sciendo

Research Article • DOI: https://doi.org/10.25143/socr.29.2024.2.75-79 • 2024 • 29(1) • 75-79

Socrates

Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence

Vitālijs Rakstiņš[1], Karina Palkova*[1], Lidija Juļa[1], Natalia Filipenko[2]

[1]Riga Stradiņš University, Faculty of Social Sciences, Riga, Latvia, Vitālijs Rakstiņš; ORCID: 0009-0003-4353-5259, Karina Palkova; ORCID: 0000-0002-6909-571X, Lidija Juļa; ORCID: 0000-0001-5139-4642
[2]National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Department of Law, Kharkiv, Ukraine, ORCID: 0000-0001-9469-3650

Abstract

Academic as well as scientific institutions are essential for advancing knowledge and innovation, but they are increasingly susceptible to foreign interference, which can compromise research integrity, academic freedom and national security. Increased remote work and study, large data volumes and disruptive technologies like Artifitial intelligence I have created new avenues for cyber threats. This article aims to explore the cyber risks associated with foreign influence on academic institutions specifically and suggest effective mitigation strategies. Foreign interference can lead to unauthorized access to sensitive research data, resulting in espionage, manipulation and lost commercialization opportunities. Dependence on foreign digital systems heightens these risks, including the potential loss of access to research data stored in third-party clouds. Furthermore, cyber interference can disrupt academic work, impacting online learning platforms and administrative systems. Common cyber threats, such as cyber-technology attacks and insider threats, underscore the need for strong cybersecurity measures.

Keywords

academic institutions • cybersecurity • foreign interference

INTRODUCTION

Academic institutions play a critical role in the advancement of knowledge and innovation, but they are also increasingly vulnerable to foreign interference that can threaten academic freedom, research integrity, intellectual property and even national security. The increasing digitalisation of academic processes, with an unprecedented amount of remote working and studying since COVID-19, the huge amounts of data and disruptive technologies such as AI bring vulnerabilities and open up new vectors for foreign interference, in particular on cyber domain (Piazza et al., 2023). For instance, only data breaches in the higher education sector cost an average of $3.7M in 2023, not analysing the impact on R&D and commercialization opportunities (Schwartz, 2023). This research article examines the cyber risks of foreign influence on academic institutions and proposes mitigation measures. This article aims to explore the cyber risks associated with foreign influence on academic institutions specifically and suggest effective mitigation strategies. The methodology begins with a literature review to identify key vulnerabilities and risks. Risk assessments will evaluate threats such as unauthorized data access and dependency on foreign technology. The legal interpretation methods will be used to provide textual analysis to ascertain the meaning of the law, contextual examination to understand its broader purpose, historical review to uncover legislative intent, systematic analysis to ensure coherence within the legal framework, teleological interpretation to align with the law's objectives and comparative analysis to gain insights from similar jurisdictions.

Foreign influence poses several risks not only to academic institutions, including risks in the digital domain, both related to cybersecurity, but also to dependencies on foreign digital systems (hardware, software, know-how, data clouds, etc.), and as a result, could lead to:

1. Unauthorised access and research integrity interference, as foreign entities may access sensitive research data, leading to potential espionage, interference and manipulation (Ivanov, 2023), loss of commercialisation opportunities through loss of intellectual property and know-how (White House Office of Trade and Manufacturing Policy, 2018).
2. Loss of research findings or sensitive technologies or loss of control over confidential data, which may lead to sanctions.
3. Loss of access to research and academic data stored in third-party data clouds.
4. Disruptions to academic operations, such as interference with online learning platforms, and administrative systems, with a cascading impact on the delivery of curricula, and the education process.
5. Damage to reputation and the credibility of research.

The most common cyberthreats to higher education are

* Corresponding author: Karina.Palkova@rsu.lv

cybertechnology attacks (viruses, malware, DDoS attacks and so on) and human-centric attacks, including insider threats (National Cyber Security Center Report, 2021). The reason for the vulnerability of cyber security is the large attack surface, as the variety of devices, end-points and systems connected to the networks of higher education institutions increases the potential points of entry (Kost, 2024). The increasing use of cloud-based services and digital platforms, as well as ageing IT infrastructure, also contribute to the vulnerability. However, as noted above, one of the key risks is the cybersecurity awareness gap, as many faculty, staff and students lack sufficient awareness and training on cybersecurity best practices (Department for Science, Innovation & Technology. Official Statistics, 2023).

RESEARCH RESULTS AND DISCUSSION

The focus of the research will be on two themes, all hazard risk management, cyber and kinetic, business continuity and dependence on foreign technology, software, hardware, clouds, etc.

Comprehensive all hazard risk management system

Many academic institutions are under obligation to have in place risk management systems or systems that are in compliance with national regulations or international standards such as ISO 31000:2018 risk management standards or ISO 27000 cybersecurity series. The main challenges are related to the risk register (risk appetite1) and to integrating risk assessment at all organisational levels. Institutions seek to limit their risk appetite to those risks that are mandated by regulation.

At the same time, there is a growing understanding of the need for all-hazards preparedness, as any one of these risks (whether it be natural disaster hazards, hybrid warfare challenges, terrorism, armed conflict or anything in between) could have a disruptive effect on the institution's operations. As threats to the security of information systems can come from various sources, cybersecurity risk management measures should be based on an all-hazards approach, aiming to protect network and information systems and their physical environment from events such as theft, fire, flood, telecommunications or power outages or unauthorised physical access and damage (Directive (EU) 2022/2555, 2022). This is an evolving concept, for example, the European Union's NIS 2 Directive states that risk management measures should be based on an all-hazards approach through the implementation of appropriate and proportionate technical, operational and organisational measures to manage risks to the security of network and information systems. This does not only mean technical measures related to cyber security, but also general operational and organisational measures (Directive (EU) 2022/2555, 2022).

Cybersecurity risk-management measures also should address the various domains like physical and environmental security of information systems by including measures to protect such systems against system failures, human error, malicious acts or natural phenomena, address human resources security and have in place appropriate access control policies (Directive (EU) 2022/2555, 2022, Preamble 79 paragraph). Given the cybersecurity risks of foreign influence, academic institutions should not only adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management, or user awareness, but also enable broader compliance process and strategic dependency mapping of any partnership with third countries. Hostile foreign interference poses a challenge because it can manifest itself with clear intent, such as economic espionage or intellectual property theft (University Foreign Interference Taskforce, 2021). But it can also subtly undermine the scientific potential and capabilities of Western nations as part of grey zone or hybrid warfare (Braw, 2022).

In summary, the implementation of the all-hazards risk approach is beyond the scope of those responsible for specific risks and requires systematic oversight and systematic centralised coordination of compliance processes.

Second challenge is the integration of risk assessment on all organizational levels, for the academic personnel, administrative staff, students and visitors. As defined in the NIS 2 Directive, a culture of risk management should be promoted and developed, including assessing risks and implementing cybersecurity risk management measures appropriate to the risks faced (Directive (EU) 2022/2555, 2022, Preamble 77 paragraph). The evolving concept is also individual risk responsibility and even the individual responsibility of management for implementing an appropriate risk management system (Directive (EU) 2022/2555, Article 20, 2022). In summary, institutions should have risk-informed decision-making systems in place at all levels. This calls for education and training of academic and administrative staff, as well as students. This training should be comprehensive, covering broader risk management and cyber hygiene, understanding compliance requirements, etc.(Henry Jackson Society, 2023).

1 ISO 31000 standard risk appetite definition stated that 'Risk appetite refers to both the amount and type of risks an organization is willing to pursue, retain, or accept'.

Dependence on foreign technology, software, hardware, clouds, etc. Business continuity planning and resilience of supply chains

Foreign interference poses a significant risk to academic and research institutions through the disruption of their operations and supply chains. Ensuring business continuity planning and resilience is an important part of the protection of these institutions against such threats (International Organization for Standardization, 2019).

The concept of business continuity in this research is broader than just ensuring the backup and recovery of operations, but focuses on the continuity of the institution's essential functions, even in a contentious environment and during crisis. By developing business continuity system, academia can continue to access to essential services, data and resources even if foreign interference occurs.

One of the key elements of business continuity is the resilience of the supply chain. In the digital domain, supply chain security includes supplier or service provider resilience, taking into account the overall quality and resilience of products and services, their embedded cybersecurity risk management measures and their suppliers' and service providers' cybersecurity practices (Directive (EU) 2022/2555, 2022, Preamble 85 paragraph). In particular, academia and research organisations should be encouraged to incorporate cybersecurity risk management measures into the procurement and contractual arrangements they have with their direct suppliers and service providers (Directive (EU) 2022/2555, 2022, Preamble 85 paragraph).

The EU is protecting the supply chains of essential service providers by setting up non-tax barriers, such as the requirement for the EU certification system or an EU-accredited product (Directive (EU) 2022/2555, Article 2, 2022). For example, the NIS 2 Directive emphasises the obligation to use ICT products, ICT services and ICT processes that are certified according to European certification schemes for cyber security.

Other potential non-technical risk factors include undue influence by a third country on suppliers, particularly in the case of alternative governance models, hidden vulnerabilities or backdoors and potential systemic supply disruptions, particularly in the case of technological lock-in or supplier dependency (Directive (EU) 2022/2555, 2022, Preamble 90 paragraph).

Noble example is the EU's 5G Toolbox, a comprehensive set of guidelines for the security of 5G networks, which addresses both technical (cyber) and strategic risks in relation to cyber security and foreign interference in critical infrastructure (EU toolbox on 5G Cybersecurity 2020). For instance, the UK Government reviewed Huawei's role due to national security concerns on research partnerships with several universities to develop and explore 5G technology (Department for Digital, Culture, Media & Sport et al., 2020). Several countries, including the United States and certain European nations, have prohibited the use of equipment from Chinese companies like Huawei and ZTE due to concerns regarding potential foreign influence (The Clean Network. U.S. Department of State, 2021). This case underscores the significance of countries and scientific institutions carefully evaluating and managing their reliance on foreign actors and technologies to safeguard autonomy, competitiveness and resilience.

To protect academic freedom and research integrity, the universities should reduce dependence on foreign equipment, software, technologies, intellectual property and skills through the development of national scientific capabilities. To enhance supply chain security, institutions should institutionalise and establish a system to identify Tier 1 suppliers and their geographical distribution in order to anticipate vulnerabilities and alternatives, avoid single-source dependencies (discourage high-risk suppliers) and avoid suppliers with questionable reputations in the areas of privacy, human rights and national security (Henry Jackson Society, 2023).

Contributions in kind, such as donating equipment and technologies, or granting access to foreign data analytical capabilities for research purposes, carry inherent risks. While these contributions can provide valuable resources and expertise, they pose concerns regarding data security. For instance, the donation of equipment by Molecular Genetics Instrumentation (MGI) has sparked concerns regarding data security, intellectual property protection and the potential for foreign influence or access to sensitive research findings (Sharma and Black, 2021).

Indirect strategic dependencies on foreign technologies may not be immediately apparent but can have significant implications for scientific institutions and national security. For example, reliance on cloud computing services hosted by foreign companies or utilising software frameworks developed by foreign entities can create vulnerabilities and potential risks. There are several risks associated with storing research and academic data in third-party data clouds. These include the potential for data breaches, unauthorised access and a loss of control over the data. In addition, the availability and integrity of critical scientific information can be at risk in the event of service disruption or provider failure. There is also a growing risk of research's data poisoning (the deliberate manipulation of data that is used for research and machine learning purposes), leading to incorrect or misleading results. This risk makes it critical for institutions to implement robust data verification and security measures, as it can compromise the integrity of academic work (Rakstiņš et al., 2024).

CONCLUSION

Due to the complexity of digital ecosystem and its supply chains, the interdependencies between cyber and kinetic domains, academic institutions need to implement a systematic and structured comprehensive risk management system to minimise foreign influence:

Establishing clear policies at all levels, structuring them as an internal in-house risk-based control system, allocating resources and defining responsibilities.

Fostering a culture of risk awareness and ensuring adequate education and training for scientists, academic staff and employees are essential to raise awareness and understanding of the risks of hostile foreign influence, including cyber security risk assessment, data security and strategic dependencies on technologies.

Implementation of robust compliance processes, including thorough due diligence on the origin of the technologies they use, minimisation of critical dependencies on foreign equipment, software and technologies.

As part of their all-hazards preparedness, academic institutions must have a comprehensive business continuity system in place to ensure that they can quickly respond to and recover from cyber attacks and disruptions, maintain business continuity, and protect their critical functions and data.

There is a toolbox of measures to mitigate and minimize the risks of foreign influence, but it requires centralized oversight and compliance. A systematic approach requires greater commitment from the institution's leadership and staff at all levels, institutionalising the process of compliance and risk management, including procurement and international partnership.

ACKNOWLEDGEMENT

This research is funded by the Latvian—Ukrainian Joint Programme of Scientific and Technological Cooperation Project (2023) 'Best Practice University: Transformation and Adaptation Process in Challenging Environment', Project No LV_UA/2023/1

REFERENCES

Braw, E. (2022). The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression. Rowman & Littlefield. ⁋AEI Press, ISBN-10⁅: ⁋0844750409, SBN-13⁆: ⁋978-0844750408

Department for Digital, Culture, Media & Sport, National Cyber Security Centre, & Dowden, O. (2020, July 14). Press release: Huawei to be removed from UK 5G networks by 2027: Decision follows a technical review by the National Cyber Security Centre in response to US sanctions. Retrieved from: https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027

Department for Science, Innovation & Technology. (2023, April 19). Cyber security breaches survey 2023: Education institutions annex. Retrieved from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

European Commission. (2020). EU toolbox on 5G cybersecurity. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

European Parliament & Council of the European Union. (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 (NIS 2 Directive). Official Journal of the European Union, L 333, 80. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Henry Jackson Society. (2023). Research collaboration with high-risk countries: What does the UK public think? Retrieved from: https://henryjacksonsociety.org/publications/research-collaboration-with-high-risk-countries-what-does-the-uk-public-think/

International Organization for Standardization. (2019). ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements. Retrieved from: https://www.iso.org/standard/75106.html

Ivanov, H. (2023). Research collaboration with high-risk countries: What does the UK public think? Retrieved from: https://henryjacksonsociety.org/publications/research-collaboration-with-high-risk-countries-what-does-the-uk-public-think/

Kost, E. (2024). The state of university cybersecurity: 3 major problems in 2024. UpGuard. Retrieved from: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges

National Cyber Security Centre. (2021, June 4). Alert: Targeted ransomware attacks on UK education sector. Retrieved from: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector#section_1

Piazza, A., Vasudevan, A., Carr, M. (2023). Cybersecurity in UK universities: Mapping (or managing) threat intelligence sharing within the higher education sector. *Journal of Cybersecurity*, 9 (1). tyad019. https://doi.org/10.1093/cybsec/tyad019

Rakstiņš, V., Palkova, K., Sprūds, A., Agapova, O. (2024). 'Minimising the risks of foreign influence in research and academic context', in M. Nechyporuk, V. Pavlikov, and D. Krytskyi (eds), *Integrated computer technologies in mechanical engineering – 2023. ICTM 2023* (Vol. 996, pp. 89–103). Springer. https://doi.org/10.1007/978-3-031-60549-9_

Schwartz, N. (2023). Data breaches cost higher education and training organizations $3.7M on average in 2023. Higher Ed Dive. Retrieved from: https://www.highereddive.com

Sharma, Y., Black, R. (2021, February 9). Scrutiny Surrounds Genetic

Sequencing Giant, as US and Australia Investigate Equipment Donation. *ABC News*. Retrieved from: https://www.abc.net.au/news/2021-02-09/scrutiny-surrounds-giant-genome-sequencing-firm-bgi/13126514

U.S. Department of State. (2021). The Clean Network. Retrieved from: https://2017-2021.state.gov/the-clean-network/index.html

UK Government. (2023). National Security and Investment Act: Guidance for the higher education and research-intensive sectors. Retrieved from: https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

University Foreign Interference Taskforce. (2021). Guidelines to counter foreign interference in the Australian university sector. Retrieved from: https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector

White House Office of Trade and Manufacturing Policy. (2018). How China's economic aggression threatens the technologies and intellectual property of the United States and the world. Retrieved from: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf