Cyber Security at Universities: Comparison of Australia, Lithuania and Ukraine

Matthew Warren[1], Marius Laurinaitis[3] and Michael Prazian[3,4]
[1]RMIT University, Australia
[2]University of Johannesburg, South Africa
[3]Mykolas Romeris University, Lithuania
[4]G.E. Pukhov Institute for Modeling in Energy Engineering, Ukraine

Matthew.warren2@rmit.edu.au

Abstract: Universities are common across all countries and perform a key function in terms of research and knowledge development as well as the development of the next generation of professionals. In this study the focus is the university sector of Australia, Lithuania and Ukraine**.** Each country manages their university sector differently from a security perspective. Australian universities operate under critical infrastructure regulations and foreign interference guidelines. Lithuanian institutions benefit from EU NIS2 directives and national collective defense systems. Ukrainian universities, facing intense cyber attacks since 2014 and have developed exceptional resilience through distributed infrastructure and international cooperation. This paper examines the distinct cyber security postures of the Australia, Lithuania and Ukraine university sector.

Keywords: Cyber security, Critical infrastructure, Australia, Lithuania and Ukraine

1. Introduction

The university sectors across Australia, Lithuania, and Ukraine face distinct cyber security challenges shaped by their geopolitical contexts, resource availability, and threat landscape. Australian universities operate as part of Australian Critical Infrastructure. A disruption to critical infrastructure could have serious implications for Australian business, governments and the community, impacting supply security and service continuity. In Australia, critical infrastructure is regulated by a number of laws, which means that the University sector has to conform to Australian national cyber security standards and national regulatory security requirements. Another factor influencing the Australian University sector are the concerns relating to foreign interference and the sector must conform with detailed guidelines related to this threat.

Lithuanian universities benefit from EU (European Union) cyber security directives in particular NIS (Network and Information Systems) 2. NIS 2 focuses on enhancing cyber security capabilities, while introducing risk management measures and developing up rules for cooperation, information sharing, supervision, and enforcement of cyber security measures (ENISA, 2025). Lithuanian universities also cooperate on national collective cyber security systems to help protect all Lithuanian universities.

Ukrainian universities have operated under extraordinary circumstances, facing relentless cyber and kinetic attacks since Russia's 2014 invasion, intensifying dramatically after the 2022 Russian invasion. These Ukrainian universities have developed remarkable resilience, implementing robust backup systems, distributed infrastructure, and rapid incident response protocols. Ukrainian universities collaborate closely with the international cyber security communities, receiving substantial technical assistance and threat intelligence. Ukrainian universities have also been targeted by kinetic physical attacks and because of these physical attacks

2. University Sectors

The paper describes the different cyber security postures of three national university sectors. The sectors are influence by regulation, budgetary considerations, threat awareness, international cooperation, and adaptive cyber security strategies. The paper will also describe where common cyber security posture exists between the three countries and finally will discuss some of the future cyber security trends that will impact each country. The countries sectors are:

Australian University Sector

Australian universities are renowned for their cutting edge research and innovation, and this attracts attention from hostile foreign actors seeking access to sensitive information and intellectual property.

In Australia Critical infrastructure is defined as being physical facilities, supply chains, information technologies and communication networks which if destroyed, degraded or rendered unavailable for an extended period

would significantly impact on the social or economic wellbeing of the nation, or affect a nation's ability to conduct national defence and ensure national security (ASD, ND). Australia has uniquely defined the university sector as part of Australia's critical infrastructure due to their strategic importance to national security, economic resilience, and social cohesion. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) expanded the definition of critical infrastructure from four to eleven sectors, explicitly including the higher education and research sector (Australian Government, 2021).

The Australian Government together with Australian higher education providers has established programs to fight foreign interference threats. The University Foreign Interference Taskforce (UFIT) and Technology Foreign Interference Taskforce (TFIT) work together to improve foreign interference resistance and research security. The Australian University Sector faces specific national security threats. The University Foreign Interference Taskforce (UFIT), established in August 2019, was created to provide better protection for universities against foreign interference, bringing together the university sector and government agencies to build trust and resilience. The task force developed specific guidelines for the University sector focused on foreign interference and cyber security (UFIT, 2021).

Australian universities face escalating cyber security threats, including data breaches, ransomware, and phishing attacks targeting sensitive research and student data (Australian Cyber Security Centre, 2023). The Australian Government's Essential Eight framework provides a baseline mitigation strategy widely recommended for higher education (Australian Signals Directorate, 2022) which has been widely adopted by the Australian University Sector. Australian universities must also comply with the Australian Privacy Act 1988 when managing personal data breaches (OAIC (Office of the Australian Information Commissioner), 2022).

In a policy context, the Australian Government wanted greater resilience within the Australian university sector towards evolving cyber security threats; the 2020 Australian Cyber Security Strategy highlight key issues such as a national response to growing foreign interference in Australia, and the government desire to uplift the University sector's collective cyber security capabilities and identified the key security considerations of the Australian university sector (Australian Government, 2020).

Lithuanian University Sector

Cyber security has emerged as a strategic area of focus for Lithuania because of the growing digitalisation of public services, economic activities, and organisational processes. As networked infrastructure grows, it becomes essential for higher education institutions not only to produce the next generation of cyber security professionals but also to incorporate security by design principles into their organisational processes. The model of cyber security education and capacity building in Lithuania is influenced by national strategies and initiatives. The National Cyber Security Centre (NCSC), which falls under the Ministry of National Defence, is the main public institution dealing with the national cyber security strategy, the management of cyber incidents, as well as the implementation of cyber security requirements. Its tasks include the monitoring of cyber threats, the coordination of incident response, and the provision of guidance on the secure operation of critical information systems (National Cyber Security Centre of Lithuania, nd(a)). The NCSC also provides training and awareness resources for improving foundational knowledge and secure practices among various groups of people, including students, employees, and other stakeholders. For instance, the online learning platform provided by the NCSC includes interactive learning modules on cyber hygiene, threat recognition, and defensive practices to reinforce foundational knowledge including a national education brand #ŽinaiBetNedarai (#YouKnowButYouDon't) (National Cyber Security Centre of Lithuania, nd(b)).

Under the Lithuanian Cyber Security Law (Republic of Lithuania, 2014) only Lithuania transposed the EU NIS2 Directive through a recast Law on Cyber Security (No. XII-1428), adopted on 11 July 2024 and in force from 18 October 2024, complemented by an implementing Government Resolution of November 2024. Under this recast law, only two categories of entities are distinguished: essential entities and important entities. Both groups face broadly similar obligations, although supervisory attention is concentrated on essential entities. Consequently, operators of critical information infrastructure, following the entry into force of the amended Cyber Security Law, will be identified based on new criteria. Operators of critical information infrastructure that are not classified as cyber security entities would formally have the right not to apply cyber security requirements. However, this right is largely theoretical, as it is anticipated that all operators of critical information infrastructure will be included in the Register of cyber security entities. Given that the concept of critical information infrastructure has been removed from the Cyber Security Law, other related legislation has been amended accordingly to reflect this terminological change.

The practical significance of NIS2 for the university sector lies in the expanded sectoral scope. In addition to sectors already regulated under the previous regime e.g. energy, finance, health, digital infrastructure and public administration the recast law brought new sectors into scope, including research. As a result, universities that carry out critical research and experimental development now fall within the regulatory perimeter as essential or important entities, rather than remaining exempt as purely educational bodies. Designation is performed by the NCSC rather than through self-registration: in April 2025 the NCSC compiled a new Register of Cyber Security Entities, which contains 1,443 organisations drawn from 18 sectors almost a fivefold increase compared with the previous list (National Cyber Security Centre of Lithuania, 2025). Designated entities must implement organisational cyber security requirements within twelve months and technical requirements within twenty four months, with the organisational requirements to be in place by 17 April 2026.

The Lithuanian universities function in a complex framework of regulations and standards. The EU General Data Protection Regulation (GDPR) sets very strict requirements regarding the lawful processing of data, data minimisation, data protection impact assessments (DPIA), notification of incidents, and the appointment of Data Protection Officers in public institutions. At the organisational level, voluntary standards such as ISO/IEC 27001 and NIST Cyber Security Framework are increasingly influencing the governance structures of organisations. Some Lithuanian universities have started the process of aligning themselves with these standards (Kaunas University of Technology, 2025), which includes real-time network monitoring, multi-factor authentication, organised access control, and regular internal audits. The Lithuanian universities are important controllers of information, handling large amounts of personal data that fall under the GDPR, financial information that is prone to fraud, and valuable research information that has strategic or commercial significance. The open academic environment, large number of users, and high connectivity to the outside world greatly increase the attack surface. Vulnerabilities include open network access policies, use of personal devices (BYOD), low cyber security literacy among non-technical users, and limited IT security budgets.

Lithuania has faced significant cyber threats that impact Lithuanian universities including phishing and social engineering attacks, ransomware incidents, distributed denial-of-service (DDoS) attacks during peak periods (registration and exams), insider threats, and attacks on unpatched vulnerabilities. Human factors are still among the most important risk drivers, highlighting the importance of developing a security culture. (Ministry of National Defence, 2024).

Ukrainian University Sector

Ukrainian universities have faced unprecedented challenges since 2022, operating in a hybrid warfare environment where cyber and kinetic attacks aim to disrupt educational continuity and national development. The war in Ukraine has profoundly disrupted the national education system, particularly higher education. According to the Ministry of Education and Science of Ukraine, more than 2,000 educational facilities have been damaged and over 220 destroyed (Alieksieieva et al., 2025). Ukrainian universities have operated under extraordinary circumstances, facing relentless cyber attacks since Russia's 2014 invasion and, since the 2022 Russian invasion, with attacks intensifying dramatically. These institutions have developed remarkable resilience by implementing robust backup systems, distributed infrastructure, and rapid incident response protocols. Ukrainian universities collaborate closely with international cyber security communities, receiving substantial technical assistance and threat intelligence. Ukrainian universities have also been targeted by kinetic physical attacks and have moved many of their operations online. Ukrainian universities have identified gaps in policy, technology, organisation, management and identified the importance of international cooperation to help Ukrainian universities transform specific domains from siloed to coordinated strategies (Beska, 2025).

In times of crisis and chaos, it may be too late to respond to the latest threat. Ukraine universities have been using a cross functional ‘command center’ team approach (Dewar et al., 2022) that could address primary threats (technical, operational, legal, and financial) and secondary threats (key stakeholders’ reactions). Effective internal and external coordination is the command center’s key function. Universities and other academic institutions in Ukraine do not use the Cyber Resilience Assessment Methodology (CRAM), which evaluates the maturity and effectiveness of Security Operations Centers (SOCs). Several managerial tools, such as organising the Computer Emergency Response Team (CERT) and the DevOps team to integrate security into the development cycle within the Security Operations Center (SOC), can help. SOCs support detection, error reduction, and crisis communication.

The SIM3 (Security Incident Management) Maturity Model assesses SOC maturity across prevention, detection, resolution, and quality control. SOC implementation must ensure regulatory compliance with standards, including the EU General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability

Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA), thereby ensuring that institutions adhere to legal requirements and protect sensitive data. Frameworks that strengthen alignment, reduce risk, and build trust might also include PCI DSS (Payment Card Industry - Data Security Standard) for merchants and processors and SOC 2 (Service Organisation Control 2) for service providers. The "SIM3 Online Tool" was developed by the 'Open CSIRT Foundation' as an online self-assessment for SIM3 (Open CSIRT Foundation, 2026). The tool is designed for all types of CSIRTs (Computer Security Incident Response Teams). Key assessment areas include:

- Mandate, constituency, authority, and responsibility;
- Service definition, incident response, media policy, and reaction time.

The SIM3 evaluation scale (0 to 4) is as follows: 0 – not available or undefined; 4 – formally defined, approved, and audited. The SIM3 framework is built on four core pillars (Open CSIRT Foundation, 2026):

1. Prevention;
2. Detection;
3. Resolution;
4. Quality control and feedback.

Additional elements for improving cyber resilience include selecting a SOC model: in-house, outsourced (hybrid, or shared services. Incorporating cyber resilience concepts across the four stages of prepare, absorb, recover, and adaptation should align with modern risk management approaches (Trump. et al., 2025).

The Ukrainian National Security Standards are ND TZI (Нормативний Документ Технічного Захисту Інформації — Normative Documents of Technical Information Protection). These standards relate to the Ukraine's national regulatory standards governing the technical protection of information in automated and telecommunication systems (Davydiuk & Potii, 2024). The standards were developed and administered by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), a specialised executive authority responsible for information protection and cyber defence responsible for information protection and cyber defence; the standards establish requirements for confidentiality, integrity, and availability (SSSCIP, 2024)These key Ukrainian ND TZI family of Security Standards are adopted and are widely used by the Ukraine university sector.

2.1 Comparative Analysis

This part of the paper presents a comparison of key security domains areas comparing Australia, Lithuanian and Ukraine. This analysis is presented in table 1.

Table 1: Cyber Security at Universities Comparative Analysis: Australia, Lithuania and Ukraine

Key Security Domain Areas	Australia	Lithuania	Ukraine
Geopolitical Context	Stable democratic nation; universities targeted by foreign state sponsored espionage and intellectual property theft.	EU/NATO member; faces Russian linked cyber threats; strategic focus on collective regional defence.	Active conflict since 2014, escalating after 2022; hybrid-warfare environment (cyber, kinetic, information, energy continuity risks).
Classification of Universities	Classified as Critical Infrastructure under the Security Legislation Amendment (Critical Infrastructure) Act 2021. one of eleven protected sectors.	Research performing universities are designated as essential or important entities under the recast Law on Cyber Security (NIS2 transposition, in force 18 October 2024)	Not classified as critical infrastructure (unlike Australia); national reference: ND TZI technical information-protection standards under SSSCIP.
Primary Regulatory Framework	Critical Infrastructure Act 2021; Essential Eight framework (ASD); Australian Privacy Act 1988; 2020 Cyber Security Strategy.	EU NIS2 Directive; Law on Cyber Security (No. XII-1428, recast 2024) and its 2024 implementing Government Resolution; GDPR.	National: ND TZI standards (SSSCIP). Benchmarks/contextual only: GDPR, ISO 22301, ISO 55000, SOC 2, PCI DSS, HIPAA, FERPA.

Key Security Domain Areas	Australia	Lithuania	Ukraine
Key Governing / Oversight Body	Australian Cyber Security Centre (ACSC) / Australian Signals Directorate (ASD); University Foreign Interference Taskforce (UFIT).	National Cyber Security Centre (NCSC) under Ministry of National Defence; ENISA at EU level.	SSSCIP; CERT-UA and institutional CERT/CSIRT/SOC functions; SBU (cyberterrorism, cyber espionage, serious cybercrime).
Cyber Security Strategies & Frameworks Adopted	Essential Eight maturity model; critical infrastructure risk management programs; national Cyber Security Strategy (2023).	NIS2 risk management measures, voluntary alignment with ISO/IEC 27001 and the NIST Cyber Security Framework, national real time network monitoring, multi-factor authentication.	Distributed infrastructure; backups; online continuity; rapid incident response; CERT/SOC models; international cooperation. SIM3, CRAM, available tools, not yet systematically adopted.
Infrastructure Resilience	High compliance standards mandated by law; significant investment in security operations; but primarily compliance driven.	EU supported shared systems; collective national cyber security infrastructure; moderate resilience bolstered by regional cooperation.	High wartime adaptive resilience; distributed, redundant infrastructure; backups; online continuity. Energy resilience and physical protection remain key cyber-physical constraints.
Data Protection & Privacy	Australian Privacy Act 1988; Notifiable Data Breaches scheme (OAIC); sector-wide requirements for managing personal data breaches.	GDPR (strictly enforced); Data Protection Officers mandatory for public institutions; Data Protection Impact Assessments (DPIAs) required.	National: ND TZI confidentiality-integrity-availability requirements; GDPR for EU-linked processing. HIPAA, FERPA, PCI DSS, SOC 2 = external benchmarks, not Ukrainian law.
Maturity of Cyber Security Posture	Mature and well regulated; strong investment in compliance and dedicated security operations; guided by a comprehensive national strategy.	Developing to mature; benefiting from EU regulatory harmonisation; resource levels vary across institutions.	Rapidly evolving; high operational resilience (distributed infrastructure, backups, online continuity, international cooperation). Formal maturity, unified standards, and consistent implementation remain uneven.

3. Discussion

As shown by Table 1, cyber security policies in Australia, Lithuania, and Ukraine are shaped by their geopolitical and regulatory environments. Australian universities, classified as critical infrastructure, adhere to stringent security standards and foreign interference guidelines. Lithuanian universities benefit from EU directives such as NIS2 (ENISA, 2025), which emphasise risk management and cooperation. Ukrainian universities have relatively advanced national cyber security regulations but face challenges aligning with international standards due to resource constraints and implementation delays.

Ukraine's national cyber security standards have gaps, including a lack of unified frameworks for information structuring and delays in adopting international standards. While modern Ukrainian standards (e.g., ND TZI series) enhance compatibility with global frameworks, the implementation lag remains a significant obstacle. Holistic frameworks, such as ISO 22301 (business continuity), ISO 55000 (asset management), GDPR, HIPAA, FERPA, PCI DSS, and SOC 2, offer comprehensive approaches that integrate cyber security with risk management, resilience, and data protection. These frameworks could address existing gaps and strengthen Ukraine's cyber security posture.

Universities in Australia, Lithuania, and Ukraine employ diverse strategies to enhance cyber security. Australian universities focus on compliance with critical infrastructure standards, while Lithuanian universities leverage EU wide cooperation and shared systems. Ukrainian universities have developed robust backup systems, distributed infrastructure, and rapid incident-response protocols to address hybrid threats. However, challenges such as energy resilience and the absence of unified standards persist.

4. Conclusion and Future Work

The University sector is key to Australia, Lithuania and the Ukraine but each country has undertaken its own cyber security journey. A key next step is starting to collect case studies of cyber incidents at universities of the three countries to gain a greater insight and understanding.

In conclusion Australian universities generally operate under a mature national cyber security framework, guided by the Australian Cyber Security Centre and national Cyber Security Strategy, with strong investment in dedicated security operations and compliance obligations. Australian Universities also have to deal with other security issues as foreign interference. Lithuanian universities benefit from the European Union's NIS2 Directive and ENISA guidance, placing them within a well regulated regional framework, though resources vary across institutions. Ukrainian universities face a uniquely challenging environment, contending with active state sponsored cyber threats intensified by ongoing conflict, which has simultaneously exposed vulnerabilities and accelerated practical cyber resilience. Across all three, a common challenge remains the gap between policy frameworks and consistent implementation at the institutional level and the protection on universities into the future.

Acknowledgements

This research was partly supported by a grant from the Research Council of Lithuania (RCL/LMT) and the US National Science Foundation (NSF EAGER: IMPRESS-U #2402580).

Ethics Declaration: No ethical clearance was required for the research described in the paper.

AI Declaration: Grammarly AI was used to improve the readability of the text.

References

Alieksieieva, H., Kravchenko, N., Horbatiuk, L., Nestorenko, T., Zhyhir, V., Kalinichenko, A., & Glazova, Y. (2025). Digital transformation of relocated higher education institutions in Ukraine under martial law. Problems and Perspectives in Management, 23, 71–85. URL: https://doi.org/10.21511/ppm.23(2-si).2025.06, accessed 20/01/2026.

Australian Cyber Security Centre (2023). *Annual Cyber Threat Report 2022–2023*. Canberra: Australian Government, URL: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023, accessed, 20/01/26.

Australian Government (2020). Australia's Cyber Security Strategy 2020. Canberra: Australian Government. URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, accessed, 20/01/26.

Australian Government (2021). Security Legislation Amendment (Critical Infrastructure) Act 2021, Act No. 124 of 2021, Federal Register of Legislation, Canberra, URL: https://www.legislation.gov.au/Details/C2021A00124, accessed 20/01/2026.

ASD (Australian Signals Directorate) (ND). Glossary, URL: https://www.cyber.gov.au/learn-basics/view-resources/glossary/c, accessed 20/01/2026.

Australian Signals Directorate (2022) *Essential Eight Maturity Model*. Canberra: Australian Government. URL: https://www.cyber.gov.au, accessed 20/01/26.

Beska, S. (2025). Cyber resilience in Ukraine: Measuring response to cyber threats in the context of hybrid warfare. Central European University.

Davydiuk, A. & Potii, O. (2024) National cyber security governance: Ukraine, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf, accessed 20/01/2026.

Dewar K., Keller S., & Malhotra W. (2022). CEO Excellence: The Six Mindsets That Distinguish the Best Leaders from the Rest. Nicholas Brealey Publishing. URL: https://www.amazon.com/CEO-Excellence-Mindsets-Distinguish-Leaders/dp/B0999V3TS8, accessed 20/01/2026.

European Union Agency for Cyber security (ENISA) (2025) NIS2 Technical implementation guidance URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance, accessed 20/01/2026.

Kaunas University of Technology. (2025). KTU and NKSC focused on cooperation and strengthening Lithuania's cyber security ecosystem. URL: https://ktu.edu/news/ktu-kartu-su-nksc-susitelke-bendradarbiavimui-ir-lietuvos-kibernetinio-saugumo-ekosistemos-stiprinimui/, accessed 04/01/2026.

National Cyber Security Centre of Lithuania. (n.d. (a)). National Cyber Security Centre of Lithuania (NKSC). New Register of Cyber Security Entities — nearly 1,500 organisations from 18 sectors. URL: https://kam.lt/naujame-lietuvoje-kibernetinio-saugumo-registre-beveik-1500-organizaciju-is-18-sektoriu/, accessed 04/06/2026.

National Cyber Security Centre (NCSC). (n.d. (b)). Training. Ministry of National Defence Republic of Lithuania. URL https://www.nksc.lt/mokymai/, accessed 04/01/2026.

Ministry of National Defence (2024). Overview of the Cyber Security Status in Lithuania: Key Information: 2024, URL: https://www.nksc.lt/doc/en/2024_key-trends-and-statistics-of-cyber-security.pdf, accessed 04/01/2026.

Open CSIRT Foundation. (2026). SIM3 v2 interim Self Assessment Tool. URL: https://sim3-check.opencsirt.org/#, accessed 04/01/2026.

Office of the Australian Information Commissioner (2022). *Notifiable Data Breaches Report*. Canberra: OAIC.

Republic of Lithuania. (2014). Law on Cybersecurity (No. XII-1428), consolidated version as of October 18, 2024. E-TAR Legal Register. URL: https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr, accessed 04/01/2026.

State Service of Special Communications and Information Protection of Ukraine (SSSCIP) (2024). Official website, Ukrainian Government, Kyiv, URL: https://cip.gov.ua/en, accessed 20/01/2026.

Trump B.D., Mitoulis S., Argyroudis S., Kiker G.A., Palma-Oliveira J., Horton R., Pescaroli G., Pinigina E., Trump J., & Linkov I. (2025). Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure. URL: https://doi.org/10.48550/arXiv.2501.01318, accessed 04/01/2026.

University Foreign Interference Taskforce (UFIT) (2021). Guidelines to counter foreign interference in the Australian university sector, Department of Education, Australian Government, Canberra, URL: https://www.education.gov.au/countering-foreign-interference-australian-university-sector/guidelines-counter-foreign-interference-australian-university-sector, accessed 20/01/2026.