data, including the financial information of institutions and the personal data of current and future leaders, professionals, and innovators. Not to mention one of the most critical targets: technological breakthroughs made by the academia. Additionally, cyber disruptions create significant operational risks, jeopardizing the daily functions of science and research organizations, which now rely heavily on digital systems, services, platforms, and infrastructure to educate, communicate, and innovate.

Global Factors Driving the Increase in Cyber-Attacks

Over the last few years, cybersecurity risks have intensified due to two main factors: the rise of a globally operating hacking industry and the escalating confrontation between global powers, with geo-tech⁹ rivalry between states as a critical element. The hacking industry has become increasingly professional, more innovative, and better organized, adopting a corporate-like structure. It has also begun offering hacking operations and tools in an “as-a-service” model.¹⁰ Cybercriminals are motivated not only by the potential economic benefits of targeting educational institutions but are also used as proxies by their states’ authorities. For some governments, cyber-attacks present an opportunity to disrupt critical public services in other countries and a means to extract cutting-edge technologies that enhance economic competitiveness and development, as well as support national security solutions. This explains why the hacking industry has become increasingly engaged in cyberespionage

⁸ Anna Maria Trawinska, Alicja Żok and Jakub Jaworski, “Cyberbezpieczeństwo sektora edukacyjnego,” *Biuletyn AGH*, December 2023, https://biuletyn.agh.edu.pl/home/biuletyn/wydania/2023/2023_PDF/189_12_2023.pdf.

⁹ Izabela Albrycht and Michał Rekowski, *Geopolitics of Emerging and Disruptive Technologies* (The Kosciuszko Institute, 2020).

¹⁰ Tamas Gaidosch, “The Industrialization of Cybercrime,” *International Monetary Fund*, June 2018, https://www.imf.org/en/Publications/fandd/issues/2018/06/global-cybercrime-industry-and-financial-sector-gaidosch?utm_source=chatgpt.com.

and even cyberwarfare.¹¹ Due to described geo-tech and geopolitical reasons, we have been also observing well-organized ecosystems being developed in many countries, including Russia, China, North Korea, and Iran, to support state-sponsored malicious cyber offensive activities of their governments and militaries, which is adding to that threat landscape even more concerning capabilities.¹² Escalating geopolitical confrontation, particularly evident since the Russian aggression against Ukraine in 2014 and 2022, has led to increased risks, with state-originated cyber-attacks being considered a key tool in hybrid warfare. These attacks are used to sow chaos and disrupt the normal functioning of Western countries and their critical entities. In the Council In recommendations on enhancing research security¹³ approved in May 2024, European decision-makers and policymakers emphasized that hybrid threats are affecting the research and innovation ecosystem, potentially leading to technology leakage. To address this, they stressed the need for proper and regular assessments, aimed at enhancing situational awareness among policymakers. This effort should be undertaken in collaboration with the Single Intelligence Analysis Capacity, particularly the Hybrid Fusion Cell, while also considering the contributions of the European Centre of Excellence for Countering Hybrid Threats, the European Union Agency for Cybersecurity, and the European Cybercrime Centre established by EUROPOL, especially regarding cybersecurity threats.¹⁴ The same conclusion was formulated by the British government after the review of the national security threats facing higher education perform at the beginning of 2024 and being presented at the security briefing for vice chancellors from twenty-four UK universities organized by the Deputy Prime Minister of the United Kingdom and attended by the Director General of MI5 and Chief Executive of the National Cyber

¹¹ Tyson Brooks, "The Professionalisation of The Hacker Industry," *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–99.

¹² Piotr Malachiński et al., "The hidden network. How China unites state, corporate, and academic assets for cyber offensive campaigns," *Orange Cyberdefense*, October 22, 2024, <https://research.cert.orange cyberdefense.com/hidden-network/report.html>.

¹³ Council of the European Union, "Council Recommendation on enhancing research security, 2024/0012 (NLE)," *Council of the European Union*, May 14, 2024, <https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf>.

¹⁴ Ibid.

Security Centre (NCSC).¹⁵ Among the many concerns to be addressed with special measures, the theft of intellectual property from academic research—particularly research with potential dual-use applications through cyber-attacks—was specifically highlighted.¹⁶

The growing importance of technologies for geopolitical and geoeconomic standing of the countries is making universities particularly vulnerable to diverse hybrid threats that include cyberespionage activities. The growing importance of technology for the geopolitical and geoeconomic standing of nations is making universities particularly vulnerable to diverse hybrid threats, including cyberespionage activities. Attacks on the academic sector, focusing on the theft of intellectual property and industrial espionage, are closely tied to rapid advancements in emerging and disruptive technologies.¹⁷ Technologies such as artificial intelligence (AI), quantum technologies, autonomous systems, biotechnologies, and many others serve as modern drivers of the economy while also having extensive applications in the military realm and defense industry. Innovations in these critical areas often become targets of cyberespionage before they can be patented. The Council of the European Union has warned that “some of the Union’s competitors are increasingly advancing their capabilities in this respect or actively pursuing civil-military fusion strategies.” This warning particularly relates to the long-term strategy pursued primarily by the People’s Republic of China. The threat is even greater from Russia, which, cut off from Western technologies due to sanctions imposed after its full-scale invasion of Ukraine in 2022, is increasingly turning to cyberespionage to bridge its technological gap.¹⁸ Therefo-

¹⁵ UK Government, “Government to launch new consultation to protect UK universities from security threats,” *GOV.UK*, April 26, 2024, <https://www.gov.uk/government/news/government-to-launch-new-consultation-to-protect-uk-universities-from-security-threats>.

¹⁶ Nathan Williams, “Foreign states targeting UK universities, MI5 warns,” *BBC News*, April 26, 2024, <https://www.bbc.com/news/uk-68902636>.

¹⁷ According to NATO definition emerging and disruptive technology areas are artificial intelligence (AI), autonomous systems, quantum technologies, biotechnology and human enhancement technologies, space, hypersonic systems, novel materials and manufacturing, energy and propulsion, next-generation communications networks. See more: https://www.nato.int/cps/en/natohq/topics_184303.htm (access at 16.07.2025).

¹⁸ Alexander Martin, “Fears grow of Russian spies turning to industrial espionage,” *The Record*, September 14, 2022, <https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage>.

re, the need to address “the risk of undesirable transfer of critical knowledge and technology to third countries, which might be used to strengthen these countries’ military capabilities and intelligence services, affecting the security of the Union and its Member States,” was also highlighted in the Council Recommendation.

An illustrative example of the current importance of technology for Western countries is the development of an innovation ecosystem for emerging and disruptive technologies initiated by NATO in 2019. This effort led, in 2022, to the establishment of the Defence Innovation Accelerator for the North Atlantic (DIANA), a NATO body aimed at fostering and protecting dual-use and deep technologies to support security and defense purposes. DIANA also plays a key role in fueling triple-helix collaboration among academia, government, and industry.¹⁹ The involvement of universities as accelerator sites affiliated with DIANA, including AGH University of Krakow,²⁰ Imperial College London,²¹ Universidad Politécnica de Madrid,²² Universität der Bundeswehr München,²³ provides yet another compelling argument to ensure they are protected and secure from external threats.

Responding to Cyberthreats

In response to these threats, systemic measures should be introduced based on a strategic approach clearly formulated at the European Union level and subsequently implemented by EU Member States. Universities and research organizations will soon need to comply with the NIS2 Directive.²⁴ As pre-

¹⁹ *The Defence Innovation Accelerator for the North Atlantic (DIANA)*, <https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana>.

²⁰ The Krakow DIANA Accelerator, the Polish site of NATO DIANA was created jointly by the AGH University of Krakow and Krakow Technology Park. See more: <https://diana.krakow.pl>.

²¹ Imperial College London serves as the DIANA Headquarters. See more: https://www.nato.int/cps/en/natohq/news_213288.htm?selectedLocale=en.

²² Universidad Politécnica de Madrid is the Spanish site of NATO DIANA. See more: <https://www.diana.nato.int/resources/site1/general/diana-affiliated-network-accelerator-sites.pdf>.

²³ Universität der Bundeswehr München is the German site of NATO DIANA. See more: *ibid*.

²⁴ “Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive),” *Official Journal of the European Union EUR-LEX*, no. 333 (2022): 80–152.

viously mentioned, the Council of the European Union is fully aware of the various threats targeting the research sector, including cybersecurity threats. Therefore, we can expect increased emphasis to be placed on addressing these challenges. The Council Recommendation on enhancing research security also called for strengthening “the evidence base for research security policy-making, through analysis of the threat landscape, including from a cybersecurity perspective.”²⁵ It also suggests regular interactions and collaboration aimed at facilitating “information exchange between research-performing organisations and research-funding organisations on the one hand, and intelligence agencies on the other hand, for example through classified and non-classified briefings or dedicated liaison officers.”²⁶ The document recognizes the threat as critical and emphasizes the need to develop or reinforce “cross-sectoral cooperation within government, notably bringing together policymakers responsible for higher education, research and innovation, trade, foreign affairs, intelligence, and security.”²⁷ Additionally, it proposes practical solutions for targeted institutions to build resilience in the sector, including “regular resilience testing and incident simulations, investment in dedicated in-house research security expertise and skills, assigning research security responsibility at the appropriate organisational levels, and fostering cyber hygiene and a culture in which openness and security are balanced.”²⁸

Universities should, where possible, allocate a budget to strengthen cybersecurity and build cyber-resilience. Cyber-resilience²⁹ is an increasingly important aspect of organizational resilience and can be achieved through measures that have been recommended for many years by cybersecurity experts and institutions. These include regular updates of software and systems, strong passwords and multi-factor authentication, regular data backups,

²⁵ Council of the European Union, “Council Recommendation on enhancing research security”.

²⁶ Ibid.

²⁷ Ibid.

²⁸ Ibid.

²⁹ “Cyber-resilience should be understood as a capability that a given enterprise possesses to manage a cyberattack and its effects in a way which retains the operational capacity”. See more: Izabela Albrycht, “Cyber-resilience,” *A Country's Systemic Resilience in the Digital Era*, ed. Izabela Albrycht, The Kosciuszko Institute, 2022, <https://cybersecforum.eu/2022/09/21/new-report-a-countrys-systemic-resilience-in-the-digital-era/> (access at 16.07.2025).

and educating employees to recognize phishing attempts and other cyber and ICT threats. Given the rise in the sophistication and frequency of cyberthreats, advanced threat detection and response systems, along with organizational changes, should be introduced. This includes establishing specialized units in universities to protect scientific and research infrastructure, such as laboratories, supercomputers, data centers, servers, and the data processed across numerous IT systems. Rectors should designate one of their deputies, such as a vice-rector, or appoint dedicated representatives responsible for these processes, granting them broad authority to oversee the cybersecurity system.³⁰

There is also a need to update relevant policies and procedures and establish new responsibilities among key decision-makers. As universities continue their digital transformation, they must develop robust cybersecurity policies and procedures, ensure these remain relevant to evolving threats, as well as conduct regular audits and risk assessments targeting the entire supply chain.³¹ Additionally, universities should perform cybersecurity exercises and implement regular training programs for scientists, researchers, staff, and students.

Many entities in the scientific and research sector are already taking steps to build so-called security operations centers (SOCs). For example, the Security Operation Center in Central Europe Region (SOCCER) consortium, which includes universities from five EU countries in the Central and Eastern Europe (CEE) region—Poland, Czechia, Slovakia, Estonia, and Lithuania—was established to support the development and advancement of SOCs within universities and Research and Technology Organizations (RTOs) in the region. The consortium has been awarded a grant from the Digital Europe Programme.³²

³⁰ Dariusz Szostek, "Cyfrowa perspektywa przed uczelniami i instytutami," *Forum Akademickie*, July 3, 2024,

^b<https://forumakademickie.pl/szkoly-wyzsze/cyfrowa-perspektywa-przed-uczelniami-i-instytutami/>.

³¹ A supply chain is a network of organizations, people, activities, information, and resources that work together to deliver a product or service from the initial stage to the hands of the end consumer or final business recipient. The supply chain includes companies that provide components to key or important entities essential to a given product or service. See more: <https://www.biznes.gov.pl/pl/portal/005120#6>.

³² "SOCCER – Cybersecurity for Academic Sector," AGH University of Krakow, accessed July 17, 2025, <https://soccer.agh.edu.pl/en/>.

Finally, it is essential to increase leadership involvement. University rectors must well recognize that the responsibility for the security and cybersecurity of their institutions ultimately rests on their shoulders. They should take steps to establish an effective management and coordination structure for this critical area of university operations. Cybersecurity considerations should also be a key criterion in the procurement process for ICT and network equipment, as well as in the selection of suppliers and business clients. This issue is underscored by the NIS2 Directive, which emphasizes the risks associated with high-risk vendors and the necessity of conducting third-party cyber risk management. At the same time, they should actively pursue opportunities to secure funding through government and EU programs. A dedicated fund is essential to systematically support the academic sector in developing competencies, resources, and tools to enhance cybersecurity. This could be modeled after existing programs supporting other sectors, such as Poland's "Cybersecure Local Government" (*Cyberbezpieczny Samorząd*) program, which provides targeted assistance to local government units.³³ However, there are many other examples of cybersecurity programs that could be explored and tailored to focus more on the cybersecurity of the Science and Research Sector. These include Programme d'Investissements d'Avenir (France), Plan Cyber (France), Nationale Roadmap Grootschalige Wetenschappelijke Infrastructuur (The Netherlands), and Piano Nazionale di Ripresa e Resilienza (PNRR) (Italy).

Conclusion

The outlook for the near future regarding cybersecurity in Western countries is not optimistic. This includes a significant increase in cyber-attacks targeting the science and research sector, among others. Addressing these challenges requires systemic measures supported by decision-makers and governments and implemented by academic leadership. The situation is further exacerbated by the malicious use of AI, which has already become a tool for cyber-attackers. AI enables them to scale and enhance their operations, such as executing advanced phishing campaigns and creating convincing

³³ "Cyberbezpieczny Samorząd," *Cyfryzacja KPRM*, accessed July 17, 2025, <https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-samorzad>.

deepfakes.³⁴ Undoubtedly, the global cybersecurity community is facing many problems and dilemmas, which will require international and inter-sectoral cooperation to be solved (or at least prepare for and counteract). It is crucial to seek opportunities to highlight the importance of cybersecurity of the research and education institutions to policymakers, decision-makers and other stakeholders. Perhaps the upcoming presidency of Poland in the Council of the EU and its priorities could be the next step towards more secure and resilient universities.

Policy Recommendations

1. Continuation of the direction set up within The Council Recommendation on enhancing research security, particularly through the creation of “cross-sectoral cooperation within government,” which should involve policymakers responsible for higher education, research and innovation, trade, foreign affairs, intelligence, and security.
2. Start counter measures in collaboration with NATO and the EU to address universities’ vulnerabilities to hybrid threats, including cyberespionage activities. These measures should include risk assessments, incident response protocols, and access to shared resources for threat intelligence.
3. Further support the NATO DIANA network’s development by ensuring its security against external threats within accelerators and test centers. Implement safeguards such as advanced threat monitoring systems and secure communication channels.
4. Introduce systemic measures based on a strategic approach clearly formulated at the European Union level, to be implemented by EU Member States. These measures should include proper public budget allocation to strengthen cybersecurity and build cyber-resilience across the sector.

³⁴ Aleksandr Yampolskiy, “What does 2024 have in store for the world of cybersecurity?,” February 15, 2024, <https://www.weforum.org/stories/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/>. See more: Izabela Albrycht, “Cyberbezpieczeństwo w erze sztucznej inteligencji”, in *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*, ed. Wioletta Brzęcka and Robert Siudak, The Kosciuszko Institute, 2022, no. 39, <https://ik.org.pl/wp-content/uploads/2023/11/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf>.

5. Provide instruments to help the sector comply with the NIS2 Directive, including guidance on risk assessment methodologies, security baselines, and compliance audits tailored to higher education and research institutions.
6. Support capacity building for research security policymaking by enhancing the evidence base through a thorough analysis of the threat landscape, including cybersecurity perspectives. This effort should include:
 - Specialized SOCs for advanced threat detection and response.
 - Cyber threat analysis based on Indicators of Compromise (IOCs).
 - Dedicated units to protect critical infrastructure.
7. Develop a cyber-resilience strategy within the sector's institutions, supported by clear political and administrative commitment from leadership, including vice-rectors or dedicated representatives. This strategy should result in updates to policies and procedures (e.g., procurement processes for ICT and network equipment) and establish new responsibilities among key decision-makers.
8. Promote collaboration with national cybersecurity agencies and relevant bodies to provide additional support for cybersecurity capacity building, particularly for small and medium-sized institutions.
9. Run awareness-building campaigns to promote cyber hygiene and foster a cybersecurity culture within the sector. These campaigns should target all stakeholders, including faculty, staff, and students, and focus on practical measures to prevent and mitigate cyber risks.

Bibliography

- AGH University of Krakow. Security Operations Center for Education and Research (SOCeR). <https://soccer.agh.edu.pl/en/>.
- Albrycht, Izabela. "Cyber-resilience." In *A Country's Systemic Resilience in the Digital Era*, ed. Izabela Albrycht. The Kosciuszko Institute, 2022. <https://cybersecforum.eu/2022/09/21/new-report-a-countrys-systemic-resilience-in-the-digital-era/>.
- Albrycht, Izabela. "Cyberbezpieczeństwo w erze sztucznej inteligencji." In *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*, editors

- W. Brzęcka and R. Siudak. The Kosciuszko Institute, 2022. <https://ik.org.pl/wp-content/uploads/2023/11/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf>.
- Albrycht, Izabela, and Michał Rekowski. *Geopolitics of Emerging and Disruptive Technologies*. The Kosciuszko Institute, 2020.
- Biznes.gov.pl. <https://www.biznes.gov.pl/pl/portal/005120#6>.
- Brooks, Tyson. "The Professionalisation of The Hacker Industry." *International Journal of Computer Science & Information Technology (IJCSIT)* 14, no. 3 (2022): 87–99.
- Check Point Research. *A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide*. <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/>.
- Council of the European Union. *Council Recommendation on Enhancing Research Security*, 2024/0012 (NLE). <https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf>.
- Council of the European Union. *Council Recommendation on Enhancing Research Security*. <https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf>.
- Cyfryzacja KPRM. *Cyberbezpieczny Samorząd*. <https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-samorzad>.
- DIANA Poland. <https://diana.krakow.pl>.
- European Union. *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*. *Official Journal of the European Union* L 333 (2022): 80–152.
- Gaidosch, Tamas. "The Industrialization of Cybercrime." *International Monetary Fund*, https://www.imf.org/en/Publications/fandd/issues/2018/06/global-cyber-crime-industry-and-financial-sector-gaidosch?utm_source=chatgpt.com.
- Kondruss, Bert. "Cyber Attacks on Universities." *KonBriefing Research*, <https://kon-briefing.com/en-topics/cyber-attacks-universities.html>.
- Malachiński, Piotr et al. "The Hidden Network. How China Unites State, Corporate, and Academic Assets for Cyber Offensive Campaigns." *Orange Cyberdefense*, <https://research.cert.orange cyberdefense.com/hidden-network/report.html>.
- Martin, Alexander. "Fears Grow of Russian Spies Turning to Industrial Espionage."

The Record, September 14, 2022, <https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage>.

NATO. *Imperial College London Serves as the DIANA Headquarters*. https://www.nato.int/cps/en/natohq/news_213288.htm?selectedLocale=en.

NATO. *NATO Topics: Defence Innovation Accelerator for the North Atlantic (DIANA)*. https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO. *Universidad Politécnica de Madrid is the Spanish Site of NATO DIANA*. <https://www.diana.nato.int/resources/site1/general/diana-affiliated-network-accelerator-sites.pdf>.

NATO. *Universität der Bundeswehr München is the German Site of NATO DIANA*. Ibid.

Szostek, Dariusz. "Cyfrowa perspektywa przed uczelniami i instytutami." *Forum Akademickie*, July 3, 2024, <https://forumakademickie.pl/szkoly-wyzsze/cyfrowa-perspektywa-przed-uczelniami-i-instytutami/>.

Trawińska, Anna Maria, Alicja Żok and Jakub Jaworski. "Cyberbezpieczeństwo sektora edukacyjnego." *Biuletyn AGH*, December 2023, https://biuletyn.agh.edu.pl/home/biuletyn/wydania/2023/2023_PDF/189_12_2023.pdf.

UK Government. *Government to Launch New Consultation to Protect UK Universities from Security Threats*. <https://www.gov.uk/government/news/government-to-launch-new-consultation-to-protect-uk-universities-from-security-threats>.

Verizon. *2024 Data Breach Investigations Report*. <https://bakotech.pl/upload/file-uploads/files/2024-dbir-data-breach-investigations-report.pdf>.

Williams, Nathan. "Foreign States Targeting UK Universities, MI5 Warns." *BBC News*, April 26, 2024, <https://www.bbc.com/news/uk-68902636>.

Yampolskiy, Aleksandr. "What Does 2024 Have in Store for the World of Cybersecurity?" *World Economic Forum*, February 15, 2024, <https://www.weforum.org/stories/2024/02/what-does-2024-have-in-store-for-the-world-of-cyber-security/>.