doi:10.25143/handbook_ISBN-978-9934-618-61-1

RĪGA STRADIŅŠ
UNIVERSITY

Handbook for Academic and Scientific Institutions

Improve Risk Management and Institutional Resilience in the face of Security Threats

Editors: Karina Palkova, Aleksandra Palkova

Handbook for Academic and Scientific Institutions

Improve Risk Management and Institutional Resilience in the face of Security Threats

Handbook for Academic and Scientific Institutions

Improve Risk Management and Institutional Resilience in the face of Security Threats

Editors: Karina Palkova, Aleksandra Palkova

RĪGA STRADIŅŠ
UNIVERSITY

RĪGA STRADIŅŠ UNIVERSITY

National Aerospace University "KhAI"

Handbook for Academic and Scientific Institutions Improve Risk Management and Institutional Resilience in the face of Security Threats

https://doi.org/10.25143/handbook_ISBN-978-9934-618-61-1

Scientific Editors:
Ph.D. in Law Karina Palkova, PhD. cand. in Sc. pol. Aleksandra Palkova

Authors: Ph.D. in Law, Assoc. Prof. Karina Palkova (Rīga Stradiņš University, Latvia), Ph.D. cand. Aleksandra Palkova (Rīga Stradiņš University, Latvia), Vitālijs Rakstins (Rīga Stradiņš University, Latvia), Ph.D. in Law Lidija Juļa (Rīga Stradiņš university, Latvia), Dr. iur., Prof., Nataliia Filipenko (National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Ukraine), Ph.D. in Law, Assoc. Prof., Serhii Lukashevych (National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Ukraine), Ph.D. in Law, Assoc. Prof.**,** Olena Andrieieva (National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Ukraine).

Project coordinator: Vitālijs Rakstins

The opinions expressed in the publication do not reflect the views expressed by the Rīga Stradiņš University or any other institution.

This project 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

Publication design: Oskars Stalidzāns

ISBN 978-9934-618-60-4 (printed)
ISBN 978-9934-618-61-1 (electronic)

Table of Contents

Introduction

Throughout history, science and academia has been characterized by international competition, giving nations economic, technological, military and other strategic advantages over their rivals. Unlike the centralized, state control approaches of the Cold War era, the current landscape requires scientific institutions and academia to take greater responsibility for self-policing and self-assessment, to establish robust internal risk assessment and screening systems. With disruptive technologies, hybrid warfare and constant state-to-state competition across all fields, academic and scientific institutions must minimize vulnerabilities, including those related to supply chain sustainability, raw materials and technologies, as well as dependence on foreign actors. Underlining their essential role in national security, it is imperative that academic and scientific institutions continue to function in times of crisis.

In today's increasingly complex and interconnected world, academic and scientific institutions are not exempt from the security challenges facing other critical sectors. As repositories of valuable intellectual property, sensitive research data, and global talent, these institutions have become prime targets for cyber threats, foreign interference, and other security risks that can disrupt operations, compromise research integrity, and endanger the safety of their communities. To meet these challenges, Higher education institutions (HEIs) must continue generating profit to reduce their dependence on government funding, which is constantly decreasing but also strengthen their image and deepen their specific training profiles on the international stage.

As universities navigate the demands of global competition, they must balance openness and collaboration with the necessity for rigorous security practices. Safeguarding institutional autonomy, intellectual property, and research integrity in an environment influenced by hybrid threats requires universities to take an entrepreneurial yet vigilant approach. This balance is essential for protecting the freedoms that underpin academic innovation while remaining resilient against external pressures. By adopting a strategic, security-centered mindset, universities can better anticipate risks, protect their research ecosystems, and uphold the values fundamental to the academic mission.

Today, the term “entrepreneurial university” is increasingly used, encompassing almost all characteristics inherent in contemporary higher education. The concept of “enterprise” covers both the economic and scientific, academic aspects of HEI activities. HEIs operate, on one hand, under traditional laws but, on the other hand, are compelled to adhere to new laws of competition and the necessity of maintaining and developing their prestige, image, and profit.

The entrepreneurial perspective on the functioning and development of the higher education system is just one of the many motives driving almost all HEIs to engage in activities influenced by globalisation processes. Differentiated academic pursuits, the internationalisation of curricula, the increasing mobility of students and faculty, and participation in auxiliary programs related to educational services are all significant manifestations of the globalisation process. It is also important to note that the funds obtained by HEIs from entrepreneurial activities can be used, based on the internal needs of the institution, to strengthen and develop the educational, teaching, research, and material-technical infrastructure.

A striking example of the interplay between the entrepreneurial approach and globalisation in higher education is the development of transnational education. In this context, one can observe the distinctive features of the modern operation of traditional higher education institutions, their actions in the international arena within the market space where HEIs assume the social roles of private education providers. During the implementation of global innovations in the higher education system, education-importing countries develop regulatory legislation that addresses consumer protection, the protection of regional (local) higher education systems, and the quality assurance of imported education. Education-exporting countries typically create codes of ethical practice in education and focus primarily on the reputation of their institutions as they operate internationally.

The improvement, reform, and enhancement of the competitiveness of higher education institutions align with the paradigm of higher education as an enterprise operating in a globally competitive space. Indeed, an HEI providing transnational education faces management challenges similar to those of any multinational organisation, including accounting for diverse cultural expectations, legal requirements, market opportunities, financial issues, and quality assurance. Ultimately, the goal of the Bologna Process, which introduced the three-tiered education system, the unification of education, the recognition of diplomas, and the mobility of both students and faculty, is achieved.

This handbook serves a dual purpose, addressing the urgent needs of Ukraine's educational and scientific ecosystem as well as those of neighboring countries affected by Russian aggression, aiming to bolster resilience and ensure operational continuity in challenging environments. Developed through the Latvian-Ukrainian Joint Programme of Scientific and Technological Cooperation, the guide is rooted in the immediate, real-world challenges faced by Ukrainian educational institutions amidst ongoing conflict. These experiences provide essential insights for institutions operating under insecure conditions, with practical guidance on crisis management, cybersecurity, and infrastructure protection.

Beyond Ukraine, the handbook offers a comprehensive framework applicable to institutions across the EU, enabling them to enhance risk management, safeguard intellectual independence, and fortify resilience against a range of external threats. This resource should also be considered by the European Union as part of its educational policy, encouraging member states to proactively adopt these guidelines to ensure preparedness in cases where martial law or other extreme measures may be necessary due to war situations.

In this context, this handbook addresses these evolving demands by strengthening institutional resilience and risk management, facilitating business continuity, and promoting a culture of preparedness within academic and scientific organizations. It provides a structured framework, practical guidelines, and actionable steps for institutional leaders, risk managers, and administrators tasked with safeguarding their organizations. Through this resource, institutions can establish robust policies, processes, and strategies to better protect against, prepare for, and respond to security threats, ensuring operational continuity and the preservation of their academic missions.

The scope of this handbook includes:

- **Advanced Risk Management**: Approaches to identifying, assessing, and mitigating security risks unique to the academic and scientific environment;
- **Institutional Resilience**: Tools and practices for building resilience across infrastructure, personnel, and research areas, supporting institutions in withstanding and recovering from disruptions;
- **Security and Continuity Planning**: Guidance on crisis response, business continuity, and cybersecurity to maintain essential functions during adverse events;
- **Case Studies and Practical Applications**: Real-world examples illustrating the successful application of these principles in addressing modern security challenges.

The implementation of this Handbook's recommendations requires the collective commitment of every member of the university or academic community. Therefore, institutions must establish a clear governance structure, designate specific personnel to manage the identified risks, and adapt institutional systems, processes and cultural practices. A key aspect of successful implementation is raising awareness and understanding of security issues among individuals within the academic community, including staff and students**.** By adopting these guidelines, academic and scientific institutions can fortify their defences against external threats, protect their assets and intellectual capital, and **foster a culture of preparedness, ultimately building resilient institutions capable of thriving amidst emerging security challenges.**

Understanding the Threat Landscape

In today’s globally interconnected environment, academic and scientific institutions are vulnerable to various security threats that extend beyond traditional risks. These include cyber threats, misinformation campaigns, hybrid warfare tactics, and physical security challenges, each of which poses unique risks to institutional integrity and continuity. As educational and research hubs, universities attract diverse actors, from opportunistic cybercriminals to state-sponsored entities seeking intellectual property or influence. Understanding these threats is crucial for institutions aiming to safeguard their operations, reputation, and academic freedom.

Hybrid Threats and Misinformation

Hybrid threats employ a strategic blend of conventional and unconventional tactics, such as cyberattacks, disinformation campaigns, and psychological operations, to destabilize institutions and undermine public trust. These tactics leverage modern technology and communication channels to reach and influence large audiences, making them particularly dangerous in an era where information spreads rapidly and credibility can be undermined with just a few well-placed falsehoods. Key elements of hybrid threats include misinformation, psychological operations, and foreign influence, all of which challenge academic institutions’ credibility, internal cohesion, and autonomy.

Misinformation campaigns, for instance, can be highly damaging, as they have the power to distort research findings, confuse the public about scientific facts, and harm the reputation of institutions. These campaigns do not only target external audiences; often, they seek to create division within academic communities themselves by sowing distrust and suspicion among faculty, students, and staff. Similarly, psychological operations target individual opinions and group dynamics, aiming to shape attitudes, foster doubt, and even create resentment towards institutions. An example might include spreading false information about a university's safety record to discourage international students from enrolling, which could lead to a tangible drop in admissions and revenue.

Another form of hybrid threat is foreign influence and economic coercion, where external actors—often states—exert subtle but persistent pressure on institutions through conditional funding, partnerships, or enrollment incentives. This can affect research agendas, educational content, or institutional policies, threatening academic freedom and compromising the integrity of research and educational outputs.

Cyber and Physical Security Threats

Academic institutions are prime targets for cyber threats due to the valuable intellectual property, sensitive personal data, and proprietary research they handle. Cyberattacks can be highly disruptive, ranging from phishing schemes and ransomware attacks to highly sophisticated attempts to steal research data. Beyond causing immediate operational disruptions, these attacks have far-reaching impacts on research integrity and financial stability. For instance, if an attacker gains unauthorized access to ongoing research in fields like biomedicine or defense, they not only threaten the confidentiality of the research but may also expose the institution to legal and ethical risks that can damage its reputation.

Insider threats represent another critical risk. While often unintended, faculty, staff, or students may inadvertently compromise security through lax practices, while some may act with malicious intent. Given their access to sensitive systems, these insiders can bypass external cybersecurity measures, making this an area where vigilance and regular training are essential.

Physical security also plays a crucial role in institutional resilience. Unauthorized access, theft, and vandalism threaten the safety of both people and resources on campus. Educational institutions, which are often open environments, face unique challenges in balancing accessibility with the need to secure high-value assets and sensitive research spaces. A robust physical security plan is essential for safeguarding these resources while still maintaining an environment conducive to academic collaboration.

Impacts on Academic and Scientific Institutions

The impacts of these diverse threats are profound, as they directly undermine the ability of academic institutions to operate effectively and independently. Cyberattacks, foreign influence, and misinformation campaigns not only disrupt daily operations but also erode public trust and credibility in research. When research data is stolen, distorted, or manipulated, it raises ethical concerns and can compromise the integrity of findings, particularly in high-stakes areas like health sciences or national security.

Reputational harm is a major risk, especially from misinformation and hybrid threats. Public confidence in academic research is vital, yet false narratives, when left unchallenged, can swiftly damage the perceived reliability of research and weaken the institution's standing. Operational disruptions are equally damaging; cyberattacks and physical threats can hinder day-to-day activities, preventing students and faculty from accessing resources essential for learning and research. Without a robust crisis response framework, an institution's mission can be compromised, impacting its ability to attract prospective students, faculty, and funding.

Finally, these threats pose a direct risk to the safety and well-being of students, faculty, and staff. Cyberbullying, harassment, and physical breaches of campus security create hostile environments that are detrimental to learning and innovation. For example, harassment targeting specific groups or individuals can deter students from attending classes or even enrolling, which negatively impacts the institution's inclusivity and academic atmosphere.

The Increasing Frequency and Sophistication of Threats

The frequency and sophistication of these threats are escalating, influenced by rising geopolitical tensions and technological advancements. For example, ransomware attacks have recently impacted higher education institutions in multiple countries, leading to significant financial losses and halting access to critical research data. The COVID-19 pandemic also underscored the impact of misinformation on scientific trust, as disinformation about health and safety spread widely, often undermining confidence in academic research.

Hybrid warfare, such as that observed during the Russo-Ukrainian War, demonstrates the impact these threats can have on education. Academic institutions are vulnerable to direct attacks on their digital and physical infrastructure, revealing the necessity for resilient crisis response frameworks that ensure continuity of operations, even amid complex and politically driven disruptions.

Resilience and Recovery Strategies

Beyond identifying and understanding threats, academic and scientific institutions must prioritize resilience and recovery strategies to mitigate damage and restore normalcy post-incident. Implementing comprehensive recovery plans – such as robust incident response protocols, data recovery mechanisms, and clear communication strategies – can greatly reduce the long-term impacts of cyberattacks, physical breaches, and misinformation campaigns. Resilience strategies also involve training staff and faculty in crisis response and ensuring systems are equipped with secure backups and redundancies. Building a recovery-oriented culture allows institutions to not only respond swiftly to disruptions but also to continuously adapt to the evolving threat landscape.

To sum up, understanding the threat landscape is the essential first step for academic and scientific institutions to develop effective resilience strategies. With a deep knowledge of these evolving risks, institutions can tailor their risk management, cybersecurity, and continuity planning efforts to better protect their assets, operations, and community members from both immediate and long-term impacts.

1. Advanced Risk Management

1.1. Building Advanced Risk Management and Resilience to Security-Related Issues (Due Diligence)

The guide provides recommendations for the enhancement of due diligence and screening in order to mitigate potential risks associated with hostile foreign influence. It emphasizes the importance of reducing dependence on foreign funding and technology while maintaining academic and research freedom as an integral part of national security. The preservation of the integrity and autonomy of research, the safeguarding of academic independence and the assurance of research integrity require the identification of risks associated with foreign investment, including debt, investment, grants, co-funding and other forms of financial, intellectual and technological support from abroad. Given the uniqueness of each institution's risk exposure, influenced by factors such as type and scale of activities and risk awareness and management culture, effective risk management is critical. Failure to manage security risks can have serious financial, legal, reputational and potentially national security consequences.

The risks posed to universities and scientific institutions by foreign interference:

- Unwanted access to and potential interference with researched, sensitive data.
- Potential loss of future partnerships, collaborations and attracting talent.
- Failure to comply with legal, contractual or regulatory obligations.
- Risk of loss of intellectual property and loss of commercialization opportunities.
- Undue influence on the curriculum agenda.
- Damaged reputation at institutional, researcher or research team level.
- Loss of public confidence, credibility and integrity of research outputs or data.

- Loss of control over confidential data or findings, particularly if another individual patents research results and restricts access by other means.
- Loss of professional recognition of work, effort and career advancement opportunities.
- Erosion of the confidence of existing or potential partners in relation to the ability to protect confidential information in the future.
- Ineligibility for future funding.
- Risk of breach of sanctions, non-compliance, litigation or criminal charges.

Scientific and academic institutions should have comprehensive risk management systems in place that comply with national and international standards, such as ISO 31000:2018. Effective risk management strategies include the integration of risk assessment and mitigation at all levels of the organization. They also include the identification of key assets within the scope of the model, such as specific research projects or data sets. Regular updating of the risk register within the institution's risk management framework is essential for the maintenance of its accuracy and relevance. The risk register should include a thorough analysis of relevant threats, intentional or unintentional, that could potentially harm the organization's assets. These may include unauthorized access, destruction, disclosure, modification or denial of service.

A comprehensive system should be set by the regulations, implemented at all levels and appropriately resourced:

- Setting clear guidelines and tasks for tracking foreign investment sources, which are the primary sources of foreign funding for universities and scientific institutions, including government grants, international foundations, philanthropic organizations, corporate sponsorships, and collaborations with foreign institutions.
- Structuring it as an in-house internal control system, approving the regulation, allocating resources and defining responsibilities. Internal oversight mechanisms of the acceptance of foreign funding should not only consist of supervision or ethics boards but should be integrated into the risk assessment at all levels, also involving non-academic staff and students and employees.

- Ensuring adequate education and training for scientists, academic personnel, and staff members is crucial to raise awareness and understanding of the risks of hostile foreign influence. These educational programs should be comprehensive and cover risk assessment, data security, intellectual property protection, responsible research practices, and compliance with relevant regulations and policies.
- Introducing robust compliance processes, including conducting thorough due diligence on the origins of the technologies and materials they utilize, ensuring compliance with ethical sourcing and sustainability and international sanctions, and actively monitoring and reviewing supply chains to prevent the use of prohibited resources.
- Structuring systematic, regular cooperation with the relevant state institutions responsible for national security.
- Ensure that staff involved in export control or dual-use technologies understand and comply with their obligations to protect university research and intellectual property both domestically and internationally.

To diversify funding sources and minimize critical dependency, universities and science institutions should:

- Diversify funding sources, reducing over-reliance on a single foreign funding source by actively seeking funding from a diverse range of domestic and international sources.
- Facilitate cooperation in basic science only with like-minded partners sharing the same values. Collaboration with a wide range of like-minded international partners fosters creation of a resilient scientific technologic diverse ecosystem, helping broaden research perspectives and reducing the risk of hostile influence on research priorities
- Foster public funding and support, as science is a part of national sovereign capabilities.
- Minimize critical dependencies on foreign equipment, software and technologies, intellectual property, and skills by facilitating the creation of national scientific capability.

In order to minimize the risks associated with foreign interference, scientific institutions and academia should implement various policies related to transparency, ethics and values, such as:

- Policies and procedures on gifts and donations.
- Guidelines for the promotion of ethical behavior in the workplace.
- Protocols for conducting responsible research.
- Codes of conduct for students and members of staff
- Policies to prevent discrimination, bullying and harassment.
- Fraud and corruption prevention controls.

By putting all these measures in place, universities and scientific institutions will be able to skilfully navigate the complex relationship between national security, financial autonomy and academic freedom.

Case Study

Avoidance of strategic dependencies in the UK universities

Since 2020, there has been sustained pressure from the UK government on universities to minimise the influence of China.

Between 2017 and 2022/23, UK higher education institutions received between at least £122 million and £156 million from Chinese sources in relation to an educational, scientific or research project or in other ways, such as charitable payments. This figure does not include the approximately £2.2 billion per year in international student fees paid by Chinese students studying at UK universities. The most extreme cases of UK universities receiving funding are either from units of the Chinese military or from companies that are directly linked to the Chinese military.

Because of Huawei's links to the Chinese military, the UK government decided to ban the company from any further role in the country's 5G infrastructure. Simultaneously, the largest single source of Chinese funding to UK universities is Huawei Technologies and its subsidiaries, accounting for 22-24% of all Chinese funding.

The Strategic Dependence of UK Universities on China – and where should they turn next? Robert Clark, Civitas: Institute for the Study of Civil Society, November 2023

Example of a Comprehensive Risk Assessment and Mitigation Strategies

Risk-benefit analysis: Do the benefits of the activity outweigh the risks?

Risk mitigation: What elements of the activity need to be adjusted to mitigate the risks? Who will be responsible for maintaining, promoting and applying risk mitigation?

Legal awareness: Are researchers and their international partners aware of their legal obligations, including the declaration of conflicts of interest?

Reputational and ethical considerations: Are there potential reputational or ethical risks for your institution associated with the collaboration or activity?

Partner assessment: Is your partner open, transparent and accountable? How does your partner's host country score on indices of public democracy, freedom and corruption?

Intellectual property rights: Does your partner respect intellectual property rights? Does your partner have institutional autonomy and independent decision-making separate from the host government?

Information Awareness: Do you have information that promotes awareness of what is shared with foreign institutions (e.g., as part of travel security, videoconferencing, or other policies)?

IT network access: What access will the partner have to your IT networks? Is this an additional risk?

Physical separation or protection: Is there a need for physical separation or protection to protect the research?

Commercialisation considerations: how ownership arrangements for any intellectual property (IP) generated? How existing IP, research data, confidential or personally identifiable data will be protected? Identification and protection of commercially valuable research or research that may benefit nation's economic interests?

Dual-use technology and economic impact: Does the technology have dual-use military, intelligence, police or security applications?

1.2. Protecting Personnel and Students

The risks to staff and students relate to targeted recruitment to further the interests of a foreign actor and inappropriate attempts to obtain sensitive information through foreign delegations, seminars or collaborations. The foreign state or non-state actor seeks inappropriate access to or influence over specific individuals through various forms of funding arrangements (e.g. donations) or collaboration, financial or other inducements targeted at individuals. This poses significant challenges to the security of the institution. It can compromise the integrity of research. It may also be a threat to the security of the academic community as a whole.

The transition from an industrial society to an information society, along with the migration of not only social and business communication into cyberspace but also the majority of individual social and payment activities and almost all forms of traditional entrepreneurship, leads to a situation where information becomes an independent entity capable of influencing individual, group, and even societal criminogenic potential. This shift in communication to cyberspace also facilitates the migration of destructive human behaviours, including the spread of cyberbullying, the use of private information to provoke suicidal behaviour, and various forms of blackmail, harassment, and other malpractices. It can be anticipated that personal information will increasingly become the target of criminal activities with diverse purposes-from outright theft and subsequent misuse to intentional distortion or destruction of a person's information.

Technological advancements suggest a growing discussion around the subjectivity of artificial intelligence (AI), which is approaching, and in some cases surpassing, human cognitive and emotional capabilities. It is crucial to recognise that AI can both assist us in our daily activities and hinder them, or even cause harm if it falls into the hands of individuals with malicious intentions. This threat encompasses not only the theft of personal data but also the disabling or blocking of global communication systems, interference with the operation of individual electronic devices (such as pacemakers, insulin pumps, smart home systems, autonomous driving systems, or baby monitors), or the disruption of essential life-support systems (including power plants, dams and water release systems, street and indoor lighting, water purification and ventilation systems, and numerous other complex systems) (Lukashevych, S. Y., 2020).

To ensure the safety of the scientific and academic community, including students, staff and visitors, a culture of security awareness is essential. This includes clearly defining responsibilities, creating an environment that encourages incident reporting and awareness-raising, providing relevant training to students and staff on security-related risks, and ensuring safety and security measures are in place for travel abroad. Through these initiatives, a robust framework for the protection of the community within scientific and academic institutions will be promoted, thereby fostering a safe, secure and resilient environment.

Scientific and academic institutions should establish a system to ensure the protection of staff, students and visitors:

- develop the necessary policy and set it down in documents;
- define roles and responsibilities;
- oversight of the system by an audit committee or a supervisory board;
- provide appropriate training to students and staff on the risks associated with security;
- identify critical personnel required to perform key functions;
- establish a system to report accidents and raise awareness;
- develop and promote a positive, risk-aware culture;
- ensure safety and security when travelling abroad by implementing risk assessment procedures for international travel, including due diligence and risk assessment (duty of care), cultural sensitivity training and vaccination, etc.;

To prevent mass terrorist attacks, riots, and to ensure the safety of university administrations and students, it is essential to employ specialised technological solutions. For instance, “Evolv Technology” has developed an AI-based security machine that operates through the “Evolv Pinpoint” application and utilises facial recognition technology. This setup can be installed at the entrances to campuses, universities, and other educational facilities. To undergo screening, individuals simply pass through the structure as they would through a conventional metal detector. The throughput capability of such a detector is 600–900 people per hour.

The verification process is carried out using an integrated camera, where the “Evolv Pinpoint” algorithms compare the faces of visitors with those in the watchlist uploaded to the system’s database. If it is determined that a visitor is of interest to the police or other services, their image and personal details are displayed on a security staff member's tablet and highlighted in red. A yellow highlight indicates a potential but unverified threat. In such cases, the profile is checked in real time within a few seconds.

Example

Starting August 15, 2023, Ukraine has launched an experimental project called "Safety Specialist in the Educational Environment." The goal of this project is to ensure safety within the educational environment by preventing, early detecting, mitigating, and eliminating potential negative phenomena. This is achieved through the implementation and organisation of the role of a safety specialist within educational settings.

A safety specialist in the educational environment is an employee of local government bodies, working within the executive body of a village, town, or city council. During the implementation period of the experimental project, this specialist is tasked with fulfilling functional responsibilities aimed at creating and maintaining a proper level of safety in the educational environment. This includes organizing and participating in coordinated measures to prevent, early detect, stop, and eliminate negative phenomena within the educational context.

The Safety Specialist directly addresses negative occurrences within the educational environment, including events that take place inside educational facilities, on surrounding premises, or on the way to and from the institution, which pose a threat to the life, physical and mental health, and property of students. Such negative phenomena include:

bullying (harassment); aggressive behaviour among students that can cause emotional or physical harm; consumption of alcohol, tobacco, and other psychoactive substances, use of such substances within the school or its surrounding areas; involvement in unlawful activities, drawing students into illegal actions or encouraging the use of psychoactive substances; cruel treatment or discrimination, any form of maltreatment or discrimination based on any grounds, or undermining the dignity of students; participation in destructive youth groups, involving students in harmful social groups; proximity to conflict zones, being near areas where measures for national security, defence against armed aggression, or active combat are taking place; poor traffic and fire safety, inadequate road safety around the educational institution and insufficient fire safety measures within the school; uncontrolled access by outsiders, unauthorised presence of strangers or the introduction of prohibited items, such as weapons, narcotics, or psychotropic substances, onto school grounds or into buildings; lack of student awareness of rights and safety, insufficient knowledge among students about their rights, safety practices (including online safety), and response protocols when their rights and interests are violated; lack of staff awareness regarding child rights, inadequate understanding among educational staff about children's rights, how to act when witnessing violations of student rights, or encountering negative phenomena in the educational environment; insufficient emergency preparedness, unawareness among participants in the educational process about how to respond to the threat or occurrence of emergencies; employment of individuals with criminal records, non-compliance with bans on employing individuals who are listed in the Unified Register of Individuals with convictions for sexual offenses against minors in roles involving contact with students; increased crime rates in school vicinities, a rise in the number of criminal offenses in the area, particularly those affecting children; suicidal, deviant, or victim behaviour among students, engagement in criminal activities, substance abuse, dependency issues, or other types of addictive behavior.

1.3. Protecting Infrastructure (Cybersecurity and Kinetic)

This chapter of the handbook focuses on the protection of the campus and assets of academic and scientific institutions from security risks, particularly in the context of potentially hostile activities. The focus is on physical security and cyber security.

Cyber Security Threats and Their Impact

Ensuring cybersecurity is one of the foremost tasks facing any state. It primarily involves the development of a comprehensive legislative framework; amending criminal laws to address existing “gaps” and aligning them with international standards; upholding the national cybersecurity strategy through continuous updates with relevant measures. This also includes integrating cybersecurity-related disciplines into the educational curriculum for students and organizing systematic, large-scale public awareness campaigns about the potential threats associated with the use of internet services (Tavolzhanskyi, O. V., 2016).

Cybersecurity measures comprise a coherent set of organizational investments and actions aimed at the prevention, detection, response and recovery from cyber threats. Any institution needs to address the range of cybersecurity threats, from sophisticated attacks on digital networks to opportunistic breaches that take advantage of low awareness. The institutions have to pay particular attention to protecting high-value information, including economically, politically and commercially sensitive material.

A comprehensive cybersecurity strategy should include (but is not limited to):

- Security policies and standards.
- Usage of published threat assessments, such as the CERT’s, to anticipate cyber threats.
- Defined security roles and responsibilities, including senior leader role.
- Establishing effective monitoring and reporting protocols for cybersecurity risks, including sharing information with government / CERTs.
- Measures to support asset, vulnerability and threat management .
- Develop policies and training packages that focus on segregating research materials, limiting access to sensitive data, and monitoring access.
- Training and awareness programmes, including appropriate training for researchers working on high security issues, controlled technologies or areas subject to export control legislation.
- Business continuity planning and disaster recovery procedures.

The development and implementation of a comprehensive, joint strategy for protecting higher education institutions (HEIs) from cyber-terrorist attacks must be based on principles of international law and common documents that outline the conditions and procedures for state cooperation in the realm of international collaboration. Only through collaborative scientific efforts can the true state of affairs and existing prospects for development be assessed, strategic and tactical objectives be identified, and the trajectory for their achievement be defined.

Protecting Physical and Digital Infrastructure

- Recognize the vulnerability of both digital and physical infrastructure to security breaches.
- Ensure that institutional policies and frameworks address specific physical security risks.
- Implement measures to protect both digital and physical infrastructure, taking into account the vulnerabilities highlighted in the case studies.

Campus Visitors and Security

- Develop frameworks, policies and risk assessments to distinguish between different types of visitors.
- Implement visitor checks before on arrival and during their stay, including identity verification and compliance with visa requirements.
- Establish clear management and oversight processes for visiting students and staff.
- Emphasize pre-arrival checks and ongoing contact points for visitors.
- Establish senior oversight and accountability for visitor and visa arrangements.
- Access restrictions and visitor guidance.
- Enforce visitor access restrictions and provide clear processes for oversight and accountability.
- Provide clear advice, information and guidance to visitors and staff on following protocols during their time on campus.

A novel initiative in protecting the premises of higher education institutions (HEIs) and campuses is the implementation of the "Educational Security Service" project. An analysis of the performance of the Educational Security Service officers demonstrates that the "Educational Security Service" project is an effective and positive mechanism for enhancing the safety of educational environments for children within educational institutions. Its sustainability is a key factor in significantly reducing crime rates both among children and towards them. Further implementation of this project in all general secondary education institutions will not only enhance the safety component (Yazan, N., Filipenko, N., 2024). Specifically, this pertains to: raising the level of legal awareness among students, educators, and parents; facilitating communication between police, education authorities, local community representatives, children, and the general public in each distinct territorial unit; the continuous presence of a dedicated police officer in educational institutions ensures prompt and effective response to all incidents of unlawful behaviour. The officer's awareness of the specific community's needs helps in identifying and effectively performing preventive functions in a way that meets the community's demands and achieves the expected outcomes.

Apply appropriate protective measures to locations containing sensitive research and materials.

To facilitate cyber security efforts should be focused on three key areas:

1. Engineering and technical security component. The main efforts are aimed at modifying the university's local network using advanced technological security achievements, the requirements for which should be taken into account not only at the stage of operation, but already at the stage of designing the university as a component of critical infrastructure.
2. Digital hygiene and moral and ethical component of security. If the technical characteristics of a computer system can be subjected to more or less correlated measurements, the human component of the internal security of a higher education institution always remains the most complex and vulnerable area of protection. That is why users of electronic networks should be trained in advance in the basic algorithms of electronic security and moral and ethical standards of behaviour in the digital space.

3. Cyber component of security. There is a need for a common joint strategy to protect higher education institutions from cyber-terrorist attacks, based on the principles of international law and joint documents that define the conditions and procedure for interaction between states, organizations and higher education institutions in the field of international cooperation. After all, only joint efforts in the field of science allow us to assess the real state of affairs and existing development prospects, define strategic and tactical goals and the trajectory of their achievement.

2. Business Continuity and Institutional Resilience

2.1. Business Continuity

Business continuity refers to the ability of an academic or scientific institution to maintain essential operations and functions during and after a disruptive event. Institutional resilience refers to institutions' ability to withstand, adapt and recover from various challenges, disruptions or crises through a holistic approach to building robustness, adaptability and sustainability. Both of these concepts involve the development and implementation of business continuity plans and procedures to ensure that critical functions and business processes can continue to operate or can be quickly restored following a disruption. The aim of business continuity is to minimize the impact of disruptions, protect assets and maintain overall business resilience, enabling the organization to adapt and recover efficiently.

The institution shall have in place a business continuity plan, which shall specify:

- the essential services and functions and the minimum level of those services and functions to be provided at least at the specified level during a crisis; and
- the critical personnel and their responsibilities;
- the resources needed (infrastructure, technological and other equipment, raw materials and other support) to continue operating;
- algorithms for operating in a crisis.

The Minimum Requirements for the Business Continuity Plan

The Business Continuity Plan (hereafter – Plan) shall be structured in a formal manner and shall contain the following elements:

1. **Recognition and formalization of the essential function**, which shall include:
   1.1. a description of the critical functions and processes;
   1.2. a definition of the scope of the critical functions to be provided at all times at the pre-defined level;
   1.3. a definition of the maximum permissible duration of interruption in the provision of critical functions and the required recovery time and priorities for the recovery and continuation of critical functions.

2. **Critical personnel:**
   2.1. assess and identify the critical personnel, including support personnel, required to ensure minimum continuity of critical services and processes;
   2.2. inform critical personnel of their status and responsibilities and ensure that they are trained and prepared;
   2.3. establish procedures for replacing or augmenting critical personnel, including procedures in the event that some critical personnel are unavailable;
   2.4. avoid reliance on foreign personnel who may be subject to mobility restrictions or be part of their domestic mobilization;
   2.5. adjust infrastructure and allocate resources in a timely manner, to the extent practicable, to allow for shift work, overnight stays or extended stays at work sites;
   2.6. the adoption of algorithms for internal communication and action in specific situations.

3. **Infrastructure**

The provision of infrastructure must include the transition to an alternative workspace (alternate location) when the routine workspace is unavailable. To achieve this:

   3.1. timely identify suitable infrastructure (alternate site) sufficiently distant (minimum 20–30 km) from existing infrastructure and suitable for critical functions (minimum requirements: communications support, alternative energy solutions where available, water availability, etc.);

3.2. make arrangements to relocate (temporary or permanent) personnel and process equipment to the alternate site, anticipating the number of transport units and other support required (including accommodation, staffing);

3.3. identify opportunities to recruit personnel and purchase or lease necessary equipment, repair and maintain equipment in the vicinity of the alternate site.

3.4. prepare to secure and fortify existing infrastructure before moving (arrange for security guards, sandbag doors and windows, etc.).

4. Essential equipment

With regard to the technological equipment and assets that are necessary for the provision of critical services, the plan shall include the following:

4.1. an inventory list of critical equipment and assets (where possible marked with the priority markers for the evacuation);

4.2. the identification of alternatives to critical equipment and assets, and options for their replacement, avoiding the use of technologies manufactured by companies whose reputation in the European Union and NATO Member States is in doubt due to suspected breaches of privacy, unauthorised acquisition of non-public information or threats to national security is not recommended;

4.3. immediate actions when equipment and assets become lost or fail;

4.4. pre-planned actions for installation and calibration of equipment in the alternative sites, maintaining, repair, replacement, upgrade or development of alternatives;

4.5. timely back-up of digital systems and equipment to ensure that data, systems and processes can be accessed from the alternate site; and

4.6. the evaluation of impact of the security of supply on the continuity of the business (availability of support staff, availability of spare parts, repairs);

4.7. the redundancy of the power supply connection to the information systems and the provision of a stand-alone power supply.

5. Transport and logistics

With regard to transport (where applicable) required to provide critical functions, the plan shall identify:

5.1. transport required to provide critical services

5.2. transport alternatives;

5.3. availability of drivers and specialists, and substitution possibilities;

5.4. fuel supply;

5.5. packaging equipment, crates for evacuation of equipment, pallets.

6. External essential services

The operational activities of each entity are heavily dependent on external essential services, which should be reflected in the plan:

6.1. electronic communications and voice telephony facilities and their databases (including access from alternative workstations, alternative or redundant communications and data transmission systems, PACE - primary, alternative, contingency and emergency communication systems);

6.2. electricity supply facilities, their alternatives and options for outsourced energy suppliers;

6.3. availability of internet and access to global networks (scientific and academic data bases);

6.4. availability of natural gas and petroleum products (and alternatives);

6.5. availability of heating, water and sewerage;

6.6. define the necessary external support required from national authorities to ensure the exercise of critical functions in the event of a national emergency, such as prioritized supply of energy, gas and petroleum products, communications and logistical support.

7. Critical supplies and raw materials

The plan should:

7.1. identify the critical raw materials and resources that are necessary for the scientific work;

7.2. assess the aspects of security and continuity of supply;

7.3. identify substitutes for critical raw materials or alternative supply chains.

8. Security and resilience of supply

The plan should address the security and resilience of the supply chain:

8.1. identify at least Tier 1 suppliers and their geographical distribution to identify vulnerabilities in the event of international supply chain disruptions and to identify possible alternatives in a timely manner;

8.2. avoid dependence on a single foreign supplier;

8.3. discourage the involvement of high-risk suppliers in supply chains whose reputation in the European Union and NATO member states is in doubt due to suspicions of privacy violations, human rights abuses, unauthorized acquisition of non-public information or threats to national security;

8.4. avoid strategic dependency on know-how, patents, intellectual property and strategic technologies, software and hardware from third countries;

8.5. local supply chains and local producers, processors and service providers shall be preferred to ensure security and sustainability of supply.

9. Algorithms for action in the event of a crisis

The priority of the institution's activities shall be the provision of critical functions within a defined scope and shall be subject to the commitment of all available internal resources.

The plan shall reflect the contingency action algorithms:

9.1. ensure the provision of critical services within defined limits in case of crisis, allocating all resources to maintaining and restoring critical functions and business processes;

9.2. establish internal and external crisis communication protocols and plans;

9.3. establish the procedure for activating and operating the crisis management team during a crisis, crisis contingency procedures and actions to be taken to restore critical functions and minimize the damage caused, implementing recovery scenarios expeditiously or relocating and continuing operations from an alternative location;

9.4. establish crisis protocols for all categories of staff (academic, students, contractors). All non-essential staff and students shall carry out safety first procedures and evacuate.

10. Systematic improvement:

The business continuity system shall be subject to review and improvement periodically by:

10.1. the identification of those responsible for business continuity planning and the allocation of the necessary resources;

10.2. formalizing business continuity processes, documents, algorithms and protocols, lessons learned;

10.3. involving senior management in business continuity planning and approval processes;

10.4. organizing periodic reviews, self-assessments, audits, periodic exercises and stress tests.

Example from Practice

At the National Aerospace University named after N. E. Zhukovsky "Kharkiv Aviation Institute" (hereinafter referred to as the University), a legal clinic (hereinafter referred to as the Legal Clinic) has been established. The Legal Clinic serves as a base for practical training and conducting internships for University students pursuing higher education in the field of "Law." The Legal Clinic is a structural unit within the Department of Law of the University's Humanities and Legal Faculty, functioning as an educational and practical laboratory for legal assistance (https://khai.edu/ua/university/normativna-baza/polozheniya1/polozhennya-bez-grupi/polozhennya-pro-yuridichnu-kliniku/).

The objectives of establishing the Legal Clinic include: reinforcing theoretical knowledge and developing practical skills and competencies in students for their future work in the legal field; providing legal assistance to those in need; enhancing the practical knowledge, skills, and competencies of University students majoring in "Law," as well as students from other disciplines in collaboration with respective departments; ensuring access to legal assistance for socially vulnerable groups; and expanding the University's cooperation with judicial, law enforcement, justice, state authorities, local governments, and other institutions, organisations, and enterprises regardless of their organisational and legal form.

During quarantine measures (such as COVID-19) and wartime activities in the Kharkiv region, the Legal Clinic of KhAI operates online, providing legal services to the population through its website (https://www.facebook.com/groups/483046942691378).

The continuous operation of the Legal Clinic enables both full-time and part-time students to undertake academic and other types of practical training. It facilitates interactions between students and practicing professionals, such as lawyers, attorneys, judges, law enforcement officers, and representatives of state and local government bodies, during their educational process. Moreover, it promotes the implementation and application of innovations aimed at enhancing the efficiency of the University's practical training processes. The Clinic also establishes an effective mechanism for information exchange between the public, the media, and the Legal Clinic, allowing for prompt responses to the practical needs of society.

2.2. Russo–Ukrainian War Case Study

As outlined in the Strategic Plan of the Ministry of Education and Science of Ukraine until 2027, ambitiously titled "Education of the Victorious," Ukraine stands on the brink of significant transformations. Currently, the educational process in our country is taking place amidst the sounds of sirens, often during enemy shelling, and in the absence of electricity and communication. Students are losing the opportunity to learn, educators to teach, and researchers to conduct their studies. War, forced migration on one hand, and globalisation and European integration on the other, necessitate changes in approaches to education and science. Despite these obstacles, education must become a key to mobilizing resources and opportunities for the future, helping people find their place in the new realities (Education of the Victorious).

At the turn of the millennium, the development issues of higher education hold special significance for our country. Amid the ongoing resistance to armed aggression, processes to overcome managerial and economic crises, liberalise the societal structure, and build a civil society are ongoing. The rich experience gained in previous years indicates that in managing various resources of educational institutions (material, financial, educational), the organisation of preparing future pedagogical staff is of utmost importance. This preparation is conducted through a comprehensive set of educational activities, setting modern goals and tasks for educators, orienting them towards corporate values, coordinating collaborative efforts, stimulating their activity and initiative, and providing training to enhance the quality and efficiency of each employee's work (Lytvynov, O., 2023).

However, in the context of the Russian Federation's armed aggression against Ukraine, one of the most crucial issues for the sustainable development of higher education institutions (HEIs) is the creation, expansion, and development of a secure environment for both higher education seekers and all staff members. As of May 2024, over 3,500 educational institutions have suffered various degrees of damage, with nearly 400 completely destroyed. Approximately $14 billion is needed to restore the educational infrastructure, according to the latest estimates by the World Bank. Some of the damaged educational institutions cannot be restored (Due to the war, 400 educational institutions have been completely destroyed in Ukraine. Ukrinform).

The full-scale Russian invasion of Ukraine severely disrupted the work of the scientific community, had an impact on cross-border projects and forced the cessation of many research activities. Over 100 scientific and academic institutions were damaged or seized by the enemy (Ministry of Education and Science, 2023). Several unique research facilities, including the Kharkiv Institute of Physics and Technology's Neutron Source and the world's largest decameter radio telescope, UTR-2, were damaged and mined (National Academy of Science, 2022). As a result of the war, many scientists have had to suspend their research or their activities have been seriously disrupted by regular power and communications cuts, air raids and security issues (Nature, 2022). Many Ukrainian scientists face challenges due to wartime restrictions on the freedom of movement abroad for male scientists of a certain age, and the possibility of mobilisation for military service (On Mobilization Training and Mobilization, 2022). The war led to a reallocation of budgetary resources, resulting in a reduction in funding for scientific projects and a temporary disruption of international scientific co-operation. The National Academy of Sciences of Ukraine accused Russia of "deliberately destroying science in Ukraine as a profession", calling this act "scienticide (Ukrainian "Наукогубство", National Academy of Science, 2022).

Kharkiv Mayor Ihor Terekhov has addressed a letter to UN Secretary-General Antonio Guterres and UNESCO Director-General Audrey Azoulay. In the letter, Mayor Terehov highlights that Russia's actions are not only destroying Ukraine's potential but also serving the ambitions of its leadership through the use of force, blatantly disregarding international law. He particularly stressed that one of the UN Sustainable Development Goals is to ensure equitable and quality education. However, Russia's military aggression has made it impossible for Kharkiv residents to fully develop their scientific and creative potential.

The mayor's office underscored Kharkiv's reputation as a "city of students, youth, and creative intellectuals," renowned globally for its numerous educational and scientific institutions. However, during the war, educational, cultural, and sports institutions are regularly shelled. According to the city council, Kharkiv has suffered significant damage to: 796 educational facilities; 271 cultural institutions; 52 sports facilities; 34 parks and squares. Since the start of the full-scale invasion, the air raid alarms have been sounding for over 172 consecutive days, averaging 16 hours per day. Consequently, our children are compelled to continue their educationin underground schools... (In Kharkiv, nearly 800 educational facilities are damaged).

The problem that needs to be addressed is the critically low level of safety in educational institutions and the organisation of a safe educational environment in Ukraine in the context of the Russo–Ukrainian war. This situation has arisen due to several factors: insufficient number of civil protection shelter facilities in educational institutions; inadequate compliance of existing civil protection shelter facilities in educational institutions with the necessary capacity requirements, the number of evacuation exits, the availability of water supply, drainage, ventilation, heating, lighting, communication facilities, internet access, medical assistance provisions, accessibility for people with limited mobility, and the possibility of organising educational processes within these civil protection shelter facilities; low level of compliance with fire safety and technological safety legislation in educational institutions; outdated legal framework in the area of civil protection regarding the creation of safe conditions for students, pedagogical, scientific-pedagogical staff, administration, and other employees in educational institutions; lack of established security procedures for educational institutions, including the involvement of police security services (with the installation of comprehensive alarm systems) connected to centralised monitoring and response points; inadequate organisation of access control in educational institutions (fencing, stationary metal detectors, access control systems); absence of external and internal video surveillance systems in educational institutions; inaccessibility of most educational institutions and civil protection shelter facilities at educational institutions for persons with disabilities and other groups with limited mobility; insufficient coverage of educational institutions by preventive police services aimed at preventing and deterring criminal activities; insufficient awareness among participants in the educational process about their rights, responsibilities, and safety protocols; lack of knowledge among participants in the educational process about safe behavior at home and traffic rules; low level of awareness about cyber threats and safe behavior online; unpreparedness of participants in the educational process to act in emergency situations, during military actions; lack of skills among educational staff in providing first aid and psychological support to students; limited access to mental health services and psychosocial support for participants in the educational process during their studies and work, considering the impact of military aggression on their mental health; lack of a comprehensive infrastructure for psycho-emotional support and psychological assistance for participants in the educational process; inadequate conditions for inclusive education and support in the educational process for students who need it, in line with the new security conditions (Concept of Security for Educational Institutions, 2023).

Minimum safety measures required for establishing a resilient security environment in educational institutions:

- **Enhancement of the regulatory framework**: improve the legal framework in the field of civil protection to create safe conditions for the presence of educational process participants in educational institutions.
- **Law enforcement representatives,** government bodies of Ukraine, and foreign stakeholders should aim to enhance monitoring and report on every incident of armed aggression against educational infrastructure. This includes providing detailed information on the type of

educational institution, the nature of the attack, the responsible party, and other relevant details) (Filipenko, N., Spitsyna, H., Agapova, O. & Palkova, K., 2023).

- **Development and construction of civil defense structures**: equip existing and build new civil defense structures for educational institutions using reusable project designs or individual project solutions, taking into account legislative requirements on fire safety, necessary evacuation exits, water supply, sewage, ventilation, heating, lighting, internet access, medical aid facilities, and accessibility for mobility-impaired individuals, including those with disabilities.
- **Ensuring fire and technological safety**: guarantee fire and technological safety in educational institutions.
- **Implementation of early warning systems**: introduce early warning systems and evacuation procedures for participants in the educational process in the event of an attack, threat of attack, or other danger to the institution.
- **Emergency response protocols**: develop and implement procedures for emergency situations, including the detection of explosive and other suspicious objects within the educational institution.
- **Mandatory safety training for staff**: enforce mandatory safety training and qualification upgrades for teaching, scientific-pedagogical, and other staff members in educational institutions on safety issues, basic psychological interventions, psychological self-help, and citizen rights, freedoms, and obligations.
- **Creating a safe physical environment**: create a safe physical environment for students and staff in Higher Education Institutions (HEIs). When using a mixed learning format, it is essential to minimise the clutter of the institution’s premises with foreign objects, furniture, flammable materials, or any other items that may hinder evacuation.
- **Regular safety training for students**: conduct regular online and in-person training sessions with students on how to act in dangerous situations. This should include meetings with relevant professionals such as bomb technicians, emergency service personnel, tactical medicine doctors, psychologists, conflict resolution specialists, etc.

- **Updating anti-bullying measures**: develop or update anti-bullying measures, which are especially important in mixed-identity groups (including internally displaced persons or refugees).
- **Emergency information lists**: create a mandatory list of information for students and staff that can be crucial in life-threatening emergencies. This should include blood type, list of chronic diseases, essential medications (e.g., for diabetes or asthma), and primary emergency contacts (e.g., close relatives). Such lists can be lifesaving in cases of injuries, being trapped under rubble, captivity, or other emergencies.
- **Engagement of the academic community in safety efforts**: Broadly involve not only HEI staff but also students in creating a secure environment through the establishment of an official "volunteer movement" in this field. Using the data and input from students will reduce risks during extreme events and ensure personal, societal, economic, and state security. This will also foster the development of personal qualities aimed at safe behavior in the environment. Additionally, achieving a culture of safety among volunteers will address objectives such as fostering correct safety behaviors and developing personal traits geared towards safe conduct in the face of military threats.

Recommendations for Expat Scientists

In order to enable the continuity of the scientist's research, relocated abroad, the scientists need to be provided with the following:

- assistance with accommodation, allowance and residence permits for the scientist and his/her family members, schools for their children;
- support in recognizing the researcher's level of education and qualifications;
- assistance in integration of the science community and academic structures;
- assistance with funding, resources and necessary equipment;
- assistance in linguistic matters;
- provide access to the necessary databases, scientific literature and laboratories;
- facilitate the mobility of the researchers, the possibility to take part in international events.

In light of the ongoing challenges posed by the war in Ukraine, there is an urgent need for transformative approaches within the educational sector. Drawing on research from the Ukrainian-Latvian cooperation project, this questionnaire has been developed to identify and assess the risks that hinder the educational process and compromise the security of students and staff. By understanding these risks, we can formulate strategies to establish a resilient security environment, ensuring the continuity of education and research in the face of adversity.

The questionnaire will help evaluate the existing safety measures in educational institutions, identify gaps in infrastructure and emergency protocols, and develop recommendations that enhance safety and facilitate a more secure educational environment.

Through this initiative, we aim not only to address immediate safety concerns but also to contribute to long-term strategies that support the sustainable development of education and research in these challenging geopolitical times. By actively engaging the academic community in these efforts, we can work collaboratively toward creating a secure and nurturing environment for learning, fostering resilience against current and future challenges. (Annex1 and Annex 2).

Example of Comprehensive Risk Assessment and Action Algorithms During Military Emergency Events

Analysis of Critical Situation No. 1: How to act during an air alarm while conducting classes or exams?

Action algorithm for addressing critical situation No. 1: Immediately suspend teaching activities and systematically evacuate the classroom, moving swiftly to the designated bomb shelter according to the evacuation plan.

Analysis of critical situation No. 2: Verification of the presence of students and others who have not evacuated (e.g., due to health conditions) in classrooms and other facilities.

Action algorithm for addressing critical situation No. 2: Designated administrative personnel, upon the alert signal, conduct a thorough check of all educational institution premises to ensure no participants of the educational process or institution staff are left behind. Upon completion of the check, proceed to the nearest shelter. If necessary, expedite emergency medical assistance and transport the individual to a medical facility.

Analysis of critical situation No. 3: The instructor is in a shelter during an air alarm. A student begins to panic and cannot calm down.

Action algorithm for addressing critical situation No. 3: Remain calm and begin to distract the student with various exercises, including tactile ones. Seek assistance from other instructors, medical personnel, or psychologists.

Analysis of critical situation No. 4: Monitor the well-being of surrounding individuals (being in shelter is stressful by itself: the confined and usually not very friendly space can negatively affect well-being).

Action algorithm for addressing critical situation No. 4: Be attentive and monitor behavior and well-being. Regularly inquire about their well-being, what you can do to help. Students will see that you care and are concerned for them, which will significantly easy their situation.

3. Guidelines as a Check Box

In this chapter, Guidelines as a Check Box, we explore a structured approach for institutions aiming to enhance their resilience against security, operational, and infrastructure risks. Rather than viewing guidelines as mere checklists to satisfy compliance requirements, this chapter encourages institutions to adopt a deeper, more integrated approach. This allows them to genuinely safeguard their mission-critical assets, operations, and people.

1. Risk Management and Security Resilience: Institutions are guided through developing robust risk management systems that go beyond basic compliance, addressing the protection of key assets such as data and research projects. The section encourages aligning practices with international standards (like ISO 31000:2018), maintaining an updated risk register, and establishing clear responsibilities for risk assessments, particularly in international research collaborations. The focus here is on creating a culture of proactive risk management, where due diligence is embedded in daily operations to prevent unauthorized access, data breaches, or other forms of organizational harm.
2. Protecting Personnel and Students: This segment highlights the importance of comprehensive safety measures to protect staff, students, and visitors. Institutions are encouraged to create documented systems and allocate the necessary resources to support these protocols. Building a culture of risk awareness is also central, with regular training for both students and staff on safety, security risks, and foreign interference. Open channels for safety reporting are emphasized, as well as ensuring that security is seen as an enabler for a safe environment, rather than a barrier.
3. Safeguarding Infrastructure: This section provides a roadmap for institutions to secure both digital and physical assets, focusing on cybersecurity and controlled access. Cybersecurity threats—ranging from sophisticated attacks to opportunistic breaches—are examined in detail, along with protocols for monitoring high-value information and controlled

technologies. Protecting physical infrastructure is equally important, with guidelines on policies for visitors, access restrictions, and monitoring processes to prevent unauthorized access to sensitive areas.

4. Business Continuity Planning: A well-prepared business continuity plan ensures that institutions can maintain essential functions during disruptions. This section covers the identification of critical functions and personnel, securing alternate locations, and planning for transport, logistics, and resource allocation. The chapter underscores the need for a systematic approach with senior management involvement, clear crisis communication protocols, and regular stress testing to keep continuity plans up-to-date and responsive to evolving risks.

Each area in this chapter includes self-assessment questions to help institutions evaluate their current practices and identify gaps. Moving beyond a checkbox approach, these guidelines aim to create a resilient institution where safety, security, and continuity are deeply embedded in the organization's values and operations. The chapter concludes by emphasizing the importance of moving past superficial compliance to adopt a culture of proactive, meaningful engagement with guidelines, thereby strengthening the institution's long-term security and stability.

[1] Building Advanced Risk Management and Resilience to Security-Related Issues

[1.1] Risk Management and Due Diligence System

□ Has the institution identified what constitutes key assets within the scope of the model, including specific research projects or data sets?

□ Does the institution have a risk management system in place? Is it in line with international standards such as ISO 31000:2018?

□ Is the risk register updated on a regular basis?

□ Does the risk register include relevant threats, whether intentional or unintentional, that may cause damage to the assets of the organisation through techniques that result in unauthorised access, destruction, disclosure, modification or denial of service?

□ How clear are requirements to undertake proportionate risk assessments before research starts?

□ Who has responsibility for conducting risk assessments of international research projects?

□ What policies exist in the university to identify research contracts that require additional oversight due to the nature of the research and/or the type of partnership?

□ Have you taken steps to ensure that any translated versions of contractual agreements include identical terms and conditions?

□ Have clear policies and responsibilities been established for tracking foreign investment sources, including government grants, international foundations, philanthropic organisations, corporate sponsorships, and working with foreign institutions?

□ Is the system structured as an in-house control system with approved policies, allocated resources and defined responsibilities?

□ Are risk assessments at all levels, including non-academic staff, students and employees, integrated with internal oversight mechanisms for accepting external funding?

□ Is there appropriate education and training for researchers, academic staff and employees to raise awareness and understanding of the risks of hostile foreign influence?

□ Do educational programmes cover risk assessment, data security, protecting intellectual property, responsible research practices, and complying with relevant regulations and policies?

□ Have robust compliance processes been put in place, including thorough due diligence on the origin of technologies and materials, ensuring compliance with ethical sourcing and sustainability principles, and actively monitoring and auditing supply chains to prevent the use of prohibited resources?

□ Is there systematic, regular engagement with relevant national security institutions?

[1.2] Diversification of Funding Sources and Minimizing Critical Dependencies

□ Have measures been taken to diversify the sources of funding by actively seeking support from a wide range of national and international sources in order to reduce the over-reliance on a single foreign source of funding?

□ Is basic research collaboration limited to like-minded partners who share the same values?

□ Does collaboration with a wide range of like-minded international partners contribute to the creation of a robust and diverse S&T ecosystem, broadening research perspectives and reducing the risk of hostile influence on research priorities?

□ Have measures been taken for the creation of science and technology ecosystems for research and higher education, with the aim of reducing national dependencies on external risks?

□ Are measures taken to minimise critical dependencies on foreign equipment, software, technologies, intellectual property and skills?

□ Is there a systematic approach involving vigilant monitoring, risk assessment and proactive measures to identify and mitigate dependencies?

[1.3] Policies and Contractual Agreements to Protect Intellectual Property

□ What policies, tools and frameworks does your institution use to protect intellectual property (IP)?

□ Who has responsibility for signing off and monitoring contractual agreements on research collaborations?

□ What is the process for contracts and agreements put in place for non-funded research projects, such as one-to-one research collaborations between academics?

□ What kind of training is available to support researchers to take measures to protect against IP theft or leveraged transfer through cybersecurity infringements or the theft of personal property?

[1.4] Dual-use technologies and export control legislation

□ Do researchers understand the term ‘dual-use’ and know how it affects them?

□ How do researchers reasonably consider the potential for their research to become dual-use?

□ What strategies are in place to ensure compliance with export control legislation and other relevant legislative frameworks?

□ What guidance exists on when researchers should seek further advice, internally or external to the university?

[2] Self-assessment: Protecting Personnel and Students

[2.1] System

□ Does the institution have a system in place for the protection of staff, students and visitors?

□ Have the necessary policies and procedures been developed and are they documented?

□ Have roles and responsibilities been clearly defined? Have the necessary resources been allocated?

□ Is the system overseen by an audit committee or a board of directors?

□ What approvals processes are in place for staff appointments at various levels at universities?

□ Are procedures in place to ensure safety when travelling abroad, such as risk assessment, due diligence, cultural sensitivity training, vaccinations, etc.? Duty of care principle when seeking accommodation abroad?

[2.2] Risk awareness

□ Is there a system in place for reporting and raising awareness of accidents?

□ Does the organisation have a system for reporting significant incidents?

□ Has appropriate and regular training been provided to students and staff regarding safety and security risks?

□ Has a positive risk awareness culture been developed and promoted? Have the necessary resources been allocated?

□ Does the system facilitate two-way conversations with staff and students about safety issues?

□ Is there an understanding of security issues across the institution, with an emphasis on security being seen as an enabler rather than a barrier?

□ Have focal points for security issues been developed and clearly communicated to support internal discussions? Are internal resources, especially websites, clear, up-to-date and easily accessible?

□ Are staff and students trained or refreshed on foreign interference at appropriate intervals during their engagement, including during orientation or induction, when promoted or when roles are changed?

□ How do students and staff have easy access to information on foreign interference, university policies, codes of conduct and consequences for breaches of the codes?

□ What training does the university provide to staff to build capacity in the identification of potential cases of foreign interference, including harassment or intimidation?

[3] Self -assessment: Protecting Infrastructure

[3.1] Cyber Security Threats

□ Are cybersecurity threats, ranging from sophisticated attacks to opportunistic breaches, being systematically addressed?

□ Has senior management ensured that robust cybersecurity policies are developed and implemented?

□ Are effective cybersecurity risk monitoring and reporting protocols in place? Including information sharing with government and the industry.

□ Is the use of published threat assessments, such as those of CERTs, incorporated to help anticipate cyber threats?

□ Is there a specific focus on the protection of high value information, including economically, politically and commercially sensitive material?

□ Is there an emphasis on the importance of appropriate training for researchers working on high security issues, controlled technologies or areas subject to export control legislation?

□ Are policies and training packages developed that focus on segregating research materials, limiting access to sensitive data, and monitoring access?

□ Is there recognition of the vulnerability of both digital and physical infrastructure to security breaches?

□ Are physical security risks specifically addressed in institutional policies and frameworks?

□ Are measures implemented to protect both digital and physical infrastructure given case study vulnerabilities?

[3.2] Visitors and Security

□ Have frameworks, policies and risk assessments been developed to differentiate between different types of visitors?

□ Are visitors screened before, on arrival and during their stay, including verifying identity and complying with visa requirements?

□ Are there clear management and monitoring procedures for visiting students/staff? Are pre-arrival checks and ongoing visitor contact points emphasised

□ Is there senior oversight and accountability for visitor and visa arrangements?

□ Are access restrictions and visitor policies enforced? Are there clear processes for monitoring and accountability?

□ Are clear advice, information and guidance provided to visitors and staff on how to follow protocols during their time on campus?

[3.3] Protection of Sensitive Research and Materials

□ Are appropriate protective measures in place for sites where sensitive research and materials are located? Have measures been put in place to prevent unauthorised access after security breaches?

[4] Self-assessment of the Business Continuity Plan

[4.1] Identification and Formalization of Essential Functions

□ Have critical functions and processes been identified and appropriately documented?

□ Is the minimum scope of critical functions clearly defined in order to provide continuous service at a pre-defined level?

□ Is there a defined maximum acceptable duration of interruption for critical functions? Are recovery times and priorities defined?

[4.2] Critical Personnel

□ Have critical personnel, including support staff, been identified to ensure minimum continuity of critical services and processes?

□ Have critical personnel been informed of their status and responsibilities? Are they adequately trained and prepared?

□ Are procedures in place for the replacement or augmentation of critical personnel, in particular in the event that some of them are unavailable?

□ Is there a strategy in place to avoid reliance on expatriate personnel, who may be subject to restrictions on their mobility or may be part of their domestic mobilisation?

□ Is infrastructure adapted and resources allocated in a timely manner to allow for shift work, staying overnight, or extended stays at sites?

□ Are there algorithms in place for internal communication and action to be taken in crisis situations?

[4.3] Infrastructure

□ Has a alternate site been identified in a timely manner, and deemed suitable for critical functions (ensuring minimum requirements: communications support, alternative energy solutions, water availability, etc.)?

□ Have arrangements been made to relocate personnel and process equipment to the alternate site, taking into account the number of transport units and other support required, including accommodation and staffing?

□ Have opportunities been identified to recruit personnel and to purchase or lease necessary equipment, and to repair and maintain equipment, in the vicinity of the alternate site?

□ Is there a preparation plan for securing and fortifying existing infrastructure before the move, including arrangements for security guards, sandbagging of doors and windows, etc.?

[4.4] Essential Equipment

□ Is there an inventory list of critical equipment and assets, possibly marked with priority tags for evacuation?

□ Have alternatives to critical equipment and assets been identified, considering replacements that do not involve technologies from companies with questionable reputations in European Union and NATO?

□ Are contingency plans in place for the loss or failure of equipment and assets?

□ Have pre-planned actions been defined for the installation, calibration, maintenance, repair, replacement, upgrade or development of alternatives for equipment at alternative locations?

□ Is there redundancy in the power supply to information systems and is there provision for a stand-alone power supply?

□ Is there a plan in place for the timely backup of digital systems and equipment to ensure that data, systems and processes can be accessed from the alternate site?

□ Has the impact of the security of supply on the continuity of business operations been assessed, taking into account the availability of support staff, spare parts and repairs?

[4.5] Transport and Logistics

□ Have transport requirements for critical functions been identified?

□ Are there alternative means of transport that are considered in the plan?

□ Is there an assessment of the availability of drivers and specialists? Alternatives?

□ Is fuel supply planned in critical situations?

□ Are packing materials, crates for evacuating equipment and pallets included in the plan?

[4.6] Essential Services from External Suppliers

□ Is there a plan for electronic communication and voice telephony facilities, including access from alternate workstations and redundant communication and data transmitting systems?

□ Are power supply facilities, alternatives and options for off-site power suppliers clearly identified in the plan?

□ Has the availability of the Internet and access to global networks, particularly scientific and academic databases, been addressed?

□ Does it plan for the availability of natural gas and oil products and consider alternatives?

□ Have provisions been made for the availability of heating, water and waste water during the crisis? Have the requirements for external support to the national authorities in the event of a national emergency been defined, such as the prioritisation of the supply of energy, gas, petroleum products, communications and logistical support?

[4.7] Security and Resilience of Supply

□ Are at least Tier 1 suppliers identified, along with their geographic distribution, to identify vulnerabilities in the event of international supply chain disruptions?

□ Is the plan in place to avoid reliance on a single overseas supplier?

□ Are measures in place to discourage involvement in supply chains with high-risk suppliers, particularly those with reputations in European Union and NATO member states that raise concerns due to suspected privacy violations, human rights abuses, unauthorised acquisition of non-public information, or threats to national security?

□ Does the plan avoid strategic dependence on know-how, patents, intellectual property and strategic technologies, software and hardware from third countries?

□ Have the critical raw materials and resources that are necessary for the scientific work been identified in the plan?

□ Is there an assessment of the security and continuity of supply of these critical raw materials and resources? Have substitutes for critical raw materials or alternative supply chains been identified in the plan?

□ Is preference given to local supply chains and local producers, processors and service providers to ensure security and sustainability of supply?

[4.8] Algorithms for Action to be Taken in the Event of a Crisis

□ Does the plan allocate all available resources to maintain and restore critical functions and business processes and ensure the provision of critical services within defined limits during a crisis?

□ Are there protocols and plans in place for internal and external crisis communications?

□ Is there a procedure for activating and operating the crisis management team during a crisis? Emergency procedures and actions to restore critical functions, minimise damage and implement recovery scenarios or relocate operations?

□ Are crisis protocols established for all categories of staff (academic, students, contractors), including safety procedures and evacuation of non-essential staff and students?

[4.9] Systematic Approach (Integrated at All Levels)

□ Are the people responsible for business continuity planning identified? Are the necessary resources allocated?

□ Are the processes, documents, algorithms and protocols for business continuity planning formalised and subject to regular review?

□ Is senior management involved in business continuity planning and approval processes?

□ Are regular reviews, self-assessments, audits, regular exercises and stress tests organised to improve the business continuity system?

Concluding Insights and Recommendations

In light of the evolving security landscape, this handbook offers a solid framework for academic and scientific institutions, focusing on enhancing resilience and safeguarding operations against diverse security threats. In today's interconnected world, universities face increasing challenges from external influences that can threaten their scientific autonomy and integrity. Universities can minimise external influence and ensure the protection of their values, partnerships and academic freedom through collaboration, awareness and prioritisation of security.

The establishment of compliance and internal risk management systems within universities that strengthen institutional resilience and protect against external threats is essential to the management of these risks. By implementing these recommendations, universities can protect their research, staff, students and reputation.

Core recommendations include promoting a culture of preparedness, integration of risk management at levels, ensuring business continuity and promoting security awareness. This includes allocating the necessary resources and creating comprehensive risk management compliance systems, adapting internal systems and processes, and promoting cultural changes that emphasise the importance of scientific and educational autonomy and security.

The handbook provides a comprehensive guide aimed at enhancing risk management and institutional resilience in academic and scientific institutions, with a strong emphasis on addressing security-related threats. Outlined below are **key recommendations that institutions can implement to bolster their resilience and maintain operational integrity in the face of these challenges:**

1. Academic institutions must establish sophisticated risk management frameworks to counteract foreign interference and other security risks.

This involves implementing rigorous due diligence processes, safeguarding intellectual property, and diversifying funding streams to minimize reliance on external entities.

2. The importance of cybersecurity cannot be overstated, with institutions needing to invest in advanced protective measures to secure sensitive information and digital infrastructure. Equally critical is the physical security of campuses, requiring proactive steps to prevent potential security breaches.
3. Institutions must develop comprehensive business continuity plans to maintain essential operations during disruptions, such as natural disasters, cyberattacks, or geopolitical conflicts. This includes clearly identifying critical functions, assigning roles to key personnel, preparing backup infrastructure, and establishing effective crisis communication protocols.
4. The experiences of Ukrainian educational institutions during the Russo-Ukrainian war underscore the need for academic systems to remain adaptable in extreme conditions. Measures such as building civil defence structures, implementing evacuation protocols, and providing psychological support for students and staff are essential for maintaining operational resilience.
5. The successful implementation of risk management strategies hinges on the active involvement of the entire academic community, including faculty, students, administrative staff, and external partners like national security agencies. A collective commitment is required to foster a culture of security and preparedness.
6. Ongoing education and training on security risks, crisis management, and adherence to international standards are crucial for both staff and students. Institutions must regularly update their members on safety protocols, strategies to mitigate risks, and the potential impact of foreign interference on academic freedom and research integrity.

This handbook addresses the urgent needs of Ukraine's educational and scientific ecosystem and neighboring countries impacted by Russian aggression, with the goal of strengthening resilience and ensuring operational continuity in challenging environments. Developed through the Latvian–Ukrainian Joint Programme, it provides practical guidance for institutions facing crisis situations, with insights from Ukrainian institutions' experiences during the conflict. The framework extends beyond Ukraine, offering EU institutions a comprehensive tool to enhance risk management, safeguard intellectual independence, and prepare for security threats, including those arising from war situations.

The handbook provides a strategic framework for academic and scientific institutions to enhance their resilience and safeguard their operations. By following its recommendations, institutions can protect their assets, personnel, and reputations, ensuring they continue to operate effectively in times of crisis. A proactive commitment to these guidelines is essential to maintain institutional autonomy, security, and long-term continuity.

In conclusion, fostering a proactive security culture within academic and scientific institutions is paramount to long-term resilience. Beyond immediate threat mitigation, this entails an ongoing commitment to security as an integral part of institutional identity. This proactive approach should include regularly updated risk assessments, a commitment to transparency in handling risks, and a focus on developing partnerships with governmental and international organizations for enhanced support. Integrating security measures with institutional values of academic freedom and scientific integrity ensures a balanced approach, where both security and autonomy are protected.

Furthermore, regular scenario-based training exercises, including simulations of cyber threats, physical breaches, and hybrid warfare tactics, will prepare both staff and students for real-world situations. These exercises can strengthen decision-making skills, response times, and the capacity for effective crisis communication. Encouraging continuous professional development in areas of cyber and physical security is also critical to adapting to the evolving threat landscape.

Ultimately, by following these comprehensive recommendations and committing to a shared culture of security and resilience, institutions can create a robust foundation for future growth and innovation while upholding their core values. In this way, academic institutions can ensure they remain safe havens for knowledge, research, and intellectual advancement despite the complexities of the modern security landscape.

Successful implementation of the recommendations of this Handbook depends on the collective commitment of all university stakeholders –faculty, staff and students.

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.

Additionally, we want to acknowledge that under Martial law, President Volodymyr Zelenskyy declared martial law on 24 February 2022, in response to the Russian invasion of Ukraine. Universities in Ukraine are operating under exceptional circumstances, with martial law significantly impacting their capacity to fully implement these recommendations. Despite facing infrastructure damage, human resource challenges, and financial strain due to the ongoing war, Ukrainian universities have shown remarkable resilience in continuing their educational and research activities. These institutions provide an inspiring example of adaptability in times of crisis, demonstrating the importance of both institutional strength and international support in overcoming such challenges.

References

1. Aisling, I. (2023). The fight to keep Ukrainian science alive through a year of war. *Nature*. https://www.nature.com/articles/d41586-023-00508-0
2. Amendments to the Law of Ukraine “On Mobilization Training and Mobilization” No. 2196-IX. (2022). Article 23. https://zakon.rada.gov.ua/laws/show/2196-20#n5
3. Appeal of the National Academy of Sciences of Ukraine to the International Scientific Community. (2022). National Academy of Sciences of Ukraine. https://www.nas.gov.ua/UA/Messages/Pages/View.aspx?MessageID=9728
4. Cabinet Regulation No. 508. (2021). Procedures for surveying critical infrastructure, including European critical infrastructure, and for planning and implementation of security measures and continuity of operation.
5. Concept of Security for Educational Institutions. (2023). Approved by the Decree of the Cabinet of Ministers of Ukraine on April 7, 2023, No. 301-r.
6. Cybersecurity Culture Guidelines: Behavioural aspects of cybersecurity. (2019). ENISA. https://www.enisa.europa.eu
7. Due to the war, 400 educational institutions have been completely destroyed in Ukraine. (2023). *Ukrinform*. https://www.ukrinform.ua/rubric-society/3832111-v-ukraini-vnaslidok-vijni-povnistu-zrujnovani-400-zakladiv-osviti.html
8. Education of the Victorious: Presenting the strategic action plan. (2023). Ministry of Education and Science of Ukraine. https://mon.gov.ua/ua/news/osvita-peremozhciv-predstavlyayemo-strategichnij-plan-diyalnosti
9. Filipenko, N., Spitsyna, H., Agapova, O., & Palkova, K. (2023). The concept of comprehensive security for higher educational institutions: Ukrainian and European experience. *Integrated Computer Technologies in Mechanical Engineering – 2023 (ICTM 2023)*, 317-327. https://link.springer.com/chapter/10.1007/978-3-031-60549-9_23
10. Guidelines to counter foreign interference in the Australian university sector. (2021). University Foreign Interference Taskforce. https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector
11. How China’s economic aggression threatens the technologies and intellectual property of the United States and the world. (2018). White House Office of Trade and Manufacturing Policy. ISBN-10: 1722711027.
12. Hundreds of UK academics investigated over weapons links to China. (2021). *The Times*. https://www.thetimes.co.uk/article/hundreds-of-uk-academics-investigated-over-weapons-links-to-china-bpcks76bv

13. Implementation of the 5G cybersecurity toolbox. (2023). European Commission. https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox
14. In Kharkiv, nearly 800 educational facilities are damaged: Terekhov appeals to the UN. (2024). *Media Port.* https://www.mediaport.ua/u-kharkovi-poshkodzheni-mayzhe-800-osvitnikh-obyektiv-terekhov-zvernuvsya-do-oon
15. ISO 31000:2018 – Risk management – Guidelines.
16. Joske, A. (2019). *The China Defence Universities Tracker: Exploring the military and security links of China's universities.* https://www.aspi.org.au/report/china-defence-universities-tracker
17. Läänemets, M. (2020). Academic cooperation with the People's Republic of China: Dangers and temptations. *International Center for Defence and Security.* https://icds.ee/en/academic-co-operation-with-the-peoples-republic-of-china-dangers-and-temptations/
18. Lukashevych, S. Y. (2020). Future crime: Criminogenic threats of the future. In V. Ya. Tatsiiy, A. P. Hetman, Yu. H. Barabash, & B. M. Holovkin (Eds.), *Law enforcement in the context of the coronavirus crisis: Materials of the panel discussion of the IV Kharkiv International Legal Forum* (pp. 144-148). Kharkiv: Pravo. http://criminology.nlu.edu.ua/wp-content/uploads/2020/11/4j-forum-2020-zabezpechennya-pravoporyadku-v-umovah-koronakrizi.pdf
19. National Security and Investment Act: Guidance for the higher education and research-intensive sectors. (2023). 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
20. Order of the National Police of Ukraine No. 398, April 12, 2024, "On approving the regulation on the Department for the Organization of the Educational Security Service of the National Police of Ukraine."
21. Overview of the current state of education and science in Ukraine under Russian aggression as of February 2023. (2023). *Ministry of Education and Science.* https://mon.gov.ua/ua/ministerstvo/diyalnist/mizhnarodna-dilnist/pidtrimka-osviti-i-nauki-ukrayini-pid-chas-vijni
22. Robison, A. (2018). Academic freedom and the Confucius Institutes. *The Diplomat.* https://thediplomat.com/2018/02/academic-freedom-and-the-confucius-institutes/
23. Tavolzhanskyi, O. V. (2016). Criminological aspects of cybercrime in modern conditions. *Journal of Eastern European Law,* (31), 80–86. http://dspace.nlu.edu.ua/bitstream/123456789/17724/1/Tavolzhanskyi_80-86.pdf

24. Ukrainian researchers in times of war survey. (2022). *UA Science Reload*, 5–10. https://www.uascience-reload.org/2022/07/05/ukrainian-researchers-in-times-of-war-results-of-survey/
25. Yazan, N., & Filipenko, N. (2024). Principles of security in Ukrainian educational institutions as an element of the critical infrastructure sector. In *Interdisciplinary Discourse: Resilience of Critical Infrastructure [Electronic Resource]: Conference Proceedings of the Scientific and Practical Conference* (pp. 144–150). Kharkiv: KHAI.
26. В Україні внаслідок війни повністю зруйновані 400 закладів освіти. (2023). *Укрінформ*. https://www.ukrinform.ua/rubric-society/3832111-v-ukraini-vnaslidok-vijni-povnistu-zrujnovani-400-zakladiv-osviti.html
27. Литвинов, О. (2023). Університетська арена думок. Про корпоративну культуру і не лише про неї. https://www.facebook.com/profile.php?id=61551406107546
28. Освіта переможців: представляємо стратегічний план діяльності. (2023). Міністерство освіти і науки України. https://mon.gov.ua/ua/news/osvita-peremozhciv-predstavlyayemo-strategichnij-plan-diyalnosti

Annex 1

Questionnaire

Assessment of risk management and resilience in academic and research institutions

1. To what extent are you familiar with the concept of risk management in an academic environment?
   - Not at all familiar
   - Slightly familiar
   - Moderately familiar
   - Very familiar
   - Extremely familiar

2. Are you aware of the potential risks posed by foreign interference in research and academic activities?
   - Yes
   - No
   - Not sure

3. Have you had any training in the identification and mitigation of security issues in research and academia?
   - Yes, comprehensive training
   - Yes, some training
   - No, but I am aware of the issues
   - No, I have not received any training

4. Does your department/institution do due diligence on acceptance of foreign funding or co-operation?
   - Yes, always
   - Yes, sometimes

- No, rarely
- No, never
- Not sure

5. Are you part of a risk assessment process for foreign partnerships or investments?
   - Yes
   - No
   - Not applicable

6. Are you aware of institutional policies to prevent foreign interference in research?
   - Yes
   - No
   - Not sure

7. Do you think current policies and procedures are effective in managing foreign influence risks?
   - Very effective
   - Somewhat effective
   - Not effective
   - Not sure

8. How well do your organisation's cybersecurity measures protect against unauthorised access?
   - Very well
   - Somewhat well
   - Not well
   - Not sure

9. Have you ever experienced a cyber security breach at your organisation or have you become aware of one?
   - Yes
   - No
   - Not sure

10. Are you aware of any protocols in place for protecting physical infrastructure (e.g., laboratories, equipment) from security threats?
    - Yes
    - No
    - Not sure

11. Does your organisation have a business continuity plan for emergencies like natural disasters, cyber-attacks or other crises?
    - Yes
    - No
    - Not sure

12. Have you been trained on what to do in the event of an emergency that could affect the operation of the institution?
    - Yes, comprehensive training
    - Yes, some training
    - No, but I am aware of the procedures
    - No, I have not received any training

13. How well prepared is your organisation to operate in the event of crisis, e.g. geopolitical conflict ?
    - Very prepared
    - Somewhat prepared
    - Not prepared
    - Not sure

14. What additional measures do you think need to be taken to improve your institution's risk management and resilience? (Open-ended)

15. Would you like to receive more training or resources on how to manage the risks associated with foreign interference, cyber security or business continuity?
    - Yes
    - No
    - Maybe

15. What kind of training would be the most beneficial for you to receive? (e.g., workshops, online courses, informational materials)

16. What is your current role at the institution?
    - Student
    - Academic staff
    - Research staff
    - Administrative staff
    - Other (please specify)

17. What is the location of your organisation?
    - Latvia
    - Ukraine
    - other country in the EU
    - non-EU country

17. How long have you been affiliated with the institution?
    - Less than 1 year
    - 1–3 years
    - 4–7 years
    - 8+ years

18. How do you perceive the threat of foreign influence on science and research in your country? Please rank from 1 to 5
    (1 - not threat, 5 - real threat). Answers: 1, 2, 3, 4, 5

19. Have you received any training in understanding the risks of hostile foreign influence in academia and research? Answers: Yes / No

20. Please indicate the three most important training courses that would be useful in order to gain a better understanding of the risks involved:
    1. Risk assessment practices
    2. Cyber security
    3. Data security and privacy
    4. Intellectual property rights protection
    5. Protocols for conducting responsible research

6. Regulatory compliance
7. Sanctions and reputational risk
8. export control or dual-use technologies
9. business continuity of the research and academic processes
10. Policies to prevent discrimination, bullying and harassment
11. Fraud and corruption prevention

21. Do you have easy access to information about foreign interference, university policies, codes of conduct and consequences for breaches of the codes? Answers: Yes / No

22. Have you been familiarised with or made aware of the guidelines and regulations for operating and evaluating projects with foreign partners (non-NATO/EU)? Answers: Yes / No

23. Do you have a designated person or structure that can provide you with advice or guidance on issues of external co-operation with countries that are not members of the EU/NATO? Answers: Yes / No

24. Are you familiar with policies and procedures regarding gifts and donations? Answers: Yes / No

25. Are you aware of the policy on ethical behaviour and the prevention of the risk of corruption, including the declaration of conflicts of interest? Answers: Yes / No

26. Have you received adequate training on the risks associated with the physical security of the campus or of the academic facilities? Answers: Yes / No

27. Do you feel safe in university buildings and campuses? Answers: Yes / No

28. Have you received adequate training on the risks associated with cybersecurity? Answers: Yes / No

29. Do you know who you need to report an accident or any suspicious activity to? Answers: Yes / No

30. Are you aware of fire safety, emergency procedures, evacuation routes and assembly points? Answers: Yes / No

31. Do you know the protocols for how to act in the event of a crisis? Answers: Yes / No

32. Are you aware of the risks and practices in place to minimise critical dependencies on foreign equipment, software, technology, intellectual property and skills? Yes / No

33. Is it possible to ask for an evaluation of the partner you are considering? Yes / No

34. Is there an opportunity for you to seek advice or consultation on foreign risk assessment at any stage of your projects, studies or research activities? Answers: Yes / No

35. When travelling abroad, do you have access to advice, risk assessment or cultural training? Answers: Yes / No

36. Do you know how to identify and protect research that could benefit the nation's economic interests or could be related to dual-use technology? Answers: Yes / No

37. Is there a way for you to proactively provide feedback and recommendations to the university on how to improve the systems? Answers: Yes / No

Annex 2

Questionnaire

"Education during the Russo-Ukrainian War"

1. What form of education do you use:
   - online (exclusively remotely);
   - blended learning (both online and on-campus);
   - attend the educational institution regularly.

2. How often are you forced to miss classes?
   - at least twice a week;
   - periodically, no more than once a month;
   - I do not miss at all.

3. What is your absence from classes mainly associated with?
   - air raid alerts, power outages, or lack of internet due to accidents, scheduled outages, etc.;
   - residing in temporarily occupied territories;
   - living in frontline and de-occupied areas;
   - living away from home;
   - learning only online;
   - illness or other reasons.

4. Do you objectively feel that your level of education and perception of materials has deteriorated?
   - yes, I feel it has;
   - no, everything remains as before.

5. What traumatic psychological conditions have you experienced since the beginning of the war?
   - fear of loud noises;
   - fear of being in confined spaces;

- irritability and apathy, indifference to learning and past interests;
- outbursts of unfounded anger, aggression;
- fear of the future;
- sleep problems, intrusive nightmares of death;
- memory and concentration problems;
- other.

6. What events related to the war have you witnessed or been involved in?
   - separation from family and loved ones;
   - relocation to another region of the country;
   - shelling and bombings;
   - prolonged stay in cold premises;
   - moving abroad;
   - being in occupation;
   - witnessing the death of family members or loved ones;
   - loss of housing;
   - experiencing hunger and lack of water; other.

7. Do you consider your current place of residence unsafe?
   - yes;
   - no;
   - I hesitate to answer.

8. Do you consider being in your educational institution safe?
   - yes;
   - no;
   - I hesitate to answer.

9. Are you satisfied with the level of safety in the educational environment at your institution of higher education?
   - yes;
   - no;
   - I hesitate to answer.

10. Are you satisfied with the level of communication with professors and university administration representatives during the war?
    - yes;
    - no;
    - I hesitate to answer.

11. What measures to improve the level of safety in the educational environment at your institution of higher education need to be improved:
    - upgrading existing and constructing new civil defense structures for educational institutions;
    - strengthening the established procedure for organizing security at institutions of higher education, including involving National Police authorities;
    - training in emergency response skills, combat actions, providing emergency medical care, and ensuring psychological support;
    - broadest engagement in creating a safe environment for students engaged in it by establishing a “volunteer movement” in this area and granting it official status;
    - other ____