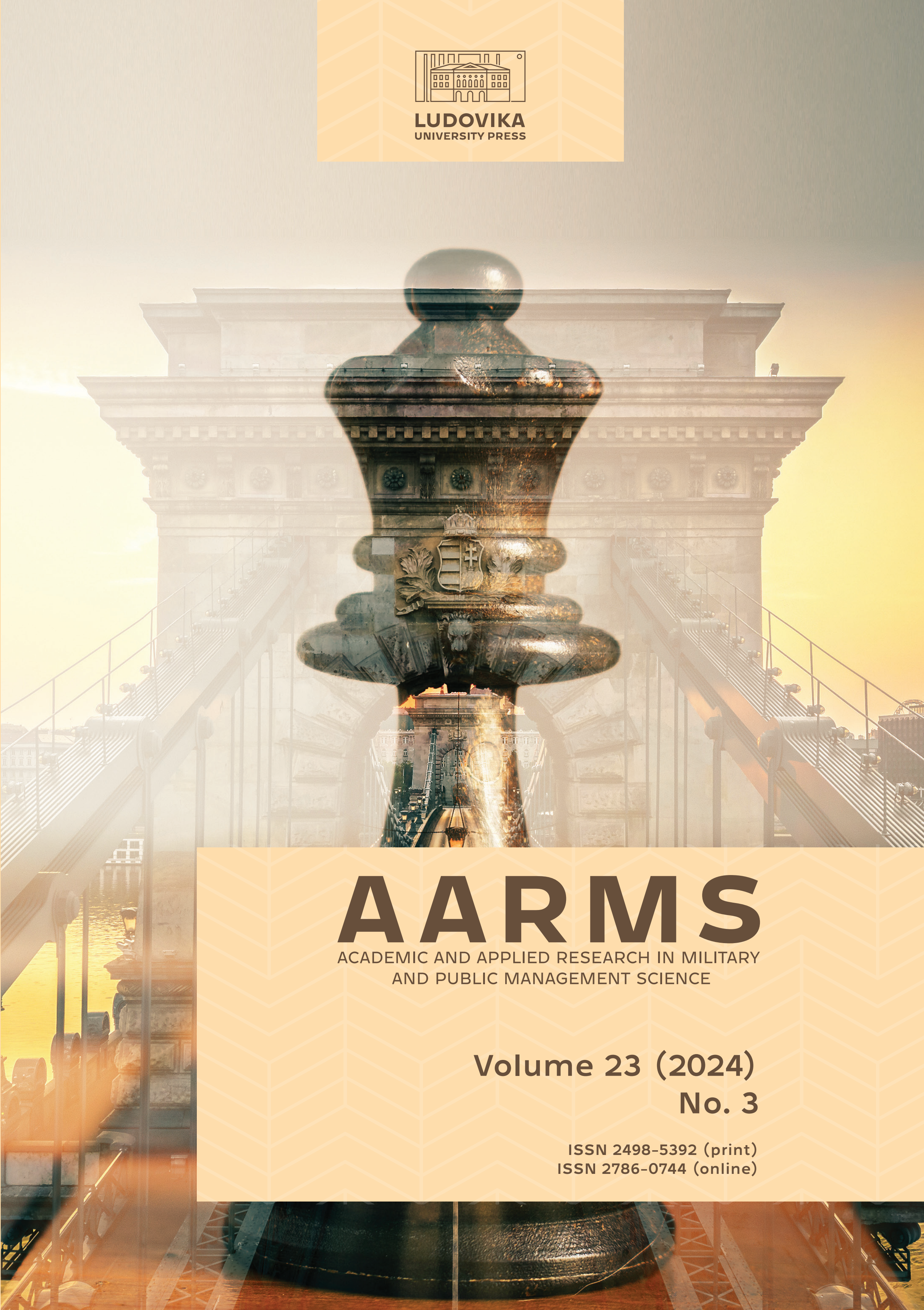

LUDOVIKA
UNIVERSITY PRESS

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY
AND PUBLIC MANAGEMENT SCIENCE

Volume 23 (2024)
No. 3

ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security and public management.

AARMS is published in one volume of three issues per year by the Ludovika University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

Articles and other text material published in the journal represent the opinion of the authors and do not necessarily reflect the opinion of the Editors, the Editorial Board, or the Publisher.

All correspondence should be addressed to Prof. József PADÁNYI, DSc, Editor-in-Chief,
Ludovika University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary
aarms@uni-nke hu

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE

Volume 23
No. 3
2024

An International Journal of Security, Strategy, Defence Studies,
Military Technology and Public Management
Published by the Ludovika University of Public Service
József PADÁNYI (Chair of the Editorial Board)
József SOLYMOSI (Honorary Chair of the Editorial Board)

Editorial:

József PADÁNYI (Managing Editor)
Ferenc GAZDAG (Editor)
Ákos ORBÓK (Editorial Assistant)

Publisher:

Ludovika University of Public Service, Ludovika University Press
Responsible for Publishing:
Gergely DELI Rector

Copy editor:

Zsuzsanna GERGELY

Typeset and print by the Ludovika University of Public Service
ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

Contents

AARMS Vol. 23, No. 3 (2024) 5–19.

10.32565/aarms.2024.3.1

Building an OT Security Microgrid Testbed

Gergő GYEBNÁR[1]

This paper introduces the development of an Operational Technology (OT) security microgrid testbed. The testbed is aligned with the IEC 62443 standard and structured to simulate and mitigate potential security risks within OT systems. It serves as a platform for evaluating cybersecurity strategies through test scenarios and cases, aimed at enhancing the resilience and responsiveness of OT environments to cyber threats. The work described here lays the foundational framework for subsequent research, focusing on cybersecurity measures, including MITRE ATT&CK-based methodologies and detection strategies using machine learning. This initial exploration emphasises the importance of creating a versatile, realistic testing environment to understand and address the unique security challenges faced by OT systems.

Keywords: *Operational Technology, cybersecurity, microgrid, testbed, IEC 62443, MITRE ATT&CK, security testing, feasibility study, simulation, cyber threat intelligence*

Introduction

Operational technology (OT) refers to the use of hardware and software for controlling industrial equipment, primarily interacting with the physical world. This collective term encompasses SCADA, DCS, PLC, SYS, CNC and other equipment utilised by critical infrastructures and the military.

The rise in OT security concerns is mainly attributed to IT–OT convergence. This convergence often requires accessing data from sites that were previously engineered to remain disconnected from the internet. Consequently, the cyber resilience of these control systems is notably compromised. Essentially, adversaries can achieve significantly greater impacts with minimal resource investments. Another significant concern regarding OT security is that since the emergence of Stuxnet, the development and research of OT vulnerabilities have followed an exponential trend. This applies to both exploit development and vulnerability research in the field of OT, with an increasing focus on the creation of "killware" – malware designed with the intention of potentially harming or even killing people.

[1] PhD student, Ludovika University of Public Service, Faculty of Military Sciences.

Given the unique nature of OT systems in the field of cybersecurity, it is advisable to establish a testbed to better model cybersecurity test cases. Many industries have digital twins, which are digital models of planned or actual physical products, systems, or processes that serve practical purposes such as simulation, integration, testing, monitoring and maintenance. However, in cases where a digital twin is not available, it is worthwhile to create a testbed. This paper examines this possibility and proposes building one testbed through a Microgrid project.[2]

A microgrid is a local energy system capable of generating, distributing and controlling electrical energy as a single controllable unit. When connected to the main grid, microgrids can operate in island mode or be sufficiently regulated to fulfil their tasks, thereby revolutionising energy management. Microgrids can be beneficial in industrial parks, commercial zones such as shopping centres, critical infrastructures, or even within smaller residential communities, supplying local energy needs and, if necessary, promoting the stability of the local electrical grid.[3]

The microgrid is a topic that enables the creation of a heterogeneous environment. However, to better prepare the environment for future test cases, it is advisable to examine the relevant frameworks and their recommendations. The testbed considers the NIST SP 800-82 Rev. 3, IEC 62443-4-2 and MITRE ATT&CK frameworks, considering the ICS (Industrial Control Systems) and Enterprise matrices in the latter case.[4]

The purpose of this paper is to develop a testing environment that might be suitable for emulating cybersecurity attacks, detecting them, automating the investigation of detections and automating the management of entire incident response scenarios. It is important to examine the methodology to perform the most complete and realistic simulation possible so that the attacks and their defences correspond as closely as possible to reality. The environment must be modularly developed for both the OT and IT aspects, along parameters that are currently given on both the attacking and defensive sides.

Test cases

IEC 62443-4-2

To model IEC 62443-4-2 test cases in a microgrid testbed, it is needed to create specific test scenarios that address the key security requirements outlined by the standard. Given the criteria and the detailed security measures within each category, below is a structured approach to modelling test cases for a microgrid testbed:

- CR: Component requirement which is common to all types of components
- SAR: Software application requirement
- EDR: Embedded device requirement
- HDR: Host device requirement
- NDR: Network device requirement

[2] Hexagon AB 2024.
[3] Szabó 2022.
[4] MITRE ATT&CK 2024.

Identification and authentication control

One of the fundamental aspects of securing any cyber–physical system is the assurance that each human and/or system user is uniquely identified and authenticated with multi-factor where it is possible. In this context, a test scenario and case focusing on the user identification and authentication process as prescribed by IEC62443 standards are presented.[5]

- *Test scenario: Validate unique identification and authentication for creating user accounts (CR) using a registration process*
  The establishment of a mechanism for user identification and authentication is essential to ensure that each user accessing the microgrid system is properly authorised. This test scenario is designed to validate the process of creating user accounts, involving a registration process that must guarantee the uniqueness and security of user identifiers.
- *Test case: Simulate user account creation (e.g. "Create Account, T1136") and verify the uniqueness of user identifiers*
  In this corresponding test case, the process of user account creation is simulated. The key objective is the verification of the uniqueness and security of the user identifiers assigned during the registration process. Through this, it is aimed to demonstrate the efficacy of the system's ability to prevent unauthorised access and ensure that each account is uniquely linked to an authorised user.
- *Test scenario: Implement multi-factor authentication for accessing microgrid services*
  In this scenario, multi-factor authentication is mandated for all human users attempting to access the system, ensuring that multiple pieces of evidence are provided before access is granted.
- *Test case: Conduct simulated login attempts with multi-factor authentication requirements (e.g. "Multi-Factor Authentication Interception, T1111")*
  In this test case, simulated login attempts incorporating multi-factor authentication requirements are conducted. The primary objective is to assess the multi-factor authentication system in preventing unauthorised access.
- *Test scenario: Ensure unique identification and authentication for software processes and devices (EDR)*
  This test scenario is crafted to ensure that all software and devices interacting with the microgrid system are uniquely identified and authenticated, thereby safeguarding the integrity and confidentiality of the microgrid operations.
- *Test case: Validate the identification and authentication process for microgrid software and embedded devices*
  In this corresponding test case, the identification and authentication process for microgrid software and embedded devices is validated. The focus is on verifying the uniqueness and security of the identifiers assigned to each component involved in the system. The process is designed to demonstrate the system's capability to identify and authenticate nearly all software processes and devices accurately, thereby preventing any unauthorised or malicious activities within the microgrid system.

[5] International Society of Automation 2024.

Use control

Other aspects of securing in any cyber–physical system is ensuring that both authorisation enforcement and the recording of auditable events are rigorously applied according to predefined security policies. This involves not only verifying that each user's activities and access rights align with their designated roles – using mechanisms such as supervisor overrides and dual approval processes where necessary – but also ensuring that all significant actions within the system are traceable and verifiable through meticulous recording and storage of auditable events. This enhances the ability to perform thorough security audits and maintain accountability. In this context, test scenarios and cases focusing on both authorisation enforcement and the management of auditable events, as prescribed by IEC62443 standards, are presented.

- *Test scenario: Test authorisation enforcement by mapping user permissions to specific roles (CR)*
  In this scenario, the permissions are mapped to specific roles to ensure that each user is granted access according to their role's privileges. This methodical mapping is crucial to maintaining operational integrity and compliance with security policies.
- *Test case: Validate supervisor override and dual approval functionalities within the microgrid system*
  During the test case, the functionalities of supervisor override and dual approval within the microgrid system are validated. The objectives are to confirm that the supervisor override can effectively alter control settings during critical situations.
- *Test scenario: Ensure auditable events are logged and stored within the microgrid environment (SAR)*
  The logging and storage of auditable events within the microgrid environment are crucial for tracking and reviewing activities to ensure security and to be able to run further queries to define alerts and investigations and compliance. This scenario is designed to ensure that all significant actions and decisions are recorded, providing a trail that can be audited to detect any unauthorised or inappropriate activities.
- *Test case: Generate auditable events and verify proper storage capacity and response to audit processing failures*
  In this test case, auditable events are generated, and it is verified whether they are properly stored with adequate capacity and whether the system correctly responds to audit processing failures. The aim is to evaluate the system's ability to record and maintain an accurate and comprehensive log of all auditable events, ensuring that data integrity and availability are upheld in case of system audits.

System integrity

Maintaining system integrity is crucial in securing cyber–physical systems, therefore, the testbed as well. This encompasses ensuring the integrity of both communications and the software and information they carry.

- *Test scenario: Authenticate communication channels (HDR)*
  In this scenario, communication channels are authenticated to ensure that data transmitted across them is intact and secure from unauthorised access. Authenticating these channels is vital to maintaining the overall security of the infrastructures, protecting it against potential intrusions and data breaches.
- *Test case: Generate a malicious network traffic injection, conduct communication integrity tests to detect and/or prevent*
  Here, a simulated scenario involving the injection of malicious PCAP into the system is used to test the security of the communication integrity measures. The test aims to challenge the implementation of authentication and detection or prevention mechanisms of the communication security protocols.
- *Test scenario: Validate software and information authenticity (CR)*
  This scenario involves validating the authenticity of software and information within the system through automated integrity checks. It ensures that the software and data have not been tampered with and remain reliable and accurate for operational needs.
- *Test case: Implement automated notification mechanisms for integrity violations during normal operations*
  The corresponding test case focuses on the implementation of automated notification mechanisms that alert operators to any integrity violations. This proactive approach is designed to quickly address and mitigate any issues that arise, thereby maintaining the operational integrity of the microgrid.

Data confidentiality

Preserving data confidentiality is a paramount concern in cyber–physical systems, where sensitive information must be safeguarded against unauthorised access.

- *Test scenario: Test the erasure and verification of shared storage resources (EDR)*
  This scenario addresses the challenge of maintaining information confidentiality by focusing on the erasure and verification of shared storage resources. The aim is to ensure that once data is no longer needed or when it is imperative to prevent unauthorised access, it can be securely and effectively erased, leaving no remnants that could be exploited.
- *Test case: Execute data erasure procedures and verify successful and secure erasure of sensitive information*
  In this test case, data erasure procedures are executed to demonstrate the system's ability to remove sensitive information securely and completely from shared storage resources. The process includes verification steps to ensure that the data is irrecoverable, thereby upholding the strict confidentiality requirements necessary for the integrity and security of the microgrid operations.

Restricted data flow

Effectively managing the flow of information within systems is critical for enhancing security and operational efficiency. Network segmentation plays a one of the core roles in this by isolating various components and restricting data flow between them.

- *Test scenario: Evaluate network segmentation (NDR)*
  This scenario focuses on evaluating network segmentation within the microgrid to ensure that data flows are properly restricted according to security policies. The aim is to prevent unauthorised access and mitigate potential cyber threats by dividing the network into distinct segments that operate independently.
- *Test case: Test zone boundary protection mechanisms to deny all, permit by exception, or operate in island mode when necessary*
  In this test case, the effectiveness of zone boundary protection mechanisms is tested. These mechanisms are designed to "deny all" access by default, "permit by exception" based on predefined security criteria or allow components to "operate in island mode" when isolation is necessary for security or operational reasons. The test evaluates how well these mechanisms enforce the segmentation policies and protect sensitive areas from unauthorised access or data breaches.

Timely response to events

The capability to respond promptly to security incidents will be the most examined test case in the future of this lab environment. This involves ensuring that audit logs are accessible and secure and queried by certain risk tolerance thresholds, providing the necessary data to analyse and respond to events effectively.

- *Test scenario: Access to audit logs (SAR) and continuous monitoring capabilities*
  This scenario aims to guarantee that audit logs are not only accessible, but also monitored continuously. Ensuring programmatic access allows for automated systems to analyse log data efficiently, facilitating quick detection of anomalies and security incidents. Continuous monitoring ensures that these systems are always aware of the current state of the microgrid, ready to respond at any moment.
- *Test case: Validate the accessibility and security of audit logs during and after simulated events*
  In this test case, the accessibility and security of the audit logs are validated during and after simulated security events. The test involves generating events and then verifying that the logs can be accessed and analysed to understand what occurred.

Resource availability

Ensuring the availability of resources is fundamental for maintaining the operational continuity and *safety,* especially under adverse conditions such as cyberattacks. Denial of Service (DoS) protection is a critical aspect of safeguarding these systems against disruptions that could compromise their functionality.

- *Test scenario: Manage communication load (NDR) to protect against Denial-of-Service attacks on microgrid components*
  This scenario focuses on managing the communication load across microgrid components to protect against potential Denial-of-Service attacks. The goal is to prevent such attacks from overwhelming the system, which can disrupt operations and reduce the availability of critical resources.
- *Test case: Test resource management and emergency power systems to ensure continuous availability during critical operations*
  In this test case, the robustness of resource management is tested to ensure they provide continuous availability and functionality during critical operations. The test evaluates the systems' ability to handle increased loads and maintain operational stability, even under potential DoS attack conditions. It ensures that essential services and components remain functional, demonstrating the system's resilience and reliability.[6]

Through these exemplary test cases, compliance with IEC62443 standards can be assessed, and areas needing enhancement may be identified to strengthen the overall security posture of the microgrid testbed.

MITRE ATT&CK

The value of threat intelligence lies in its capacity to thwart cyberattacks through effective countermeasures. An illuminating framework for understanding this concept is David Bianco's Pyramid of Pain.[7]

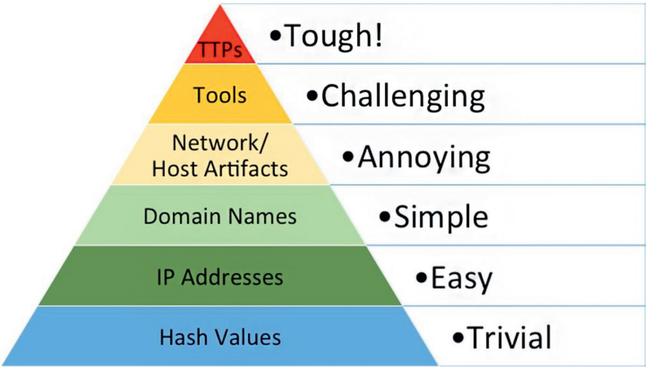

Figure 1: David J. Bianco's Pyramid of Pain
Source: AttackIQ Enterprise 2022

[6] Fritsch 2021.
[7] AttackIQ Enterprise 2022.

This model illustrates how various indicators used to detect adversary activities correlate with the level of difficulty or "pain" it inflicts upon them when those indicators are rendered ineffective. By detecting and mitigating Tactics, Techniques and Procedures (TTPs), we address the entirety of adversary behaviours rather than just their tools. This holistic approach maximises effectiveness, as it compels adversaries to expend considerable effort adapting to new strategies. Consequently, timely prevention or response to adversary TTPs compels them to undertake the most arduous task: acquiring new skills. By amalgamating the outcomes of this evaluation with an analysis of sector specific TTPs, actionable insights emerge, guiding efforts towards areas where they can inflict the greatest obstacles for potential attackers.[8]

Hence, establishing TTP-driven test cases as robust constants within security operations is imperative. Exemplary blueprints for both Operational Technology (OT) and Enterprise realms can be formulated and validated within the microgrid framework available at: https://github.com/blackcellltd/Heatmaps

In military jargon, a heatmap can be interpreted as an RCP (Recognized Cyber Picture), which requires specialised threat intelligence.

By structuring test scenarios and corresponding test cases based on the specific IEC 62443-4-2, and MITRE ATT&CK security criteria and requirement categories, there is an opportunity to effectively model and evaluate the security posture of a microgrid testbed. These test cases should be executed in a controlled environment that mirrors real-world microgrid operations to accurately assess security controls and identify potential vulnerabilities or weaknesses. Continuously refine and iterate on test scenarios based on test results to enhance the overall security of the microgrid infrastructure.

Architecture and design

Printed circuit board (PCB)

One central component and visualisation element of a microgrid is the printed circuit board (PCB), on top of which the components are applied using a screen-printing technique. Essentially, there are three input units: the grid supply, the wind turbine and the solar panel. Each is connected to a main switch, a power unit and a power meter. The three sources charge the central battery unit, which supplies electricity to the lighting of two barracks, illustrated with two conventional bulbs to represent understandable consumption.

[8] Black Cell Ltd. 2023.

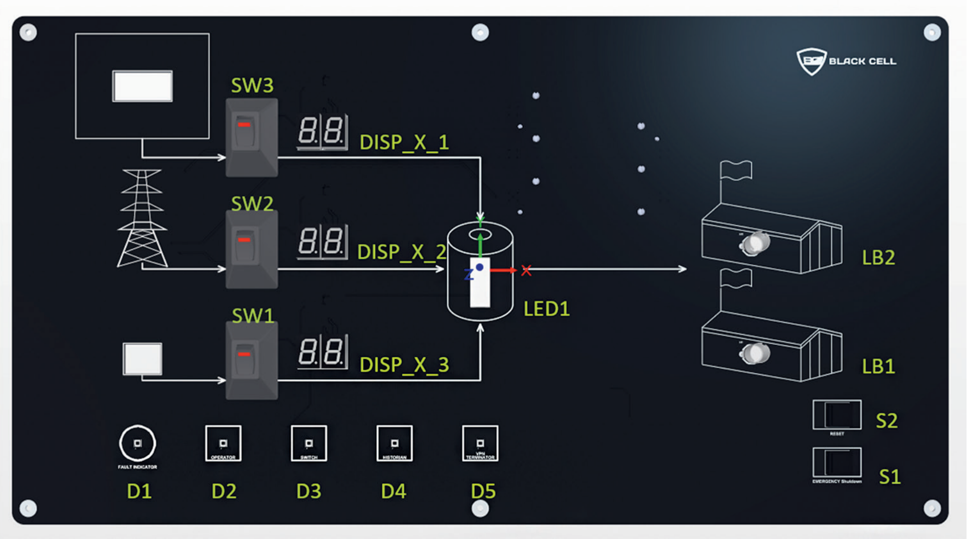

Figure 2: Printed circuit board by Gergo Gyebnar
Source: compiled by the author

IED

A microcontroller at the heart of a microgrid's power unit plays a pivotal role in orchestrating the charging process and overall energy management. It is an Intelligent Electronic Device (IED) as defined by the IEC 62443 standard, which focuses on the security for industrial automation and control systems. This microcontroller is equipped with software designed to manage inputs from diverse energy sources, such as solar panels, wind turbines and grid supplies, ensuring optimal charging of the central battery unit.

As an IED, the microcontroller performs real-time monitoring and control of the power flow, dynamically adjusting to changes in energy production and consumption. It integrates various functions such as data acquisition, automatic control and communication with other IEDs in the network to ensure seamless operation and efficiency. By leveraging advanced algorithms, it can predict energy needs, manage storage and even perform tasks like demand response and load balancing.

In compliance with IEC 62443, this microcontroller incorporates robust security features to protect against cyber threats. These features include secure communication protocols, authentication and authorisation mechanisms, and regular security updates to safeguard the microgrid's operations. This ensures that the microgrid not only operates efficiently but also securely, preventing unauthorised access and ensuring the integrity and availability of the power supply.

Through its advanced capabilities and adherence to international security standards, the microcontroller epitomises the evolution of power management systems into smart, autonomous and secure components of the modern energy landscape.[9]

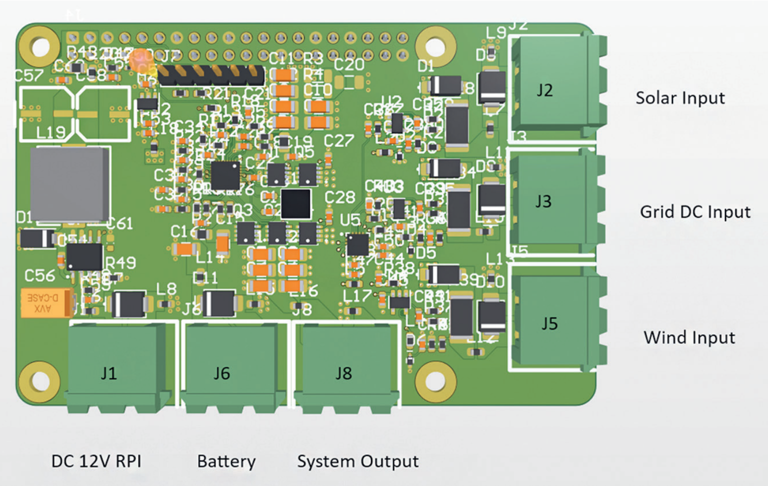

Figure 3: Raspberry Pi based microcontroller (IED) by Gergo Gyebnar
Source: compiled by the author

PLC

The Click Programmable Logic Controller (PLC), equipped with both digital and analogue cards, serves as a versatile and efficient component in a microgrid testbed environment. Its primary function is to provide reliable control and automation of the microgrid's operations, enabling the integration and management of various energy sources, storage solutions and load demands. With its ability to handle both digital (on/off) signals and analogue (variable) signals, the Click PLC can monitor and control a wide range of devices and parameters, from simple switches to complex sensors measuring voltage, current, or temperature.[10]

Integration into microgrid testbed

In a microgrid testbed, the Click PLC can perform several critical functions:

- Energy management: By analysing inputs from solar panels, wind turbines and grid connections, the PLC can optimise the charging of battery storage units and manage the distribution of power to meet the demands efficiently.

[9] Nabidoust 2024.
[10] Crestani Tasca et al. 2020: 21–22.

- Load control: The PLC can prioritise and control various loads within the microgrid, implementing strategies like load shedding or demand response to maintain stability and efficiency.
- Interfacing with IEDs: As part of a broader network of Intelligent Electronic Devices, the Click PLC can communicate and coordinate actions, enhancing the microgrid's resilience and adaptability.
- Data acquisition and monitoring: Collecting data from both digital and analogue sources, the PLC provides valuable insights into the performance and health of the microgrid, enabling predictive maintenance and system optimisation.

IEC 62443 test case opportunities

The incorporation of IEC 62443 standards into the operation of the Click PLC within a microgrid testbed offers numerous opportunities for enhancing security and reliability:

- Security by design: Implementing IEC 62443 from the design phase ensures that the PLC is equipped with necessary cybersecurity measures, such as secure authentication, encrypted communications and access control.
- Anomaly detection: Through continuous monitoring of network traffic and device behaviour, the PLC can help identify potential security threats or anomalies, enabling proactive responses to mitigate risks.
- Resilience testing: Leveraging the IEC 62443 framework, the microgrid testbed can simulate cyberattack scenarios to test the resilience of the PLC and the microgrid's response mechanisms, ensuring that operations can be maintained even under adverse conditions.

Historian

An integrated SQL Server acting as a Historian Server in a microgrid setup plays a crucial role in data management, analysis. This specialised database system is designed to efficiently collect, store and retrieve vast amounts of time-series data generated by the microgrid's various components, including energy production units (like solar panels and wind turbines), consumption data and operational logs from devices like the Click PLC.

Functionality in a microgrid

In the context of a microgrid, the SQL Historian Server's primary functions include:

- Data aggregation and storage: It collects and archives real-time and historical data on energy generation, usage, system performance and events across the microgrid. This data is vital for operational analysis, optimisation and regulatory compliance.
- Trend analysis and reporting: By analysing historical data, the server can identify patterns, predict future energy needs and optimise the balance between energy

supply and demand. It supports decision-making processes related to energy trading, maintenance scheduling and infrastructure investment.
- Performance monitoring: The server monitors the health and efficiency of the microgrid, providing alerts for anomalies or failures. This enables predictive maintenance, reducing downtime and extending the life of equipment.

Other components

Linux web server: Acts as the backbone for data management and user interface, hosting applications that collect, process and display data from across the microgrid. It facilitates remote monitoring, control and optimisation of the testbed operations.[11]

- Operator workstation: The central hub for human operators, equipped with software tools for system monitoring, data analysis and decision-making. It is where strategies are formulated and deployed, leveraging data served by the Linux web server.
- Switch: Manages data flow within the microgrid network, ensuring that communications between devices, sensors and the control systems are efficiently routed. It supports the segmentation of networks for better performance and security.
- Firewall: Protects the microgrid's digital infrastructure from external threats and unauthorised access, ensuring that only legitimate communication and control commands pass through to the microgrid components.[12]
- Human Machine Interface (HMI): Provides a graphical interface for real-time interaction with the microgrid systems, offering a visual overview of operations, alarm status and control options for quick adjustments and interventions.
- Load simulator: LED: Simulates electrical loads within the microgrid to test how well the system can manage and distribute power under various demand scenarios. LEDs represent energy consumption patterns, helping to analyse the efficiency of power distribution.
- Emergency shutdown button: A critical safety feature allowing immediate cessation of all microgrid operations in case of an emergency, helping to prevent damage to equipment or hazards to personnel.
- Reset button: Enables the quick restoration of system operations following tests, faults, or after emergency shutdowns, ensuring the microgrid testbed is readily brought back to its operational state.
- Fault indicators: Visual or auditory signals that alert operators to system abnormalities or failures, facilitating rapid diagnosis and troubleshooting of issues within the microgrid.
- Power supply: Provides stable and reliable electrical power to the testbed components, ensuring that all devices and systems are operational for testing and simulation purposes.

[11] Thompson 2024.

[12] GnosisX 2023.

- Battery: Acts as energy storage within the microgrid, simulating how real-world systems store excess energy for later use, contributing to the efficiency and resilience of the grid.
- Renewable energy source simulator: Comprising Solar Panel and Air Turbine simulators, these components mimic the behaviour of actual renewable energy sources, allowing the testbed to evaluate how well the microgrid integrates and utilises renewable energies in various conditions.

Conclusion

In conclusion, this paper presents the development of an Operational Technology (OT) security microgrid testbed, interpreted as a feasibility study. This testbed is structured around the IEC 62443 standard through the opportunity for testing of tailored use cases of the OT environment's specific vulnerabilities and threat landscape but fit for the purpose for MITRE ATT&CK based research and development. The testbed offers an approach to identifying, analysing and mitigating potential security risks,[13] and provides the ability for essential security prerequisites for in-depth research into specialised security strategies. By integrating defined technical test cases, the resilience and responsiveness of the proposed systems against cyber threats could be effectively evaluated.

This paper is the first part of a series that forms the foundation of my research. Its purpose was to present, as a kind of feasibility study, how to build an OT testbed for defining cybersecurity test cases. Subsequent parts of the series will focus on presenting and analysing the military recognised cyber picture (RCP). This part will centre on the military interpretation and adoptability of the MITRE ATT&CK, utilising Cyber Threat Intelligence and SIEM. The latter is related to designing, automating and incorporating Detection as code within an Elastic stack.[14]

Due to the characteristics of OT systems' cybersecurity, it is necessary to deal with mirrored traffic, where a network IDS (Intrusion Detection System, Suricata) and the Zeek network querying language will play a central role. The latter is essential for interpreting OT protocols and for inventory purposes, highlighting that not only detection coverage but also log source analysis is extremely important. Further advanced detections will be introduced, such as passive vulnerability scanning and the exploration of honeypots as an option.[15]

In the fourth part, the necessary dataset and the appropriate alert system will be available, thus the construction of the attack environment will be based on MITRE CALDERA foundations. This will create a central repository for attackers, where attack campaigns can be easily orchestrated.[16]

[13] Wesley 2022.

[14] French 2023.

[15] Satta–Bennacer 2023.

[16] Nachaat 2022: 55–57.

Following this, the key part of my research focuses on the investigation of alerts and the management of events, including the modelling and comparison of tracing processes by machine models against human performance. This will be done using real-world SOC metrics, via TTP IDs. The main hypothesis of my research is: Can machine learning perform more effectively and reliably than a SOC Level 1 analyst? The final and in my opinion most useful part of the series will focus on attacking and defending machine learning within the framework of MITRE ATLAS. The outcome of this concluding section will be a comprehensive offensive and defensive capability, specifically within the AI dimension.[17]

References

AttackIQ Enterprise (2022): *What is the Pyramid of Pain?* Online: www.attackiq.com/glossary/pyramid-of-pain/

Black Cell Ltd. (2023): *Sector Specific MITRE ATT&CK Heatmaps for Detection Engineering.* Online: https://github.com/blackcellltd/Heatmaps

Crestani Tasca, Laurence – Pignaton de Freitas, Edison – Rech Wagner, Flávio (2020): A Study on the Performance Impact of Programmable Logic Controllers Based on Enhanced Architecture and Organization. *Microprocessors and Microsystems,* 76, 21–22. Online: https://doi.org/10.1016/j.micpro.2020.103082

French, David (2023): *From Soup to Nuts: Building a Detection-as-Code Pipeline.* Online: https://medium.com/threatpunter/from-soup-to-nuts-building-a-detection-as-code-pipeline-28945015fc38

Fritsch, Sebastian (2021): *IEC 62443-4-2 Use Case Industrial Firewall.* Online: www.teletrust.de/fileadmin/user_upload/2021-TeleTrusT-IEC_62443-4-2_Use_Case_Industrial_Firewall.pdf

GnosisX (2023): *pfSense.* Online: https://medium.com/@contact_45426/pfsense-3616ceb0ded0

Hexagon AB (2024): *Digital Twin Solution for Projects and Operations.* Online: https://exploreali.hexagon.com/interactive/digital-twin-solution-for-projects-and-operations

International Society of Automation (2024): *ISA/IEC 62443 Series of Standards.* Online: www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Liaghati, Christina (2024): *MITRE ATLAS Overview.* Online: www.dau.edu/sites/default/files/2024-03/MITRE%20ATLAS%20Overview%20for%20sharing.pdf

MITRE ATT&CK (2024): *Enterprise Matrix.* Online: https://attack.mitre.org/matrices/enterprise/

Nabidoust, Fatemeh (2024): *EMI Filter and PFC (Power Factor Control) Schematic #AltiumDesigner.* Online: www.researchgate.net/publication/379861549_EMI_Filter_and_PFC_Power_Factor_Control_Schematic_hashtagAltiumDesigner

Nachaat, Mohamed (2022): Study of Bypassing Microsoft Windows Security Using the MITRE CALDERA Framework. *F1000Research,* 11, 55–57. Online: https://doi.org/10.12688/f1000research.109148.3

[17] Liaghati 2024.

Satta, Abdelwahhab – Bennacer, Samir (2023): *Industrial Control Systems Security with Elastic Security and Zeek.* Online: www.elastic.co/blog/industrial-control-systems-elastic-security-zeek

Szabó, Gergely Gábor (2022): *Mit jelent a mikrogrid és mire használható?* Online: https://szgg.hu/mit-jelent-a-mikrogrid-es-mire-hasznalhato/

Thompson, Katrina (2024): *The 10 Most Common Website Security Attacks (and How to Protect Yourself).* Online: www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself

Wesley, Lee (2022): *Developing OT Security Monitoring Use Cases.* Online: www.linkedin.com/pulse/developing-ot-security-monitoring-use-cases-wesley-lee/?trk=public_post

10.32565/aarms.2024.3.2

Hungary's Eastern Opening Policy and Cooperation with the Turkic States in the Fields of Trade, Transport and Energy

Ali Kılıçarslan TOPUZ[1]

The present study depicts Hungary's eastern opening policy as to when and how it was initiated, then analyses Hungary's increasing economic, transport and energy relations with the Turkic countries, namely, Azerbaijan, Kazakhstan, Kyrgyzstan, Türkiye, Turkmenistan and Uzbekistan. In the first part, the reasons and expectations of the Hungarian Government in initiating the eastern opening are explained and the priorities the Hungarian Government put forward in starting this initiative are mentioned. In the second part, the development of the idea of the Organization of Turkic States and the road to institutionalisation is summarised and Hungary's link into the system, which is a critical element of the Eastern Opening, is delved into. In the following section, the economic benefits that Hungary is seeking to reach in the relations with the Turkic states are underlined and then the increasing trade with Turkic states are put forward as part of the developing commercial relations with special reference to Hungary's observer status in the Organization of Turkic States. In the fourth part, the increasing significance of the Middle Corridor, which is the route that links China to Europe through Central Asia, is shown and the importance attached to this corridor by the Hungarian Government is summarised. In the fifth part, the energy cooperation between Hungary and the Turkic states is mentioned, with which Hungary exerts efforts to become a hub for energy in Europe. In the conclusion part, after a summary of Hungary's achievements from the eastern opening policy and the relations with the Turkic countries, the potential of Hungary's opening to the Turkic world is explained.

Keywords: *Hungary's global–eastern opening policy, Organization of Turkic States, trade cooperation, transport cooperation, energy cooperation*

Introduction

During the period when the wave of the fall of communism in 1989 was affecting the Eastern Bloc just like other parts of the world, the Republic of Hungary was proclaimed on

[1] Ludovika University of Public Service, e-mail: alikilicarslantopuz@gmail.com

23 October 1989 and the country peacefully transitioned into a democratic parliamentary republic. The foreign policy of the Republic was based on three strategic pillars which were to "deepen Hungary's relations with developed countries and integrate into the Euro-Atlantic union, establish good neighbourly relations with the countries in its region, and ensure that Hungarians outside the border of the country have their rights".[2] These priorities in foreign policy were to a large extent followed by the consecutive governments of Hungary until 2010 when the Orbán Government came to office for the second time since the proclamation of the Republic in 1989.

In the professional circles of the Hungarian state administration, especially in the Ministry of Foreign Affairs, the transformation of foreign relations was on the agenda from time to time, but still in the 1990s Euro-Atlantic integration and the neighbourhood were the focus of foreign policy activity. Some regional concepts were created in the middle of the 1990s, such as the CIS countries, the Mediterranean region and the Balkans. Further to that, the Hungarian foreign relations strategy that was completed in 2008 also returned to the main strategic directions such as competitive Hungary in the European Union, successful Hungary in the region, Hungary being responsible in the world. However, it was the second Orbán Government which took office in 2010 which formulated for the first time Hungary's "global opening" and/or "eastern opening" program. The government program emphasised that Hungary needs a new global economic opening, which also meant opening to the East while keeping the advantages Hungary enjoyed as a member of the European Union. The Hungarian export economy must also be linked to the rapid development of China, Russia, India and other East Asian economies. This would open new markets for Hungarian agricultural products, the processing industry and tourism. The professional discussion paper of the Foreign Trade Strategy aimed at three-way geographical diversification of Hungarian foreign trade, the first of which is the "powerful eastern opening", all to reduce the vulnerability of the Hungarian economy: "Export development to eastern countries is based on the objective that domestic enterprises benefit through their exports from the increase in imports of dynamically developing economies (China, India, Russia)." The strategy specifically emphasises the priority of opening up to China, Russia, India, Korea, Türkiye, Africa and the Gulf region, as well as the CIS and ASEAN countries.[3]

In 2010, in addition to the European and global economic crisis, the preparations for the impending EU presidency made it essential to further think about and expand the foreign policy priorities established by the late Prime Minister József Antall after the regime change. Added to this was the fact that Hungary also applied for non-permanent membership of the UN Security Council, and in case of success, a stronger global diplomatic presence than before would have been necessary. The government program called for restoring Hungary's authority, increasing its international influence, and establishing relations with Eastern countries on a new basis in addition to the alliance with the West. The expert work started in the summer of 2010 at the Ministry of Foreign Affairs, the task of which was to lay the foundation for this modified foreign policy priority system – regional policy,

[2] Varga 2000: 117–118.

[3] Nagyné Rózsa 2016: 191–192.

Euro-Atlantic orientation, and global opening and involving researchers – to examine the East, Africa and Latin America.

On 19 December 2011, Foreign Minister János Martonyi presented the strategic document "Hungarian Foreign Policy after the Hungarian Presidency of the Council of the European Union" at the Hungarian Institute of International Affairs and on 20 December at the Foreign Affairs Committee of the Parliament, which summarised the strategic directions of Hungarian foreign policy. It was then that the term "global opening" first appeared in writing, formulated as a foreign policy program, but it was nothing new in the sense that it was a summary of all the strategic elements that the government, including the Ministry of Foreign Affairs, has been following for a year and a half. The "global opening", therefore, has been the revitalisation of Hungary's relations that have fallen into the background in foreign policy over the past years, strengthening action in the international community and increasing activity in the field of dealing with global challenges. Of all the designated geographic and thematic areas, the five priority areas of global opening in geographical terms were: the post-Soviet region, Asia, the Middle East and North Africa, the sub-Saharan Africa and the Sahel, and Latin America. While in a thematic sense, it meant issues that apparently do not necessarily directly affect Hungary, but are important in a global context, and are therefore gaining importance in international life (e.g. terrorism, world food, world health, the ecological state of the seas). The aim of the "global opening" was to strengthen Hungary's international positions and territorial diversification of Hungarian foreign trade, but aspects such as moral responsibility for the world's common interests and job creation also played a role.

One of the tools for implementing the global opening was the existing foreign affairs structure, and at the same time, new representations were also opened as part of the process. The other tool was Hungary's activities in the UN and other global and/or regional organisations, as well as the establishment of relations with countries in which Hungary cannot open a representative office in the foreseeable future. In order to enforce and implement the global opening program, the Deputy State Secretariat for Global Affairs was established in the Ministry of Foreign Affairs.

Parallel to the program of global opening, the program of "opening to the east" appeared in the foreign policy rhetoric, which was primarily associated with Prime Minister Viktor Orbán. As part of the Széll Kálmán Plan 2.0, the Hungarian Government in 2012 adopted a new foreign trade strategy, the main goal of which was to diversify and increase Hungarian exports. And the direction of these export strategy was aimed at Asian markets.[4]

Particularly from June 2012, when the position of Secretary of State for Foreign Affairs and Foreign Trade was established in the Prime Minister's Office, Péter Szijjártó, from March 2013 was the Government Commissioner responsible for Hungarian–Russian economic relations and the coordination of Hungarian–Chinese bilateral relations. Viktor Orbán already spoke in 2010 about the fact that "the wind is blowing from the east in the world economy", but the term opening to the east was first used in May 2011, in Paris. Hungary wanted to adapt to the changes in the global world economy with the policy

[4] Bernek 2021: 74.

of opening up to the East. Although the concept of the East was not precisely defined, the primary target areas of the Opening to the East program were Russia, the CIS countries (mainly the Caucasus and Central Asia), East Asia, especially China, and the Arab countries. That is, Hungary must increase its trade turnover with these states and attract capital from these countries. The goal of opening up to the East was to increase Hungarian export markets geographically; its main pillars are the growth of export activity, a more balanced export structure and the "internationalisation" of small and medium-sized enterprises. One of the key elements of the Eastern opening was the opening of trading houses, which the Hungarian state also took part in implementing, and whose task was to assist and coordinate the export activities of export-capable small and medium-sized companies. The first trading house was opened in Baku (Azerbaijan) on 5 December 2012.[5]

The development of the idea of the Organization of Turkic States and the road to institutionalisation

The fall of communism in 1989 and the disintegration of the Soviet Union in 1991 had big impacts all over the globe. This great incident, which heralded the starting of a new era for the liberation of lives, markets, borders and minds, brought the end of the Soviet Empire which almost for 100 years enslaved different nations. The peoples of the republics in the Soviet Union were torn away from their original cultural elements by the artificial concept of Sovietisation. The policy of Sovietisation was forced particularly upon the Turkic republics in the Soviet Union. A coercive process imposed on the peoples of the Turkic countries, namely Azerbaijan, Kazakhstan, Kyrgyzstan, Turkmenistan and Uzbekistan, fundamentally altered their cultural and social structures through the suppression of local traditions and the imposition of Soviet political, economic and linguistic policies.[6]

Among the Turkic republics, Türkiye was the only country who had not fallen under the yoke of the Soviet Empire. This plain fact was putting a critical responsibility on the shoulders of the Republic of Türkiye who could not turn a blind eye to the developments in the collapse of the Soviet Union. In fact, only very few scholars and politicians predicted the fall of the Soviet Union[7] and Türkiye was no exception in this regard. The end of the Soviet Union brought both challenges and opportunities with it. Türkiye, although it could be said to be unprepared for the collapse, took the first initiative to start a process of building the initial pillars for the establishment of cooperation with the Turkic states in 1992. As a matter of fact, Türkiye has been the first country to recognise the independence of the Turkic states. In this context, Türkiye, taking into consideration among many other aspects, the fraternal ties, the political, economic, cultural and linguistic challenges and opportunities, started the cooperation process for Turkic-speaking states in 1992. In the foundation period for the newly established Turkic republics, the main purpose was to rapidly initiate the statehood and take the prestigious place they deserve in the international

[5] Nagyné Rózsa 2016: 192–195.

[6] Roy 2005: 58.

[7] Stone 2019: 230.

community. Türkiye aimed to help the young Turkic republics in their transformation to liberal democracy and market economy.

The process called the "Heads of State Summit of Turkic-Speaking Countries" commenced in 1992 with the initiative of Türkiye. The first summit was realised on 30–31 October 1992 in Ankara hosted by the then President of the Republic of Türkiye Turgut Özal. The Head of State of the Republic of Azerbaijan, Ebulfez Elcibey, the Head of State of Kazakhstan, Nursultan Nazarbayev, the Head of State of the Kyrgyz Republic, Askar Akayev, the Head of State of Uzbekistan, Islam Karimov and the Head of State of Turkmenistan, Saparmurad Niyazov took part and contributed to the Summit. The final document of the Summit was the Ankara Declaration which foresaw the harmonisation of customs regulations among the Turkic states, the foundation of a free trade area which would allow the free flow of goods and services, the establishment of an investment and development bank, the development of telecommunications in addition to railroads, highway and air way connections, the transfer of the natural resources of Turkic countries to Europe via Türkiye, and finally the development of the coordination and cooperation among Turkic countries in the field of economy in order to integrate the Turkic countries into the global economy.[8]

After the first summit in 1992, which put forward the goal of the Turkic states for more cooperation, the leaders of the Turkic states came together in the following summits for 10 times, held in 1994, 1995, 1996, 1998, 2000, 2001, 2006, 2009 and 2010, respectively, each of which had a different theme and purpose.[9]

In the 9th Summit held in Nakhchivan; the four Turkic States, namely, Azerbaijan, Kazakhstan, Kyrgyzstan and Türkiye signed the "Nakhchivan Agreement on the Establishment of the Cooperation Council of Turkic-Speaking States" on October 2009 which was a significant step taken for the institutionalisation of the process. The Nakhchivan Agreement transformed the process into the structure called the "Cooperation Council of Turkic-Speaking States" or in short, the "Turkic Council". After the institutionalisation process, Turkic Council consists of the Council of Heads of State, the Council of Foreign Ministers, the Senior Officials Committee, the Council of Elders and the Secretariat in İstanbul. The 10th Summit of the Turkic-Speaking States was held in İstanbul on 15–16 September 2010 and the "Cooperation Council of the Turkic-Speaking States" was established. Ambassador Halil Akıncı from the Republic of Türkiye was assigned as the first Secretary General of the Turkic Council as for Türkiye's leading role and the host country for the venue of the Secretariat. The following Secretary Generals assumed their positions with the rule of alphabetical order. Respectively, following Ambassador Halil Akıncı, Ambassador Ramil Hasan from Azerbaijan between 2014 and 2018 and Ambassador Baghdad Amreyev from Kazakhstan between 2018 and 2022 took office. Currently, since November 2022 Ambassador Kubanychbek Omuraliyev from Kyrgyzstan is the Secretary General.

Following the 10th Summit in İstanbul after the institutionalisation of the process, the first Summit of the Turkic Council was held in Almaty on 20–21 October 2011 with

[8] Organization of Turkic States 2022.

[9] Ministry of Foreign Affairs of the Republic of Türkiye 2024.

the focus on economic and commercial cooperation. From 2011 onwards until 2023, 10 summits were held with different themes from educational, scientific and cultural cooperation to transportation, tourism, media and information technologies. In 2018, Hungary with its linguistic, cultural and ethnic affinity to the Turkic world joined the Turkic Council at the 6th Summit in Cholpon Ata as an observer. In his speech in Cholpon Ata, Prime Minister Viktor Orbán stated that Hungarian is a language related to Turkic languages and that Hungarians are standing on foundations of Hun–Turkic origins.[10]

On 19 September 2019, the inauguration ceremony of the "Representation Office of the Turkic Council in Hungary" was realised whereby the only Representation Office of the Turkic Council was opened which aimed at being a bridgehead of the Turkic countries to Europe. In the 7th Summit of the Turkic Council in Baku in 2019, Uzbekistan became a full member.

The 8th Summit of the Turkic Council was a historic summit which was held in İstanbul on 12 November 2021 with the theme of "Green Technologies and Smart Cities in the Digital Age". With this summit, the Turkic Council changed its name and became the "Organization of Turkic States" (OTS) referring to a further and deeper cooperation will of the member states. In this historic Summit during which the 30th year of the independence of the Turkic States was celebrated, Turkmenistan received an observer status. In addition to the name change, Turkmenistan, which holds a strong geostrategic position with its natural resources became part of the OTS system. Another factor which makes the 8th Summit a historic one is the adoption of the "Turkic World Vision 2040" document which sets out the Organization's long-term goals and tasks.

The 9th Summit of the OTS was held in Samarkand in 2022 which was another historic Summit where the Turkish Republic of Northern Cyprus was granted an observer status. None of the OTS members, except for Türkiye recognises officially the Turkish Republic of Northern Cyprus. One other element that makes the Summit a historic one is the focus on the Middle Corridor with the cooperation in trade, transportation and energy.

The 10th Summit of the OTS was held in Astana on 3 November 2023 with the motto of Turktime, which reflects the visions of the Turkic states for their will and ambition to bring the Turkic states to a much stronger level in the world with the cooperation areas it has been operating. In the 10th Summit also the ECO was granted an observer status. The 11th Summit of the OTS is planned to be held in Bishkek on 24 October 2024.

Currently, the OTS is operating in 31 areas of cooperation. These areas are political, economic, customs, transport, tourism, education, information and media, youth and sports, diaspora, information and communication technologies (ICT), energy cooperation, health cooperation, migration, agricultural, justice, humanitarian issues and development, Muslim religious institutions, space cooperation, human resources, international organisations, family and social policy issues, ministries of internal affairs/police, ministries of emergency and disaster management, consular affairs, official research centres, coordination committee of Turkic Cooperation Organizations, ministers of environment and ecology, mapping institutions, agencies responsible for land registry and cadastre and cultural relations. In each cooperation area, the officials from member and observer states meet regularly and look

[10] Miniszterelnök 2018.

for ways to increase cooperation and coordination among the Turkic states. Hungary is also contributing to these cooperation areas.

There are affiliated and related institutions of the OTS, which are the International Organization of Turkic Culture (TURKSOY), the Parliamentary Assembly of Turkic States (TURKPA), International Turkic Academy, Turkic Culture and Heritage Foundation, Turkic Chamber of Commerce and Industry and Turkic Investment Fund, and OTS is an umbrella organisation for Turkic cooperation mechanisms.

As part of the Eastern Opening policy of the Hungarian Government and the impetus reached in developing the bilateral relations with Türkiye, Hungary became observer at the TURKPA in 2014, received an observer status in the International Turkic Academy in 2017 and signed an MoU with the TURKSOY in 2019.[11]

The implementation of the eastern opening policy towards the Turkic states and economic relations

Most of the Hungarian trade was realised with the EU countries before the initiation of the Eastern Opening and in fact, the policy was aimed at increasing the political and commercial ties with the eastern countries including the Turkic states. Aside from China, Russia, Japan and South Korea, the Turkic States have been credible partners in the eastern opening. Türkiye has always been a crucial partner but now with the implementation of the eastern opening to the Turkic states, namely Azerbaijan, Kazakhstan, Kyrgyzstan, Türkiye, Turkmenistan and Uzbekistan, Türkiye became a key country for the development of relations with the aforementioned countries. The diverse economy of Türkiye and the energy potential of the Turkic countries introduced a significant opportunity in terms of trade relations.

Shortly after the introduction of the Eastern Opening, the number of diplomatic representations of Hungary in the Turkic countries and the embassies of the Turkic countries in Budapest increased. For the opening dates of the embassies of Hungary in the Turkic states and the embassies of Turkic states in Budapest, see Table 1.

Table 1: Opening year of embassies of Turkic states in Budapest and Hungarian embassies in the Turkic states

Opening dates of Hungarian embassies in the Turkic states	Republic of Azerbaijan Baku 2012	Republic of Kazakhstan Almaty 1993	Kyrgyz Republic Bishkek 2020	Republic of Türkiye Ankara 1924	Republic of Uzbekistan Tashkent 2017
Opening dates of embassies of Turkic States in Budapest	Embassy of the Republic of Azerbaijan in Budapest 2004	Embassy of the Republic of Kazakhstan in Budapest 1993	Embassy of the Kyrgyz Republic in Budapest 2022	Embassy of the Republic of Türkiye in Budapest 1924	Embassy of the Republic of Uzbekistan in Budapest 2023

Source: compiled by the author

[11] Egeresi 2020.

Accordingly, there has been a sharp increase in the number of bilateral visits, as well. The rapprochement between the Turkic states and Hungary became more concrete when Hungary received observer status in the Parliamentary Assembly of Turkic States (TURKPA) in 2014. The relations reached their peak point when Hungary received an observer status in the then Cooperation Council of Turkic-Speaking States – Turkic Council in 2018 at the 6th Summit in Kyrgyzstan. Following this development, during the Extraordinary Meeting of the Council of Foreign Ministers held in Budapest in 2019, the Representation Office of the Turkic Council was opened. The Representation Office is the only office of the Organization of Turkic States (OTS) in Europe which plays a crucial bridging role between the OTS states and the European countries. Naturally, the Representation Office added to the speed of the relations between Hungary and the OTS as it played an important role by hosting a number of official events since the date of its establishment.

As part of the increasing relations with the Turkic states, the Hungarian Government in order to push forward and encourage economic relations, opened credit lines for the companies from the OTS member states. The Hungarian Eximbank has opened a credit line worth a total of USD 1.5 billion, for the promotion of investment, trade and project cooperation with the six Turkic-speaking countries.[12] The trade volume with the Turkic states is gradually increasing (see Figure 1).

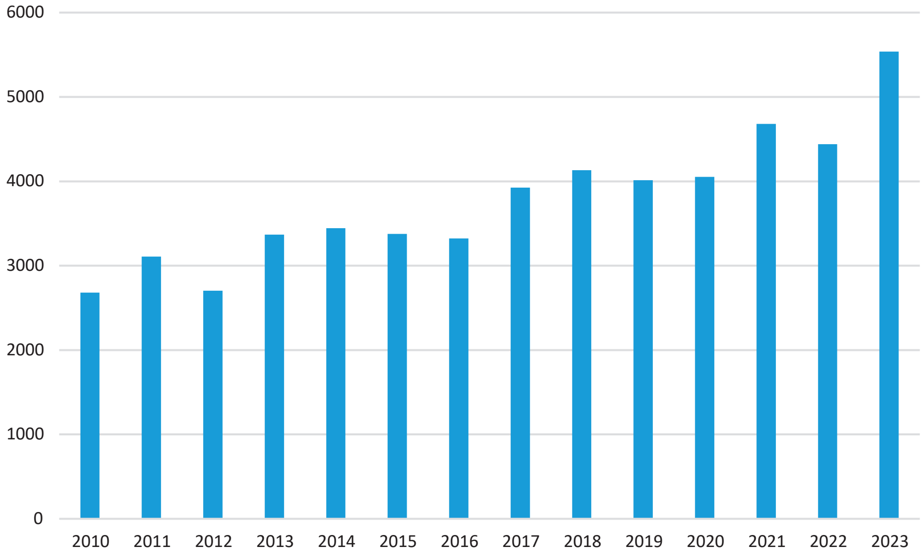

Figure 1: Annual trade turnover between Hungary and the Turkic States (million USD)
Source: KSH 2023

[12] Miniszterelnök 2018.

Hungary after receiving observer status in the OTS has become a part of the cooperation areas of the OTS system. The OTS, which is very strong in the economic cooperation field, has realised a total of 11 ministerial and 13 working group meetings on economic cooperation. Further to that, business forum meetings are held under the umbrella of the OTS, of which one of the six meetings was held in Budapest. Thus, Hungary started to achieve concrete economic benefits since its adaptation to the OTS system.

An essential development regarding the relations between Hungary and the Turkic states is the establishment of the Turkic Investment Fund (TIF). The TIF, which was decided to be founded at the Samarkand Summit of the OTS on 11 November 2022, is expected to bring together the economic strength of the member and observer states to implement joint projects and boost trade opportunities. The TIF mainly aims at supporting the SMEs of the OTS member and observer states in the areas of agriculture, transport and logistics, energy efficiency, renewable and alternative energy, industrial projects in manufacturing, information and communication technologies, tourism, infrastructure projects, public–private partnership projects, human development, creative industries, natural and urban environment schemes. Hungary in addition to other member and observer states pledged to be part of the TIF whereby it will have the opportunity to benefit from joint projects. In this context, on 28 June 2024 Hungary joined the TIF by handing over Hungary's instrument of accession to the Agreement Establishing the Turkic Investment Fund to Deputy Secretary General Sadi Jafarov.[13]

Hungary's cooperation with the Turkic states in the area of transportation

Transportation is another crucial area of cooperation among the OTS countries and Hungary is to play a critical part in this regard. The economic crisis in the early 21st century changed the economic policies of many EU states and Hungary was no exception as it initiated the Eastern Opening. The economic crisis has driven countries to find alternative transportation links and methods between Europe and Asia.[14]

With the Belt and Road Initiative (BRI) originally known as the One Belt, One Road policy, China in 2013 under President Xi Jinping aimed to build a huge infrastructure and broaden trade links between Asia, Africa and Europe. The BRI aims to improve overland connections to China's neighbours and beyond, and to establish a 'maritime sea road' ultimately linking waterways as far as the Indian Ocean, the Gulf and the Red Sea. This ambitious framework was introduced with the commitment of significant funding to accelerate infrastructure construction, financial institutions development, and economic cooperation aimed at building a Silk Road Economic Belt and a Maritime Silk Road.[15]

In this connection, with the BRI of the Chinese Government, which foresees micro land bridges from southeastern European ports via Hungary towards Western Europe,

[13] Organization of Turkic States 2024.

[14] Farkas et al. 2016: 3.

[15] Frankopan 2014: 15.

also shortens the routes easing congested northwestern ports. Hungary has a significant place and potential in this route to become a hub and provide economic and geopolitical benefits.[16]

The current conflict in Ukraine obstructs the trade route between Asia and Europe through Russia namely the northern corridor. In this context, the Trans-Caspian International Transport Route (TTIR), also called the Middle Corridor (MC) is gaining critical importance. The Middle Corridor has the potential to transport up to 10 million tons annually, in up to 200,000 containers.[17] Under the current circumstances, the Middle Corridor is only at the 10% capacity of the northern route. Efforts are ongoing by the Central Asian countries to increase the capacity of the Middle Corridor by investing in the infrastructure.[18] The transportation through the Middle Corridor already increased by 120% from January to March 2022 when compared to the same period in 2021. The leading companies from Denmark, Finland and Germany, such as Maersk, Nurminen Logistics, CEVA Logistics, Azerbaijan's ADY container, and some Chinese rail operators have started to use the Middle Corridor.[19]

One significant development that further adds to the significance of the Middle Corridor is the victory of Azerbaijan over Armenia in 2020. Until the end of this war, the connection between Azerbaijan and the Nakhchivan Autonomous Republic had not been established. With the victory of Azerbaijan, the potential of the Zangezur corridor is revealed which is expected to add to the smooth operation of the Middle Corridor, as this new connection also provides a route between Türkiye and Central Asia.

Hungary, together with the OTS Representation Office in Budapest, hosted the 5th meeting of the Ministers in charge of Transport of the Member and Observer States of the OTS on 14 October 2021 in Budapest. The meeting was hosted by the Minister of Innovation and Technology of Hungary, László Palkovics moderated by Secretary General Baghdad Amreyev, and also attended by the Elder of the OTS from Türkiye Binali Yıldırım. During the meeting, Minister Palkovics informed the parties about the current efforts of the Hungarian Government on transforming the country into a strategic transport hub in Europe, building modern railroad infrastructure and ensuring efficiency and transparency in the transport sector. OTS Elder Binali Yıldırım highlighted the significant economic potential of the Turkic States. Underlining significant steps taken by the member countries to improve the infrastructural capacity and transit potential of the Trans-Caspian East–West–Middle Corridor, Mr. Yıldırım stressed the importance of putting further efforts to decrease logistical costs and accelerate the speed of the transport and customs operations through the corridor.[20]

This time on 25 April 2024 the meeting of the Transport Coordination Committee was held in Budapest under the aegis of the OTS. The member and observer states with the coordination and cooperation of the partners took up the ways to further improve the Middle Corridor and the problems observed in this direction.

[16] Farkas et al. 2016: 3.

[17] Baghirov 2022: 62.

[18] Vasa–Bárkányi 2023: 21.

[19] Eldem 2022: 4.

[20] Topuz 2023: 10.

In a recent interview which was given by Hungarian Foreign Minister Péter Szijjártó to Azerbaijani Trend news agency on November 2023, the Hungarian Foreign Minister mentioned that Hungary is interested in the development of the Middle Corridor. Minister Szijjártó stated that currently China is the second source of imports for the Hungarian economy and that Hungary is the number one country for Chinese investment in Central Europe. According to Minister Szijjártó, Hungary is buying more and more energy resources from the region such as oil from Kazakhstan and natural gas from Azerbaijan. In this regard, Minister Szijjártó mentioned that Hungary is very much interested in the development of the capacity of the routes between Asia and Europe. In this context, Minister Szijjártó mentioned that Hungary is willing to contribute to the development of the capacity of the Middle Corridor either in the transport route, railway, or the transport of electricity or gas.[21]

Hungary's cooperation with the Turkic states in the field of energy

Hungary is largely dependent on Russia for fossil fuels. Under the deal made between Russia and Hungary in 2021 for a period of 15 years, Hungary receives 4.5 billion cubic meters (cbm) of natural gas per year through Bulgaria and Serbia. Hungary's energy dependency is above 50%, and more than 80% of oil and natural gas imports come from Russia. In this context, Hungary is seeking ways to diversify its energy supplies.

After the EU sanctions on Russia, Hungary managed to exempt itself from certain elements of the sanction packages against Russia. In 2022, Prime Minister Orbán blocked further steps towards EU sanctions using Hungary's veto right. The Hungarian Government argues that as a landlocked country, Hungary is very much dependent on energy carrier imports and does not have the alternatives that the other EU countries have.

Currently, the EU countries would like to diversify their energy sources and routes. In this context, Hungary is playing a pivotal role where both natural gas and electricity imports from Azerbaijan will pass through Hungary; then it will also be able to diversify its sources and supply routes. Azerbaijan will also be able to reach Hungary's energy market and diversify its gas exports.

After becoming an observer to the OTS and becoming a part of all cooperation fields in 2018, Hungary started to fully coordinate activities in the energy sector with the OTS countries. The Ministers of Energy of the OTS countries met in 2021, 2022 and 2023. In the Almaty meeting in 2022, Hungary pledged to host the 2023 meeting of the ministers in charge of energy in Budapest. Through the Energy Ministerial Meeting on 30 March 2023 in Budapest, Hungary met all the member countries' energy ministers and has once again put forward its intention to be an energy hub in Europe.[22]

Azerbaijan and Hungary signed a gas deal on 2 June 2023. Hungary's state-owned energy group MVM agreed to purchase 100 million cubic meters of natural gas from

[21] 1tv.ge 2023.
[22] Topuz 2023: 11.

Azerbaijan's state energy firm SOCAR, with the gas planned to be transported by the end of the year. Further to that, the Hungarian oil firm MOL Group became a shareholder in Azerbaijan's Azeri–Chirag–Gunashli (ACG) offshore oil field, buying the shares that previously belonged to the American energy firm Chevron. With this new deal, Hungary made a very critical investment in the region.[23]

On 17 December 2022, Azerbaijan, Georgia, Romania and Hungary signed the "Agreement on Strategic Partnership on Green Energy" that supports effective long-term green energy cooperation. The agreement foresees the import of electricity from Azerbaijan through underwater electric cables under the Black Sea from Georgia to southeastern Europe. The significance of this agreement stems from the fact that it will reduce Hungary's electricity MIC by reducing the use of natural gas for electricity production. As Azerbaijan is the starting spot for this route connecting the Caspian Sea to Europe, Hungary will be a green energy transit hub where it will have the possibility to expand to new countries.[24]

Conclusion

The Hungarian Government started the eastern opening policy with the second Orbán Government in 2010. In the initial phase, Hungary's policy focused on the global outreach, with the Hungarian administration's position that Hungary should expand its relations beyond Europe. While keeping the benefits of the relations with Europe, Hungary wanted to seize the opportunities coming from China, Russia and other important countries of the east mainly in terms of trade.

The eastern opening in addition to the relations with big powers like China and Russia has opened the possibility for Hungary to increase relations with the Turkic countries. In this connection, Hungary started to increase its diplomatic presence in these countries as also the Turkic countries started to open embassies in Hungary. Particularly, Hungary's observer status in the Organization of Turkic States in 2018 and the opening of the Representation Office of the OTS in Hungary thereafter further increased the pace of developing relations.

The rapidly developing relations between Hungary and the Turkic countries are reflected in the fields of trade, transport and energy. In trade, the trade volume between Hungary and Turkic countries almost doubled since the initiation of the eastern opening policy. The advancement of relations thanks to Hungary's observer status in the OTS also contributed to the trade relations. The Business Forum organised by the Representation Office of the OTS in Budapest was a critical event that further boosted the developing trade relations between Hungary and the Turkic countries.

In the field of transport, the Chinese Belt and Road Initiative and the Russia–Ukraine crisis revealed the importance of the Middle Corridor where the Northern route started to lose its old significance. Although the Middle Corridor currently is not at full capacity,

[23] MOL Group 2019.

[24] Euronews 2022.

Hungary shows interest in consolidating the infrastructure for the full operation of the route. In this regard, Hungary has been the host of the OTS Transport Meetings and will continue to do so in the future.

The route from Turkic countries in Central Asia to Europe is also critical in the field of energy. As a country that would like to diversify its energy options, Hungary is taking active steps to its energy alternatives to become a hub in Europe. The OTS provides again opportunities for Hungary to come together with the Turkic states, the recent example of which was in 2023 when Hungary hosted the energy ministerial meeting in Budapest.

Hungary, as part of its eastern opening policy, is continuously developing its relations with the Turkic countries in many fields. The areas of cooperation in trade, transport and energy are critical which would provide Hungary with a unique position in the supply of goods and energy in Europe in the future. Although Hungary's trade with the Turkic countries is very small when compared to trade numbers with China and Russia, Hungary seems to have invested in a critical region with which it would acquire significant advantages.

Hungary's strategic location in Central Europe places it at a crossroads between Western Europe and Eastern Europe, as well as between Northern and Southern Europe. The geostrategic location and the awareness of the political elite through the eastern opening puts Hungary in a key location for trade and energy routes. Hungary can play a critical role by leveraging its strategic location to connect different geopolitical and economic spheres. Hungary's participation in major energy projects like the Southern Gas Corridor and TurkStream pipeline highlights its role as a critical transit country for energy supplies from the East to the West. These projects enhance Hungary's importance in ensuring energy security for Europe.[25]

References

1tv.ge (2023): Hungary Interested in Middle Corridor Development, FM Says. *1tv.ge*, 25 November 2023. Online: https://1tv.ge/lang/en/news/hungary-interested-in-middle-corridor-development-fm-says/

Baghirov, Orkhan (2022): The Organization of Turkic States' Economic Potential and Cooperation Prospects among its Members. *Perceptions: Journal of International Affairs*, 27(1), 53–73.

Bernek, Ágnes (2021): *Geopolitics of Central and Eastern Europe in the 21st Century. From the Buffer Zone to the Gateway Zone.* Frankfurt am Main: Peter Lang. Online: https://doi.org/10.3726/b18155

Egeresi, Zoltán (2020): Hungary's Opening Towards the Turkic World. *Avrasya Dünyası*, 4(6), 48–54.

[25] Bernek 2021: 71.

Eldem, Tuba (2022): Russia's War on Ukraine and the Rise of the Middle Corridor as a Third Vector of Eurasian Connectivity. Connecting Europe and Asia via Central Asia, the Caucasus, and Turkey. *Stiftung Wissenschaft und Politik*, 2022/C 66. Online: https://doi.org/10.18449/2022C64

Euronews (2022): Hungary, Romania, Georgia, and Azerbaijan Agree to the Black Sea Electricity Project. *Euronews*, 17 December 2022. Online: www.euronews.com/2022/12/17/hungary-romania-georgia-azerbaijan-agree-to-black-sea-electricity-projct

Farkas, Andrew Z. – Pap, Norbert – Reményi, Péter (2016): Hungary's Place on Eurasian Rail Land Bridges and the Eastern Opening. *Hungarian Geographical Bulletin*, 65(1), 3–14. Online: https://doi.org/10.15201/hungeobull.65.1.1

Frankopan, Peter (2015): *The Silk Roads. A New History of the World.* London: Bloomsbury.

KSH (2023): *External Trade in Goods in HUF by Countries.* Hungarian Central Statistical Office. Online: www.ksh.hu/stadat_files/kkr/en/kkr0007.html

Ministry of Foreign Affairs of the Republic of Türkiye (2024): *Organization of Turkic States (OTS).* Online: www.mfa.gov.tr/turk-konseyi-en.en.mfa

Miniszterelnök (2018): *Prime Minister Viktor Orbán's Speech at the 6th Summit of the Cooperation Council of Turkic-speaking States.* Online: https://2015-2022.miniszterelnok.hu/prime-minister-viktor-orbans-speech-at-the-6th-summit-of-the-cooperation-council-of-turkic-speaking-states/

MOL Group (2019): Mol Agrees to Purchase a 9.57% Stake in Azerbaijan's ACG Oil Field and 8.9% in the BTC Pipeline. *MOL Group*, 4 November 2019. Online: https://molgroup.info/en/investor-relations/investor-news/mol-agrees-to-purchase-a-957-stake-in-azerbaijans-acg-oil-field-and-89-in-the-btc-pipeline

Nagyné Rózsa, Erzsébet (2016): Magyarország és az arab Közel-Kelet. In Koller, Boglárka – Marsai, Viktor (eds.): *Magyarország Európában, Európa a világban. Tanulmánykötet Gazdag Ferenc 70. születésnapjára.* Budapest: Dialóg Campus, 189–199.

Organization of Turkic States (2022): Baghdad Amreyev Is Appointed as the President of the Turkic Investment Fund by the Leaders of OTS. *OTS*, 12 November 2022. Online: www.turkicstates.org/en/news/baghdad-amreyev-is-appointed-as-the-president-of-the-turkic-investment-fund-by-the-leaders-of-ots

Organization of Turkic States (2024): Hungary Joins the Turkic Investment Fund. *OTS*, 28 June 2024. Online: www.turkicstates.org/en/news/hungary-joins-the-turkic-investment-fund

Roy, Olivier (2005): *The New Central Asia. Geopolitics and the Birth of Nations.* New York: New York University Press.

Stone, Norman (2019): *Hungary. A Short History.* London: Profile Books.

Topuz, Kılıçarslan A. (2023): Hungary and the Organization of Turkic States: Prospects for the Region and Beyond. *Mediterrán és Balkán Fórum*, 17(1–2), 2–14.

Varga, Imre (2000): Development of the Hungarian Foreign Policy in the Last Ten Years: A Comparison of the Foreign Policy Programs of the Post-Transition Hungarian Governments. *National Security and the Future* 2(1), 117–131.

Vasa, László – Bárkányi, Péter (2023): Geopoltical and Geo-Economic Importance of the Middle Corridor: A Comprehensive Overview. *Eurasian Journal of Economic and Business Studies*, 67(2), 20–32. Online: https://doi.org/10.47703/ejebs.v2i67.295

10.32565/aarms.2024.3.3

Partner or Ally? V4 Countries' Bilateral Relations with the United States

Comparative Analysis of Strategic Documents between 2020 and 2023

Péter SELJÁN[1]

After its summit in Prague on 27 February 2024, the Visegrád Group suffered a breakdown of relations, mainly due to the divergent views of its member states regarding Russia's war in Ukraine. The V4 countries split into a pro-Ukraine block (Poland and the Czech Republic) and a Ukraine-sceptic block (Hungary and Slovakia), which made it difficult for the group to present a united front on key issues and diminished its ability to influence broader European policy. In addition, the lack of unity weakens the V4's collective security posture while the Central European region has gained strategic importance as part of NATO's eastern flank. The deterioration of the security environment also impacted the V4 countries' bilateral relations with the United States, as the pro-Ukraine countries intend to maintain close cooperation with Washington, while the sceptics are staunch critics of Western policies supporting Ukraine. This paper highlights the fundamental differences between the latest security strategies and foreign policies of the Visegrád Group countries towards the United States, Russia and China, looking at these countries' latest national security strategies and the 2022 integrated country strategies of the United States Department of State. Our comparative analysis shows that Hungary can be considered an outsider among the V4 countries since the Hungarian Government intends to pursue pragmatic cooperation with Russia and China while U.S.–Hungarian relations are gradually deteriorating. In contrast, the other three member states – especially Poland and the Czech Republic, but also Slovakia regardless of Robert Fico's return to power in 2023 – favoured closer ties with the United States and shared most of the same concerns over Moscow and Beijing.

Keywords: *Visegrád Group, United States, Hungary, Poland, the Czech Republic, Slovakia*

[1] Security and Defence Policy Expert, PhD in International Relations, Corvinus University of Budapest, e-mail: peter@seljan.hu

Introduction

Four Central European nations – Hungary, Poland, the Czech Republic and Slovakia – form the Visegrád Group, sometimes referred to as the Visegrád Four or the V4, which seeks to further the integration with the European Union (EU) while advancing cooperation in military, economic, cultural and energy-related areas. Furthermore, all four states are members of the Bucharest Nine (B9) and the North Atlantic Treaty Organization (NATO). The role and relevance of this subregional cooperation are changing dynamically and are often the subject of debate among experts.[2] Instead of attempting to add to that discourse, this paper aims to highlight the differences among the member states concerning their relationships with the United States and their security strategies driving their foreign policy decisions regarding Russia and China.

The Visegrád Four became politically divided[3] as a result of different responses to Russia's full-scale invasion of Ukraine in 2022, despite some suggesting earlier that "the Visegrád Group's greatest strength lies in its flexibility to become more responsive to the challenges it faces and it is likely therefore to remain appealing to its member states and to be a permanent feature within the wider cohort of European Union subregional partnerships".[4] We have witnessed a significant rupture among the V4 countries when Russia's war in Ukraine drove a wedge between the Hungarian Government and the rest of the group: Slovakia, the Czech Republic, and especially Poland.[5] While many consider the Hungarian Prime Minister, Viktor Orbán to be Russian President Vladimir Putin's closest ally in the EU,[6] the Polish Government is traditionally one of Europe's most hawkish on Russia, and the vast majority of Polish people see the Russian Federation as a major threat.[7] Similarly, while Hungary's relations with the United States hit an all-time low recently,[8] Warsaw can be considered one of the most important allies of Washington in the region, and their relations keep getting stronger.[9]

This rupture of relations within the Visegrád Group is apparent even when listening to statements from the respective governments regarding the war in Ukraine.[10] Its reality becomes even more evident when taking a closer look at the national security strategies of the V4 countries. In the following pages, after providing some historical context, we conduct a comparative analysis of the latest national security strategies of Hungary, Poland, the Czech Republic and Slovakia, published between 2020 and 2023. We focus on how these strategic documents reference the United States, Russia and China and whether they view these great powers as close allies, reliable partners, or security threats. We also examine how these documents describe these defining bilateral relations. To facilitate this comparison, we present our findings in a table.

[2] Basora 2011; Rošteková–Roulet 2014; Daniška 2018; Groszkowski 2018.
[3] Beck 2024.
[4] Törő et al. 2014.
[5] Gosling 2022.
[6] Radio Free Europe – Radio Liberty 2019; Janjevic 2018.
[7] Poushter et al. 2022.
[8] McCausland 2023; Morris 2023; Higgins 2024.
[9] U.S. Department of State 2024a.
[10] Fiala 2022; Bayer 2023; Higgins 2023; Al Jazeera 2024; Pollet 2024; Janicek 2024; Reuters 2024.

Additionally, we draw on the relevant 2022 Integrated Country Strategies (ICS) for each state – published regularly by the United States Department of State to articulate U.S. priorities[11] – to look for similar descriptions of the bilateral relations between the United States and the V4 countries. These descriptions and this comparative analysis allow us to assess the "tightness" of these bilateral relations. Although we are talking about NATO countries that are officially allies, "increasing tightness" makes it more apparent to leaders which states would more likely stand with them in a conflict and which would potentially distance themselves or stand against them.[12] The paper also includes a summary of the overlaps in the content of the examined strategic documents and highlights the striking differences, particularly in Hungary's approach towards the United States, Russia and China, in contrast to the strategies of the other three member states.

Historical context

Before 2010, Hungary's relations with Russia were characterised by a cautious and often unfriendly stance. After the dissolution of the Warsaw Pact and the collapse of the Soviet Union in 1991, Hungary sought to distance itself from Russian influence, focusing on closer ties with the West, joining institutions like NATO and becoming a member of the European Union. The legacy of Soviet oppression and the 1956 Hungarian Revolution continued to cast a shadow over Russian–Hungarian bilateral relations. Political relations were strained despite the existing economic ties, reflecting Hungary's desire to assert its independence and align more closely with the West. In contrast, Sino–Hungarian relations have always been generally positive, although, after 2010, Hungary and China have also significantly strengthened their bilateral relations, primarily through economic cooperation and investment, with Hungary becoming a key partner in China's Belt and Road Initiative. This period has also seen increased diplomatic exchanges and cultural ties, solidifying a close partnership between the two nations.[13]

Traditionally, Poland's relations with Russia have been marked by tension and conflict, particularly due to historical grievances, not just because of recent geopolitical events like the 2014 annexation of Crimea and the 2022 invasion of Ukraine. In contrast, Poland's relationship with China has been more pragmatic, focusing on economic cooperation and trade, especially under the Belt and Road Initiative. However, Warsaw remains cautious of China's growing influence in Europe and traditionally aligns closely with the United States and the European Union on strategic issues.[14]

[11] U.S. Department of State s. a.

[12] Organski and Kugler offer a method for measuring alliance behaviour or the tightness of an alliance. They developed it from a scale built initially based on four categories: defence pact, mutual nonaggression pact, entente and no alliance. Using the tightness and looseness of alliances, they developed a simple eight-point scale that reflects both the degree of commitment and the direction of change in commitment. A positive change means the given state increased its alliance commitments with other nations, while a negative change means the given country decreased its commitments. Moreover, a position on the negative end of the scale means cutting ties (Organski–Kugler 1980: 38–42).

[13] Greilinger 2023; Szandelszky 2024.

[14] Paszak 2021; Bachulska 2021; Pardo 2024.

Relations between the Czech Republic and Russia have been marked by significant tensions, particularly due to events like the Russian annexation of Crimea and the Vrbětice ammunition depot explosion in 2014.[15] These incidents, along with the poisoning of Sergei Skripal in 2018[16] and the Russian invasion of Ukraine, have led to a substantial deterioration in diplomatic ties. The economic relationship between the Czech Republic and China has been more complex and has evolved over time. Initially, during President Miloš Zeman's tenure, there was a push to strengthen ties with expectations for Chinese investments and increased trade. However, these expectations were not fully met, leading to a reassessment of the relationship. Major Czech companies such as Škoda Auto and PPF (Home Credit) have either reduced their presence or completely withdrawn from the Chinese market.[17] The current Czech administration under President Petr Pavel has indicated a shift towards a more cautious approach, focusing on European and transatlantic relations.[18]

Slovakia has historically maintained strong economic ties with Russia, particularly in the energy sector, as Moscow has been a major supplier of natural gas, oil and nuclear fuel to Slovakia. Despite EU sanctions following the 2014 Russian annexation of Crimea, Slovakia has continued to engage with Russia, although it has also taken steps to reduce its energy dependence on Russian supplies.[19] The relationship has been marked by a mix of cooperation and tension, especially in the context of broader EU–Russia relations. Regarding Sino–Slovakian relations, over the past decades, Slovakia and China have developed a relationship primarily centred on economic cooperation, with Slovakia becoming a significant exporter of automobiles to China.[20] However, this relationship has faced challenges, including trade imbalances and political tensions related to broader EU–China relations.[21] In contrast, Slovakia and the United States have strong diplomatic ties, cooperating closely in military and law enforcement areas since establishing relations in 1993. In 2022, right before the Russian invasion of Ukraine, Slovakia's parliament and president approved a Defense Cooperation Agreement[22] with the United States that allows the U.S. military to use two Slovak air force bases for ten years.[23] The treaty was supported by the government of then Prime Minister Eduard Heger, while it was fiercely opposed by the opposition, including Robert Fico's Smer party, which led the government in 2018 when talks with the U.S. began. Critics claimed the defence agreement compromised the country's sovereignty, making possible a permanent presence of U.S. troops on Slovak territory and even enabling a possible deployment of nuclear weapons in Slovakia.[24]

[15] Janicek 2021.

[16] Castle 2018; Corera 2021.

[17] Zemánek 2023.

[18] Kowalski 2023.

[19] Euractiv 2014; Ceenergy News 2023.

[20] OEC 2022a.

[21] Sebena 2024.

[22] Agreement on Defense Cooperation Between the Government of the United States of America and the Government of the Slovak Republic 2022.

[23] Zachar 2022.

[24] Hrabovska Francelova 2022.

Diverging security interests?

Hungary

Hungary's 2020 National Security Strategy references the United States in the 112th paragraph under the section describing the country's fundamental interests. The document emphasises the importance of the alliance between Europe and the United States based on shared values, interests and civilisational ties. The document recognises that maintaining a strategic relationship with the United States, including high-level defence and economic cooperation, is fundamental to Hungary's interests. Additionally, the strategy acknowledges the United States as a crucial player in international security policy in the future.[25]

Russia is referenced as an important player in global and regional security matters in paragraph 118. Hungary's National Security Strategy recognises recent "major tensions" between NATO and Russia and between the EU and Russia.[26] However, it does not consider the Russian Federation a threat to international security.[27] Instead, it highlights that NATO maintains open channels of political dialogue, although the Alliance has strengthened its deterrence and defence capabilities and suspended cooperation with Moscow. The Hungarian Government firmly believes that political dialogue with the Kremlin and measures that reduce risk and build trust are necessary, especially considering the deteriorating strategic environment. Hungary prioritises maintaining the cohesion of NATO and the EU while supporting the pragmatic development of Hungarian–Russian relations and economic cooperation.[28]

In the following paragraph, Hungary's National Security Strategy mentions China as the world's second-largest economy, noting that Beijing is becoming more assertive politically and militarily, suggesting that its military and security policies need long-term monitoring. As the document states, Hungary seeks to strengthen its relations with China, which the Hungarian Government considers pragmatic. The document highlights the importance of the "Modern Silk Road" program (the Belt and Road Initiative), which aims to enhance trade relations and connect Europe, Africa and Asia, which the Hungarian Government considers mutually advantageous. However, Hungary's National Security Strategy also mentions the potential vulnerabilities arising from China's investments in critical infrastructure, its role as a supplier of advanced infocommunications technology, and its growing regional influence.[29]

[25] Government Resolution 1163/2020 (IV. 21.) on Hungary's National Security Strategy, paragraph 112.

[26] The Government Resolution 1163/2020 on Hungary's National Security Strategy was adopted on 21 April 2020, and published on 21 June 2021, less than a year before the Russian invasion of Ukraine, which started on 24 February 2022, but six years after the Russian Federation annexed Crimea in March 2014.

[27] While Hungary's National Security Strategy does not consider Russia a threat, NATO's 2022 Strategic Concept identifies Russia as "the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area" that "seeks to establish spheres of influence and direct control through coercion, subversion, aggression and annexation" (NATO 2022 Strategic Concept 2022: 4).

[28] Hungary's National Security Strategy 2020, paragraph 118.

[29] Hungary's National Security Strategy 2020, paragraph 119.

Poland

According to the 2020 National Security Strategy of the Republic of Poland, the most important factor shaping Poland's security is its embedding in the transatlantic and European structures and developing bilateral and regional cooperation with key allies. In addition, the strategic document mentions that the transatlantic relationship has been tested in recent years and that the strategic bonds between the United States and its European allies are evolving. Poland strives to strengthen its security through its NATO and EU membership, "strategic partnership" with the U.S., and regional cooperation. Poland's security has been bolstered by assistance from the U.S. in security and defence, energy, trade, investment, and research and development. In addition, the enduring presence of the U.S. Armed Forces in Poland is an integral part of the bilateral partnership.[30]

Poland's security strategy states that "the most serious threat is the neo-imperial policy of the authorities of the Russian Federation, pursued also by means of military force". The strategic document also highlights that Russia is intensively developing its offensive capabilities while it carries out hybrid nature activities, and its actions aim to destabilise the Western states and societies and to create divisions among Allies. The Polish strategic document adds that it should be assumed that Russia will continue undermining the international order to rebuild its power and spheres of influence. It is worth highlighting that the Polish strategy also mentions that within the European Union, divergent approaches concerning its further development are emerging and that there is also a noticeable risk of undermining the coherence of the positions of NATO and EU member states as a result of increasing internal tensions and actions undertaken by external entities, which can be considered a reference to Russia's growing influence in the region.[31]

In addition, Poland's National Security Strategy also mentions the growing strategic rivalry between the United States, China and Russia, and interestingly, this context of increasing geopolitical competition among the great powers is the only time China is mentioned in the document, noting that this rivalry affects the entire international system.[32]

The Czech Republic

The 2023 National Security Strategy of the Czech Republic mentions developing bilateral relations with the United States only briefly among the "other important interests" that serve the country's "vital and strategic interests" and improve the society's resilience to security threats.[33]

[30] National Security Strategy of the Republic of Poland 2020: 6; Ministry of National Defence, Republic of Poland 2024.

[31] National Security Strategy of the Republic of Poland 2020: 6–7.

[32] National Security Strategy of the Republic of Poland 2020: 7.

[33] Security Strategy of the Czech Republic 2023: 6.

Concerning Russia, the document states in the key messages that Russia's war against Ukraine has put an end to the period of peace, stability and cooperation in Europe and that Moscow acts deliberately against the Czech Republic's political, economic and social stability. In addition, the document identifies Russia as a "fundamental threat" to the security of the Czech Republic. Under the section describing security threats and sources of instability, the Czech strategy states: "Russia is the biggest immediate and longstanding direct threat to the security of Europe and the international rules-based order." Like Poland's strategy, the Czech document includes that Russia seeks to retain and expand its sphere of influence in Europe, even by using force, and it seeks to destabilise its neighbourhood and other regions. The Czech security strategy also mentions that Russia uses hybrid operations targeting the Czech Republic's interests and security.[34]

Regarding China, the Czech strategic document states that Beijing poses a "fundamental systemic challenge" globally and in terms of conducting direct influence operations in democratic countries, including the Czech Republic. It challenges the international order, which has adverse implications for Euro-Atlantic security. The Czech Republic's National Security Strategy highlights that China is increasing its military capabilities, including its nuclear forces. It also engages in cyber espionage and aims to control global data flows. Additionally, it uses various forms of economic coercion and hybrid interference tools. Chinese companies are closely associated with the state and are willing to work towards its goals. The Czech National Security Strategy also notes that Russia and China share the same interest in weakening the influence and unity of democratic countries.[35]

Slovakia

The 2021 Security Strategy of the Slovak Republic also includes a section on the country's strategic security interests, where it first mentions the United States. According to the strategy, maintaining NATO's credible deterrence and collective defence – along with the transatlantic strategic partnership and the United States military presence in Europe – is crucial for Slovakia.[36] The United States is mentioned again later under the section detailing the security policy of Slovakia, according to which the U.S. is a "strategic transatlantic ally" of the Slovak Republic in NATO, with which Slovakia shares common values and is bound by a strong historical alliance and commitment to collective defence. Here, the strategy underscores again that it is in Slovakia's security interest to maintain the military presence of the United States in Europe, which contributes to the stability and security of the region and is the key deterrent and guarantee of effective defence against a possible armed attack on European NATO members.[37]

[34] Security Strategy of the Czech Republic 2023: 15.

[35] Security Strategy of the Czech Republic 2023: 14–15.

[36] Security Strategy of the Slovak Republic 2021: 6.

[37] Security Strategy of the Slovak Republic 2021: 22.

Table 1: The main findings of the national security strategies of the V4 countries regarding the United States, Russia and China

	Hungary (2020)	Poland (2020)	The Czech Republic (2023)	Slovakia (2021)
USA	Maintaining the strategic relationship and the high-level defence and economic cooperation with the U.S. is in Hungary's fundamental interest, as the U.S. will remain a decisive player in international security policy in the future.	Poland's security is also shored up through the development of strategic cooperation with the USA in the fields of security and defence (including in the form of enduring the presence of the U.S. armed forces in Poland), technology, trade and energy.	Developing bilateral relations with the United States serves the country's vital and strategic interests.	The USA is a strategic transatlantic ally of the Slovak Republic in NATO. Our security interest is to maintain the military presence of the USA in Europe.
Russia	One of the key actors in the international system, managing several global and regional security issues. Hungary has an interest in the pragmatic development of Hungarian–Russian relations and economic cooperation.	The most serious threat is the neo-imperial policy of the authorities of the Russian Federation, pursued also by means of military force.	Russia poses a fundamental threat to the security of the Czech Republic, and it is the biggest immediate and long-standing direct threat to the security of Europe and to the international rules-based order.	Slovakia is interested in developing good mutual relations with Russia. Moscow is an important actor and partner in addressing international threats and challenges. At the same time, with its confrontational approach in the military, security and political areas, represents a key security challenge.
China	Has the second-largest economy, a centre of civilisation, and it is playing an increasingly important role in the international system. Hungary is interested in the pragmatic strengthening of Sino–Hungarian relations. The Belt and Road Initiative is mutually advantageous.	Poland's National Security Strategy mentions the growing strategic rivalry between the United States, China and Russia. This is the only time China is mentioned in the strategic document.	China poses a fundamental systemic challenge globally and in terms of direct influence operations. It calls into question the international order, which has adverse implications for Euro-Atlantic security. Russia and China share the same interest – weakening the influence and unity of democratic countries.	China is an important actor and partner in addressing global challenges, but also an economic and technological competitor and systemic rival of the EU.

Source: Hungary's National Security Strategy 2020; National Security Strategy of the Republic of Poland 2020; Security Strategy of the Czech Republic 2023; Security Strategy of the Slovak Republic 2021

Slovakia's security strategy mentions Russia twice. The first mention is made under the section that assesses the security environment of Slovakia and its neighbouring regions. This section highlights that the Russian Federation's aggressive behaviour led to the conflicts in Georgia and eastern Ukraine and the illegal occupation of Ukrainian Crimea and Sevastopol. These actions are considered a gross violation of international law. The second mention of Russia is made under the security policy section, where the document states that Slovakia aims to foster good relations with Russia since it is an important actor and partner in addressing international threats and challenges. However, the document notes that Moscow's confrontational approach in the military, security and political domains is a key challenge to Euro-Atlantic security. The document emphasises that Slovakia cannot ignore Russia's violations of international law, interference in the democratic processes of other states, and efforts to weaken the European security architecture, including the unity of NATO and the EU. Therefore, Slovakia's policy towards Russia will continue to be based on seeking shared interests while also engaging in open critical dialogue on issues where values and interests diverge. The security strategy also mentions that Slovakia will support the application of restrictive measures against the Russian Federation if necessary.[38]

In Slovakia's national security strategy, China is an important actor and partner in addressing global challenges, an economic and technological competitor, and a "systemic rival" of the European Union. As the document says, China is rapidly increasing its military capabilities and using its economic strength and strategic investments assertively to advance its interests. Beijing promotes its own model of governance and a different understanding of human rights and freedoms. Slovakia takes these factors into account in its mutual relations with China and its positions within international organisations.[39]

Many overlaps with a few striking differences

The national security strategies of Hungary, Poland, the Czech Republic and Slovakia all emphasise the importance of their alliances with the United States and the European Union. Also, they all recognise Russia and China as significant players in global and regional security matters. In addition, to a certain extent, all four countries' security strategies take note of the growing strategic rivalry between Washington, Beijing and Moscow, and seek to strengthen their security through NATO and EU membership, strategic partnerships and regional cooperation. However, compared to Hungary, their national security strategies reveal some striking differences in their approaches, particularly in their perceptions

[38] Security Strategy of the Slovak Republic 2021: 24–25.

[39] Security Strategy of the Slovak Republic 2021: 25.

of Russia as a threat, their attitudes toward China[40] and their priorities in international relations, summarised in Table 1.

Poland and the Czech Republic see Russia as a serious or fundamental security threat, Slovakia takes a more balanced approach, and Hungary takes an especially conciliatory approach towards Moscow. Based on their national security strategies, Poland and the Czech Republic are the closest allies of the United States among the V4 countries, as both consider the U.S. their strategic ally, Russia a threat and China a strategic rival and a systemic challenge. Slovakia is taking the middle ground, considering Washington a strategic ally and China an important actor and partner, but also developing good relations with the Russian Federation while acknowledging that Moscow represents a key security challenge. Hungary alone occupies the other end of the spectrum as it seems closer to the Kremlin and the Chinese Communist Party (CCP) than the other three countries, seeking "pragmatic cooperation" and better relations with Moscow and Beijing.[41]

Partner or staunch ally

The United States Department of State publishes four-year Integrated Country Strategies (ICS), articulating the U.S. priorities in each country. The Chief of Mission leads this ICS to develop a common set of goals and objectives through a coordinated and collaborative planning effort among the State Department and other government agencies with programming in the country. Higher-level planning documents and strategies inform the ICS, like the U.S. National Security Strategy.[42] The following pages examine the ICS for Hungary, Poland, the Czech Republic and Slovakia. At the end of this section, we provide a brief summary and present the main findings in Table 2.

[40] Regardless of the security strategies of the individual states, China maintains a robust trade relationship with the V4 countries, which favours Beijing. China exported a significant amount of goods to these countries, including electronics, machinery and various manufactured products. For instance, Hungary imported $10.5 billion of goods from China while exporting $2.89 billion, primarily in navigation equipment and cars. Poland's imports from China reached $43.9 billion in 2022, with the main imports being refined copper and gas turbines. In 2023, despite claiming to be wary of Beijing, the Czech Republic also imported $40.3 billion worth of goods from China (similarly to Poland), while Slovakia's Chinese imports also exceeded $8.5 billion. For more see OEC 2022a, 2022b, 2022c; Trading Economics 2023a, 2023b.

[41] It is worth noting that in NATO's Washington Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 10 July 2024 – including the Hungarian Prime Minister, Viktor Orbán – the Alliance agreed that "Russia remains the most significant and direct threat to Allies' security". Moreover, they added that "the People's Republic of China's (PRC) stated ambitions and coercive policies continue to challenge our interests, security and values". Furthermore, the declaration states that "the deepening strategic partnership between Russia and the PRC and their mutually reinforcing attempts to undercut and reshape the rules-based international order are a cause for profound concern". In addition, the document notes that "the PRC has become a decisive enabler of Russia's war against Ukraine through its so-called 'no limits' partnership and its large-scale support for Russia's defence industrial base" which "increases the threat Russia poses to its neighbours and to Euro-Atlantic security" and states that "the PRC continues to pose systemic challenges" (NATO 2024a).

[42] U.S. Department of State s. a.

Hungary as a partner

The United States and Hungary first established diplomatic relations in 1921, following the dissolution of the Austro–Hungarian Monarchy after World War I.[43] Later, during World War II, Hungary severed ties to the U.S. and allied with Nazi Germany in 1941. Bilateral relations were re-established only after the end of the war in 1945, while Soviet forces occupied the country and set up a communist regime that lasted for over four decades, despite an uprising in 1956 that the Soviet Union violently crushed. In 1989, after the collapse of communism, the United States supported Hungary in transitioning to a democratic political system and a free market economy. Hungary joined NATO in 1999, the EU in 2004, and the U.S. Visa Waiver Program[44] in 2008. In 2019, the United States and Hungary signed a Defense Cooperation Agreement[45] to modernise military cooperation between the two countries. Today, the United States and Hungary cooperate on a wide range of transatlantic and other issues. After Hungary joined the EU in 2004, the United States discontinued bilateral development support. However, Washington still provides security assistance to Hungary through Foreign Military Financing (FMF),[46] International Military Education and Training (IMET)[47] and other capacity-building funds, such as the Peacekeeping Operations (PKO)-funded Global Defense Reform Program,[48] which advises the Hungarian Defence Forces on joint and operational planning. This security aid supports regional stability, assists Hungary in coalition operations, and fosters the continuous development of a flexible, sustainable and interoperable Hungarian military capable of satisfying NATO commitments. In addition, the United States is among

[43] Treaty Establishing Friendly Relations Between the United States and Hungary 1922.

[44] The United States imposed restrictions for Hungarian passport holders under its Visa Waiver Program on 1 August 2023, saying Budapest has not addressed security vulnerabilities repeatedly raised by Washington. According to the U.S., Hungary granted citizenship to about one million people between 2011 and 2020 – mostly ethnic Hungarians living in neighbouring states – "without adequate security measures in place to verify their identities". The validity period offered to Hungarians under the Electronic System for Travel Authorization (ESTA) was immediately reduced from two years to one year. Now, only single visits are allowed under the system, not multiple. These unprecedented modifications did not apply to any of the other 39 participants in the Visa Waiver Program (Than 2023).

[45] Agreement on Defense Cooperation Between the Government of the United States of America and the Government of Hungary 2019.

[46] The Arms Export Control Act (AECA), as amended [22 U.S.C. 2751, et. seq.], authorises the President to finance procurement of defence articles and services for foreign countries and international organisations. The FMF enables eligible partner nations to purchase U.S. defence articles, services and training through either FMS or, for a limited number of countries, through the foreign military financing of direct commercial contracts (FMF/DCC) program (U.S. Department of Defense 2024a).

[47] Among the goals of IMET are to train future leaders, create a better understanding of the United States, establish rapport between the U.S. military and the country's military to build alliances for the future, and enhance interoperability and capabilities for joint operations (U.S. Department of Defense 2024b).

[48] The Global Defense Reform Program (GDRP) is a flexible PKO-funded program that seeks to improve security sector governance and institutional capacity of select U.S. partners at the service, ministerial and national levels (U.S. Department of State 2024b).

the leading foreign investors, and U.S. investment supports more than 100,000 jobs in Hungary,[49] which has had a direct, positive impact on the Hungarian economy.[50]

As per the Chief of Mission Priorities articulated in the 14-page U.S. Integrated Country Strategy for Hungary, the United States faces many diverse global challenges to defend and renew the foundations of security, prosperity and democracy, and Americans and Europeans have the chance to restore our well-being and shape the economy of tomorrow, seizing the opportunity to show that "democracies can deliver". According to the United States, Hungary can be a partner in these efforts as a NATO Ally, EU member, and trade and investment partner. Russia's aggressive behaviour in the region made taking advantage of all the possibilities even more important. As the document puts it, the United States and Hungary have a long-standing relationship with important shared security and economic interests. Hungary has made valuable contributions by joining NATO Allies in missions abroad and modernising its military. The United States aims to revitalise the NATO Alliance and seeks Hungary's full support to strengthen the transatlantic partnership. The mission is to work with Hungary to make it a more capable NATO ally, actively participating in NATO and bilateral deterrence activities and military exercises.[51]

The U.S. Integrated Country Strategy emphasises the economic opportunities in the American–Hungarian partnership. It suggests that we can work to strengthen our economic and technological cooperation, which can lead to significant growth and diversification. These opportunities are important for shaping both countries' economies in line with U.S. interests and values. Additionally, they provide a chance to diversify away from energy markets influenced by autocratic regimes and to protect our critical infrastructure from technologies that might compromise security. As a reference to China and Russia, the document notes that working together in this manner can help insulate Hungary and the transatlantic community from the efforts of geopolitical powers that seek to undermine the international rules-based order.[52]

The document underscores that democratic values lie at the foundation of U.S. foreign policy. Bolstering human rights and democratic values is not just a priority, but an essential element to the long-term health of the alliance and bilateral relationship between the United States and Hungary. The rule of law, democratic backsliding and corruption are priority areas for the United States in Hungary. Several U.S. administrations in the United States have viewed the erosion of certain aspects of the rule of law in Hungary with concern. The United States is working with European partners, multilateral organisations and Hungarians to foster free and fair elections, and the U.S. mission is ready to cooperate

[49] It is worth mentioning that the U.S. Department of the Treasury terminated a 1979 tax treaty with Hungary to pressure Hungarian Prime Minister Viktor Orbán to agree to implement the 15% global minimum tax agreed by nearly 140 countries. The United States notified Hungary on 8 July 2022, of its termination of the Convention between the Government of the United States of America and the Government of the Hungarian People's Republic for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income. The termination itself has become effective on 8 January 2023, and the Convention has ceased to have effect on 1 January 2024 (Reuters 2022; U.S. Department of the Treasury 2022).

[50] U.S. Department of State 2021a.

[51] Integrated Country Strategy: Hungary 2022: 1–2.

[52] Integrated Country Strategy: Hungary 2022: 2.

with Hungarian officials at any level to combat corruption. The United States encourages Hungary to cooperate in efforts to strengthen democracy and the rule of law globally.[53]

Describing the U.S. Mission Goals and Objectives, the ICS notes that as a NATO Ally, Hungary should give full political support to NATO's engagement with its Alliance partner Ukraine and other NATO deterrence efforts and highlights the fact that a failure to secure Hungary's full support for NATO will perpetuate Hungary's block on high-level NATO engagement with Ukraine and that Hungary could also block other NATO responses to emerging challenges.[54] As another risk, the ICS mentions that Hungary could also veto EU and NATO cooperation with the United States in certain areas (like efforts to compete with revisionist powers). As the document puts it, failure to coordinate with European Allies, including Hungary, in the Western Balkans could threaten regional stability and enhance the influence of non-democratic outside actors.[55]

Poland as a loyal ally

Poland is a "stalwart ally" of the United States and one of its strongest partners in Central Europe in fostering security and prosperity regionally, throughout Europe and the world. The United States and Poland cooperate closely on NATO capabilities, counterterrorism, non-proliferation, missile defence, human rights, economic growth and innovation, energy security, and regional cooperation in Central and Eastern Europe. Poland plays a crucial role in NATO operations, hosting various NATO headquarters and units, meeting defence spending commitments and contributing to operations abroad. The country also hosts thousands of U.S. military personnel,[56] facilitates military exercises, and enables a more significant rotational U.S. presence under the 2020 U.S.–Poland Enhanced Defense Cooperation Agreement (EDCA).[57]

In contrast to the reference to Hungary as a partner, the Chief of Mission Priorities in the 35-page U.S. Integrated Country Strategy for Poland refers to Poland as a "staunch U.S. Ally" and a "strategic partner" on NATO's eastern flank. As the ICS for Poland puts it, the United States' relations with Poland are "surging across the board", driven by a profound strategic commonality that links national interests with universal values, including democracy and the rule of law. According to the document, the bilateral affection is further deepened by their history, close cultural affinities and strong economic ties, laying the groundwork for an ambitious blueprint to strengthen the American–Polish

[53] Integrated Country Strategy: Hungary 2022: 2.

[54] NATO Secretary General Jens Stoltenberg met with Hungarian Prime Minister Viktor Orbán in Budapest on 12 June 2024, to discuss preparations for the Washington Summit. Following Stoltenberg's visit, Hungary agreed not to veto NATO support for Ukraine. However, Prime Minister Viktor Orbán insisted that his government would not provide funds or military personnel for any joint assistance effort (Cook 2024).

[55] Integrated Country Strategy: Hungary 2022: 6–7.

[56] According to the Department of State, in total, Poland hosted approximately 4,500 rotational U.S. military personnel on any given day in 2021 (U.S. Department of State 2021b).

[57] The EDCA enables a more prominent rotational U.S. presence in Poland and lays out Warsaw's burden-sharing support to U.S. forces. For more, see the Agreement Between the Government of the United States of America and the Government of the Republic of Poland on Enhanced Defense Cooperation 2020.

partnership through joint, practical action. The country strategy emphasises that by focusing on what is possible, the United States and Poland could increase their bilateral trade volumes to the highest levels in their history. Their top scientists, engineers and entrepreneurs could collaborate to address climate change and combat infectious diseases. Working together, they can shorten the transition from Poland's reliance on coal to greener energy sources, thereby reducing their carbon footprint. Strengthening security ties can lead to a more robust Poland contributing to collective security. In addition, the United States supports Poland's goal of becoming a top-tier NATO Ally and the primary regional leader in collective defence.[58]

Regarding the security cooperation, as the ICS mentions, the U.S.–Poland shared commitment to freedom dates back to the American Revolution when Polish heroes such as Tadeusz Kosciuszko and Casimir Pulaski aided the American cause. The United States was the first country to recognise independent Poland in 1919. Today, Poland remains a stalwart Ally and one of the United States' strongest partners in fostering security regionally and globally. The United States and Poland partner closely on NATO capabilities, counterterrorism, non-proliferation, missile defence, border security, transnational crime and combatting cyber threats. Poland is in the middle of a multi-year (2020–2035), $133 billion military modernisation program and was one of only a handful of Allies meeting NATO guidelines to spend 2% of GDP on defence and 20 of defence spending on modernising equipment and infrastructure in 2022. Poland jointly hosts the NATO Multinational Corps and Division Northeast Headquarters and the forward command post of the U.S. Army's newly established V Corps headquarters. A U.S. aviation detachment is located in Poland, and the country is hosting a ballistic missile defence site under the European Phased Adaptive Approach.[59] In July 2024, after years of development, the Aegis Ashore missile defence site in northern Poland (Redzikowo) finally reached operational status.[60] Poland's cyber capacity is growing and will help improve the Polish Government's nascent preparedness for potential domestic and transient attacks. The country strategy notes that the United States and Poland are addressing traditional and emerging threats to provide regional, European and global security.[61]

Describing the U.S. Mission Goals and Objectives in Poland, the respective ICS notes that a failure to continue setting conditions for enhanced U.S. military presence and supporting Poland's military modernisation program would reduce bilateral military cooperation and slow Poland's military modernisation efforts. This failure would weaken NATO's ability to deter and, if necessary, resist aggression on the Alliance's eastern flank. Among other objectives, the United States would like to improve Poland's ability to address cyber threats, and a failure to continue cooperation with Poland in cybersecurity would mean greater exposure to cyber threats from malign actors.[62] Another risk the document identifies concerns improving Poland's energy security, which is necessary if the country

[58] Integrated Country Strategy: Poland 2022: 1.

[59] Judson 2024; Naval Sea Systems Command 2024.

[60] NATO 2024b.

[61] Integrated Country Strategy: Poland 2022: 1–2.

[62] Integrated Country Strategy: Poland 2022: 13.

does not want to remain vulnerable to pressure from outside influences. As the country strategy notes, should malign actors seek to restrict Poland's access to energy supplies, it could cause political and social instability and have serious economic consequences.[63]

The Czech Republic, a steadfast ally

According to the 21-page Integrated Country Strategy for the Czech Republic, the United States considers Prague a "steadfast ally" and a "like-minded partner". In the Chief of Mission Priorities, the document says that the Czechs are among the most enthusiastic partners of the United States in standing firm against authoritarianism and advocating democracy. The document notes that the Czech Republic's outspoken and passionate support for Ukrainian sovereignty makes this more evident than anywhere else. The United States supports the Czech Government's efforts to meet its NATO budget and capability targets. Both countries are collaborating to address global challenges by combatting misinformation, strengthening cyber defences, and enhancing security and stability worldwide. Additionally, efforts are being made to identify opportunities for U.S. defence firms to promote interoperability and commercial prospects for U.S. exporters through engagement with Czech officials.[64]

The Czech Republic and the United States aim to strengthen their technology, research and innovation partnership. They are working on establishing smart regulations for the digital economy to maintain oversight of global technology networks and promote access to U.S. products and services. Additionally, they are focusing on promoting trade and investment, especially in technology, defence, agriculture and tourism, to create and preserve jobs in both countries. As the Czech Republic is transitioning from coal, it needs to build new nuclear power generation facilities and tap new renewable energy sources. Prague is coordinating closely with the United States to address its energy needs using U.S. commercial technology. To assist the Czech Republic in addressing the growing efforts of authoritarian regimes to destabilise the country and its institutions through propaganda, disinformation, economic coercion and other harmful activities, the United States is collaborating with the Czech Government, media and civil society partners to identify, counter and protect the Czech society against these threats.[65]

In the section describing the Mission Goals and Objectives, the ICS mentions the risk of the Czech Republic not reaching the NATO budget and capability commitments, which is essential to help the Alliance sustain its deterrence and defence posture against global threats. Another U.S. objective focuses on Czechs advocating for policies within the European Union and other multilateral organisations that strengthen the transatlantic relationship and combat global challenges. As the document highlights, without the European Union as a strong and like-minded partner of the United States to tackle global challenges, the U.S. risks being unable to address critical issues such as Russian aggression

[63] Integrated Country Strategy: Poland 2022: 19.

[64] Integrated Country Strategy: Czech Republic 2022: 1–2.

[65] Integrated Country Strategy: Czech Republic 2022: 2.

and China's malign influence. Moscow and Beijing may seek to drive wedges in EU and NATO unity and promote their authoritarian worldview in multilateral bodies, which would harm U.S. interests. In addition, the United States supports the Czech Government in improving its ability to identify and combat disinformation and build resilience against malign information operations.[66]

Slovakia as an important ally

The 18-page U.S. Integrated Country Strategy for Slovakia refers to the Slovak Republic as an "important NATO ally" and an EU member state. Among the Chief of Mission Priorities, the document notes that in recent years, Slovakia has faced quickly changing geopolitical, economic and security landscapes as Central Europe has become a highly contested space increasingly under external pressure. Disinformation campaigns, influence operations, conventional and hybrid threats, and emerging disruptive technologies build on weaknesses in Slovakia's education system and a general lack of opportunities, threatening U.S. and European security in Europe and beyond. In addition, Russian efforts to undermine democratic institutions risk turning back the possibilities of Slovakia enacting much-needed anti-corruption reforms. Democratic backsliding has taken a toll regionally in general. As the ICS highlights, in this context, Slovakia's dedication to democratic ideals and its transatlantic identity is critically important in its neighbourhood and the EU, NATO and beyond.[67]

The document also stresses that Slovakia's role as a significant democratic model is at risk because a considerable portion of the population relies on disinformation sources and online conspiracy theories as their primary source of information. The ICS describes Slovakia as being at a crucial point regarding its geopolitical positioning. Its increasing desire to play a key role in the transatlantic community is being tested by a rising threat from the eastern direction, which could disrupt Europe and weaken the "values we all hold dear". Therefore, the primary goal of the U.S. Mission in Slovakia, is to expand bilateral and multilateral cooperation to bolster regional and global security and stability and address hybrid threats, so Slovakia can become a more active and capable partner in confronting the challenges the West is facing. The secondary goal of the U.S. – to strengthen Slovakia's resilience and responsiveness to its democratic institutions – is to keep Slovakia a stable partner and bulwark against the regional erosion of democratic ideals. According to the ICS, the United States intends to engage the Slovak public to build support for shared values and endeavour to reinforce Slovakia's commitment to the West and the common transatlantic identity. In this regard, the document notes that significant segments of Slovak society do not identify their country as fully anchored in the West, increasing Slovakia's vulnerability to the Russian Government's efforts to erode support for Slovakia's Western orientation and democratic institutions.[68]

[66] Integrated Country Strategy: Czech Republic 2022: 7–8.

[67] Integrated Country Strategy: Slovak Republic 2022: 1.

[68] Integrated Country Strategy: Slovak Republic 2022: 3.

Table 2: The main findings of the United States Department of State's integrated country strategies for Hungary, Poland, the Czech Republic and Slovakia

Hungary	Hungary can be a *partner* in U.S. efforts to defend and renew the foundations of democracy and security as a NATO Ally, EU member, and trade and investment partner. Russia's aggressive behaviour in the region made taking advantage of all the possibilities even more important. The rule of law, democratic backsliding and corruption are priority areas for the United States. The erosion of certain aspects of the rule of law in Hungary is a major concern.
Poland	The United States sees Poland as a *staunch ally* and a *strategic partner* on NATO's eastern flank. Polish–American relations are "surging across the board", driven by a profound strategic commonality that links national interests with universal values, including democracy and the rule of law. The bilateral affection is further deepened by their history, close cultural affinities and strong economic ties. The United States and Poland partner closely on NATO capabilities, counterterrorism, non-proliferation, missile defence, border security, transnational crime and combatting cyber threats.
Czech Republic	Prague is a *steadfast ally* and a *like-minded partner* of the United States. The Czechs are among the most enthusiastic partners of the U.S. in standing firm against authoritarianism and advocating democracy. The two countries are collaborating to address global challenges by combatting misinformation, strengthening cyber defence, and enhancing security and stability worldwide.
Slovakia	The Slovak Republic is an *important NATO ally* and an EU member state in the eyes of the United States. Slovakia has faced quickly changing geopolitical, economic and security landscapes as Central Europe has become a highly contested space increasingly under external pressure. Russian efforts to undermine democratic institutions risk turning back the possibilities of Slovakia enacting much-needed anti-corruption reforms. Democratic backsliding has taken a toll regionally in general. Slovakia's dedication to democratic ideals and its transatlantic identity is critical. Slovakia is at a crucial point in terms of its geopolitical positioning. Therefore, expanding bilateral and multilateral cooperation to strengthen regional and global security and stability and confront hybrid threats is a priority for the United States.

Source: Integrated Country Strategy: Hungary 2022; Integrated Country Strategy: Poland 2022; Integrated Country Strategy: Czech Republic 2022; Integrated Country Strategy: Slovak Republic 2022

Describing the U.S. Mission Goals and Objectives in Slovakia, the respective ICS identifies expanding bilateral and multilateral cooperation to strengthen regional and global security and stability and confront hybrid threats as the primary mission goal. In this regard, the document notes that nationalism, far-right extremism and Russian disinformation campaigns undermine public support for Slovakia's Western orientation and its membership in the EU, NATO and other transatlantic institutions. Another risk the ICS mentions is the failure to uphold and advocate for key transatlantic values in regional organisations and in domestic actions, which – as the ICS puts it – would damage Slovakia's international standing. The country strategy goes further and says that in this case, Slovakia "would be grouped with other backsliding V4 members and viewed as a block on EU progress in key democratization and rule of law issues", which is most probably a reference to Hungary and Poland before Donald Tusk's return as Polish Prime Minister at the end of 2023. Regarding Slovakia's vulnerability to hybrid threats – including disinformation and cyber threats – the document states that without concrete steps to mitigate the impact of these threats, Slovak opposition will continue to undermine public confidence in Slovak institutions and weaken the government by discrediting Western values and the transatlantic alliance.[69] In addition, the document acknowledges that the lack of resilient, democratic institutions and reforms to fight corruption to increase public trust will bolster authoritarian and extremist political movements and make Slovakia more susceptible to external influences. The ICS also notes that a failure to protect the vital role of the media and civil society could degrade democracy and empower anti-Western forces in the country.[70]

A summary of the U.S. perspective vis-à-vis the V4 countries

The U.S. Integrated Country Strategies for Hungary and Poland highlight the importance of strengthening relationships with these countries. Both strategies emphasise the significance of democratic values and human rights and the need to counteract aggressive behaviour from geopolitical powers such as Russia and China. They also stress the importance of economic and technological cooperation to benefit the U.S. and the respective countries. However, the ICS for Hungary mainly positions Budapest as a partner in addressing global challenges, while the one for Poland describes Warsaw as a staunch U.S. ally and a strategic partner on NATO's eastern flank. The focus on Poland's role as a key ally in NATO sets it apart from the description of Hungary as a partner. Additionally, the ICS for Poland emphasises the deep historical, cultural and economic ties that strengthen the American–Polish partnership, while the ICS for Hungary primarily focuses on Hungary's potential to contribute as a NATO ally and an EU partner. Overall, while both ICSs mentioned above share common themes related to democratic values, human rights and economic collaboration, the specific emphasis and positioning of each country set them apart. This is even though, according to Hungary's National Security Strategy, the "Hungarian and Polish nations are linked by a thousand years of shared history and brotherhood-in-arms", and Hungary "strives to maintain a strategic partnership with the Republic of Poland".[71]

The U.S. Integrated Country Strategies for the Czech Republic and Slovakia emphasise the importance of democratic ideals, transatlantic relations and combatting global challenges. Both countries face threats such as disinformation, cyberattacks and regional instability and are considered crucial allies by the United States. More precisely, the Czech Republic is seen as a steadfast ally and like-minded partner of Washington, fully dedicated to supporting Ukrainian sovereignty, meeting NATO commitments, collaborating on technology, research and innovation, and addressing energy needs using U.S. commercial technology. The ICS also highlights the Czech Republic's outspoken

[69] Integrated Country Strategy: Slovak Republic 2022: 7–9.

[70] Integrated Country Strategy: Slovak Republic 2022: 11.

[71] Hungary's National Security Strategy 2020: paragraph 111. Speaking at a festival in Tusnádfürdő, Romania, on 27 July 2024, Hungarian Prime Minister Viktor Orbán commented on Poland, saying the Poles are "pursuing the most hypocritical and deceitful policy in Europe": they are lecturing Hungary morally and criticising the Hungarian Government for Hungary's relations with Russia, while at the same time, Poland is also buying gas from Russia, albeit indirectly (Joób – Horváth Kávai 2024).

support for U.S. interests and the need for the European Union as a strong and like-minded partner. Regarding Slovakia, the ICS emphasises the country's dedication to democratic ideals and its transatlantic identity. At the same time, it underscores the risk of increasing threats from the East disrupting Europe and weakening shared values. The ICS aims to expand bilateral and multilateral cooperation to bolster regional and global security and stability. In addition, the U.S. ICS highlights the risk of increasing disinformation and online conspiracy theories as a primary source of information in Slovakia.

In regard to foreign policy towards Moscow and Beijing, the U.S. is concerned about Russian and Chinese influence and their efforts to undermine democratic institutions. The United States has expressed concern about Hungary's "too close" relationship with Russia several times in recent years.[72] The ICS for the Czech Republic highlights the importance of addressing these threats with the European Union and NATO, and improving its ability to combat disinformation. Meanwhile, regarding Slovakia, the respective country strategy highlights the need to address disinformation campaigns, influence operations and hybrid threats, and it also aims to become a more active and capable partner in responding to these challenges.

Conclusion

After analysing the national security strategies of Hungary, Poland, the Czech Republic and Slovakia, it is evident that the Visegrád Group countries have distinct approaches to their relationships with the United States, Russia and China. The recent breakdown of relations within the V4 countries, primarily stemming from their responses to Russia's invasion of Ukraine, made the fundamental differences in their security strategies apparent. This rupture has resulted in a division within the group, with Poland and the Czech Republic forming a pro-Ukraine block and Hungary – joined in rhetoric by Slovakia with Robert Fico's return to power – comprising a Ukraine-sceptic block. Furthermore, Hungary stands out as an outlier among the V4 countries since it aims to pursue pragmatic cooperation with Russia and China amid the deterioration of relations with the United

[72] In October 2023, Hungarian Prime Minister Viktor Orbán met Russian President Vladimir Putin at the Belt and Road Forum in Beijing. He was the only EU leader to attend the forum or to maintain close ties with Moscow since Russia invaded Ukraine on 24 February 2022. In response, U.S. Ambassador to Hungary David Pressman issued a statement expressing the United States' concerns about Hungary's relationship with Russia. This has occurred after a year-long deterioration in relations between Budapest and Washington, primarily due to Hungary's extended delays in ratifying Sweden's NATO membership. Pressman has for months criticised Orbán for effectively siding with Putin over the war in Ukraine. By March 2024, his remarks indicated that trust in Hungary among NATO allies had effectively collapsed. The U.S. Ambassador to Budapest warned that Prime Minister Viktor Orbán is jeopardising Hungary's position as a trusted NATO ally with "its close and expanding relationship with Russia", and with "dangerously unhinged anti-American messaging" in state-controlled media. The Hungarian Prime Minister sparked controversy when he visited Ukraine, Russia and China consecutively as part of a "peace mission" for Ukraine – as the Hungarian Government called it – right after Hungary began its six-month rotating presidency of the Council of the European Union in July 2024, giving Orbán a higher profile (Győri 2023; Higgins 2024; Troianovski–Higgins 2024; Buckley–Higgins 2024).

States. In addition, Hungary's example shows that going against the pro-Ukrainian camp can draw heavy criticism.[73]

The divergence in views within the Visegrád Group has implications for the V4 countries' future interactions with each other, and this division will also be visible when it comes to these countries' bilateral relations with the United States, Russia and China in the future. While the pro-Ukraine countries intend to maintain close cooperation with Washington, the Ukraine-sceptic countries are critical of Western policies supporting Ukraine. This contrasting stance can have significant ramifications in light of the strategic importance of the Central European region, particularly as part of NATO's eastern flank.

Considering how the V4 countries' differing perspectives regarding the United States, Russia and China are reflected in their national security strategies, this recent rupture within the Visegrád Group or the deterioration of U.S.–Hungarian relations and the improvement of the U.S.–Polish relations is not that surprising. The nature of these references sheds light on whether these great powers are viewed as close allies, reliable partners, or security threats. This comparative analysis highlights the complexities and divisions within the Visegrád Group. However, it also points out the dynamic nature of international relations.

In our analysis, we did not go deeper into the geopolitical events of recent years, the internal political developments that occurred in individual countries or government changes. The analysis of the deterioration of the strategic environment, domestic events and shifts in foreign policy could be the topic of further research. Also, examining the bilateral relations between V4 countries and Russia or China could help us better understand our region's current state of affairs. In the meantime, we may expect a new national security strategy from certain V4 member states that would better reflect recent years' developments.

References

Agreement Between the Government of the United States of America and Government of the Republic of Poland on Enhanced Defense Cooperation (ECDA). United States of America, Department of State, 15 August 2020. Online: www.state.gov/wp-content/uploads/2021/01/20-1113-Poland-EDCA.pdf

Agreement on Defense Cooperation Between the Government of the United States of America and the Government of Hungary. United States of America, Department of State, 4 April 2019. Online: www.state.gov/wp-content/uploads/2019/10/19-821-Hungary-Defense-TIMS-61984-Frank.pdf

[73] According to the Hungarian Prime Minister, Russia's leadership was "hyper-rational", and Ukraine would never be able to fulfil its hopes of becoming a member of the European Union or NATO. Viktor Orbán forecasts a shift in global power away from the "irrational" West towards Asia and Russia. As he put it in a speech in July: "In the next long decades, maybe centuries, Asia will be the dominant center of the world" (Reuters 2024).

Agreement on Defense Cooperation Between the Government of the United States of America and the Government of the Slovak Republic. United States of America, Department of State, 1 April 2022. Online: www.state.gov/wp-content/uploads/2022/05/22-401-Slovakia-DCA.pdf

Al Jazeera (2024): Poland's Tusk Says Ukraine–Russia War a Fight 'Between Good and Evil'. *Al Jazeera,* 22 January 2024. Online: www.aljazeera.com/news/2024/1/22/poland-pm-visits-ukraine-in-latest-show-of-solidarity-in-war-against-russia

Bachulska, Alicja (2021): What's Behind Poland's Sudden Change of Heart About China? *China Observers in Central and Eastern Europe (CHOICE),* 21 July 2021. Online: https://chinaobservers.eu/whats-behind-polands-sudden-change-of-heart-about-china/

Basora, Adrian (2011): The Value of the Visegrad Four. *Atlantic Council, Issue Brief,* 14 February 2011. Online: www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-value-of-the-visegrad-four/

Bayer, Lili (2023): Orbán Is Telling Ukraine to Quit. *Politico,* 1 February 2023. Online: www.politico.eu/article/hungary-viktor-orban-is-telling-ukraine-to-quit-russia-war/

Beck, Robert (2024): The Visegrád Four: From Troubled to Broken. *Foreign Policy Research Institute,* 3 April 2024. Online: www.fpri.org/article/2024/04/visegrad-four-from-troubled-to-broken/

Buckley, Chris – Higgins, Andrew (2024): Viktor Orban, Hungary's Leader, Surprises Europe again with Visit to China. *The New York Times,* 7 July 2024. Online: www.nytimes.com/2024/07/07/world/asia/orban-hungary-china-xi.html

Castle, Stephen (2018): Former Russian Spy Mysteriously Falls Ill in Britain. Again. *The New York Times,* 5 March 2018. Online: www.nytimes.com/2018/03/05/world/europe/russian-spy-falls-ill-in-britain-again.html

Ceenergy News (2023): SPP Renews Gas Contracts to Strengthen Energy Diversification in Slovakia. *Ceenergy News,* 13 April 2023. Online: https://ceenergynews.com/oil-gas/spp-renews-gas-contracts-to-strengthen-energy-diversification-in-slovakia/

Cook, Lorne (2024): Hungary Agrees Not to Veto NATO Support to Ukraine as Long as It's Not Forced to Help out. *The Associated Press,* 12 June 2024. Online: https://apnews.com/article/nato-ukraine-russia-war-hungary-support-assistance-a08164782c1391076fda550190580a4c

Corera, Gordon (2021): Salisbury Poisoning Suspects 'Linked to Czech Blast'. *BBC News,* 18 April 2021. Online: www.bbc.com/news/uk-56790053

Daniška, Jaroslav (2018): Visegrad: From Intellectual Idea to Political Reality. *International Issues & Slovak Foreign Policy Affairs,* 27(1–2), 43–53. Online: www.jstor.org/stable/26592068

Euractiv (2014): Slovakia Nurtures Special Ties to Russia, Despite EU Sanctions. *Euractiv,* 23 May 2014. Online: www.euractiv.com/section/central-europe/news/slovakia-nurtures-special-ties-to-russia-despite-eu-sanctions/

Fiala, Petr (2022): Czech PM: Ukraine's Fight Is Our Fight too. *Politico,* 31 October 2022. Online: www.politico.eu/article/ukraine-russia-war-czech-pm/

Gosling, Tim (2022): The War in Ukraine Undermines Orban's Illiberal Project. *Foreign Policy,* 10 May 2022. Online: https://foreignpolicy.com/2022/05/10/ukraine-conflict-visegrad-group-orban-hungary-illiberal/

Government Resolution 1163/2020 (IV. 21.) on Hungary's National Security Strategy. Online: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html

Greilinger, Gabriela (2023): China's Growing Foothold in Hungary. *The Diplomat*, 27 February 2023. Online: https://thediplomat.com/2023/02/chinas-growing-foothold-in-hungary/

Groszkowski, Jakub (2018): The V4 and the EU. *International Issues & Slovak Foreign Policy Affairs*, 27(1–2), 3–15. Online: www.jstor.org/stable/26592065

Győri, Boldizsár (2024): U.S. Says It Is 'Concerned' about Hungary's Relationship with Russia. *Reuters*, 20 October 2023. Online: www.reuters.com/world/europe/us-says-it-is-concerned-about-hungarys-relationship-with-russia-2023-10-20/

Higgins, Andrew (2023): No One in Europe Is Telling Poland to 'Shut Up' Now. *The New York Times*, 21 February 2023. Online: www.nytimes.com/2023/02/21/world/europe/poland-russia-ukraine.html

Higgins, Andrew (2024): Orban Endangers Hungary's Status as an Ally, U.S. Diplomat Says. *The New York Times*, 14 March 2024. Online: www.nytimes.com/2024/03/14/world/europe/orban-hungary-nato-us.html

Hrabovska Francelova, Nina (2022): Slovak–US Defence Pact Encounters Fierce Resistance. *Balkan Insight*, 18 January 2022. Online: https://balkaninsight.com/2022/01/18/slovak-us-defence-pact-encounters-fierce-resistance/

Integrated Country Strategy: Czech Republic. Department of State, United States of America. March 21, 2022. Online: www.state.gov/wp-content/uploads/2022/06/ICS_EUR_Czech-Republic_Public.pdf

Integrated Country Strategy: Hungary. Department of State, United States of America. May 3, 2022. Online: www.state.gov/wp-content/uploads/2022/10/ICS_EUR_Hungary_03MAY2022_Public.pdf

Integrated Country Strategy: Poland. Department of State, United States of America. June 13, 2022. Online: www.state.gov/wp-content/uploads/2022/07/ICS_EUR_Poland_Public.pdf

Integrated Country Strategy: Slovak Republic. Department of State, United States of America. March 25, 2022. Online: www.state.gov/wp-content/uploads/2022/06/ICS_EUR_Slovak-Republic_Public.pdf

Janicek, Karel (2021): Czechs Expel 18 Russians Over Huge Depot Explosion in 2014. *The Associated Press*, 17 April 2021. Online: https://apnews.com/article/czech-republic-russia-andrej-babis-c593f724a16622eb6d0a19bae3d710be

Janicek, Karel (2024): Deep Divisions on Russia's War in Ukraine Were Evident at a Meeting of 4 Central European Countries. *The Associated Press*, 27 February 2024. Online: https://apnews.com/article/czech-republic-poland-ukraine-war-russia-cb30efe44a452b8e4871aa1d1182ddda

Janjevic, Darko (2018): Putin and Viktor Orban's Special Relationship. *Deutsche Welle*, 18 September 2018. Online: www.dw.com/en/vladimir-putin-and-viktor-orbans-special-relationship/a-45512712

Joób, Sándor – Horváth Kávai, Andrea (2024): Orbán's Grand Strategy for Hungary during the Impending Change in World Order. *Telex*, 27 July 2024. Online: https://telex.hu/english/2024/07/27/from-the-rational-russians

Judson, Jen (2024): Aegis Ashore Poland Enters Maintenance Period Ahead of NATO Acceptance. *Defense News,* 22 January 2024. Online: www.defensenews.com/naval/2024/01/22/aegis-ashore-poland-enters-maintenance-period-ahead-of-nato-acceptance/

Kowalski, Bartosz (2023): The Czech Republic Puts Another Dent in China's Relations with Europe. *RUSI*, 13 February 2023. Online: www.rusi.org/explore-our-research/publications/commentary/czech-republic-puts-another-dent-chinas-relations-europe

McCausland, Phil (2023): Hungary's Prime Minister Called U.S. a Main Adversary, Leaked Documents Say. *NBC News,* 12 April 2023. Online: www.nbcnews.com/politics/national-security/hungary-prime-minister-calls-us-adversary-leaked-documents-rcna79367

Ministry of National Defence, Republic of Poland (2024): *Increasing the US Military Presence in Poland.* Online: www.gov.pl/web/national-defence/increasing-the-us-military-presence-in-poland

Morris, Loveday (2023): CIA Leak, Sanctions Highlight Strained Relations between U.S. and Hungary. *The Washington Post*, 12 April 2023. Online: www.washingtonpost.com/world/2023/04/12/hungary-bank-sanctions-orban/

National Security Strategy of the Republic of Poland 2020. Online: www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

NATO 2022 Strategic Concept (2022). Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2024a): Washington Summit Declaration. *North Atlantic Treaty Organization*, 10 July 2024. Online: www.nato.int/cps/en/natohq/official_texts_227678.htm

NATO (2024b): NATO Missile Defence Base in Poland Now Mission Ready. *North Atlantic Treaty Organization*, 10 July 2024. Online: www.nato.int/cps/en/natohq/news_227649.htm

Naval Sea Systems Command (2024): Aegis Ashore Poland Completes First Maintenance Availability. *Forward Deployed Regional Maintenance Center,* 6 June 2024. Online: www.navsea.navy.mil/Media/News/Article-View/Article/3799399/aegis-ashore-poland-completes-first-maintenance-availability/

OEC (2022a): *China–Slovakia.* Observatory of Economic Complexity. Online: https://oec.world/en/profile/bilateral-country/chn/partner/svk

OEC (2022b): *China–Hungary.* Observatory of Economic Complexity. Online: https://oec.world/en/profile/bilateral-country/chn/partner/hun

OEC (2022c): *China–Poland.* Observatory of Economic Complexity. Online: https://oec.world/en/profile/bilateral-country/chn/partner/pol

Organski, Abramo Fino Kenneth – Kugler, Jacek (1980): *The War Ledger.* Chicago–London: The University of Chicago Press. Online: https://doi.org/10.7208/chicago/9780226351841.001.0001

Pardo, Pedro (2024): Leader of NATO Member Poland Visits China, Talks to Xi about Ukraine, Peace and Trade. *The Associated Press*, 24 June 2024. Online: https://apnews.com/article/china-poland-duda-xi-russia-ukraine-f82b4b95830f908b00d576295f23e329

Paszak, Pawel (2021): Poland–China Relations in 2021: Current State and Prospects. *Warsaw Institute*, 29 January 2021. Online: https://warsawinstitute.org/poland-china-relations-2021-current-state-prospects/

Pollet, Mathieu (2024): Slovak PM: Ukraine Must Give Up Territory to End Russian Invasion. *Politico,* 21 January 2024. Online: www.politico.eu/article/slovakia-prime-minister-robert-fico-ukraine-cede-territory-russia-moscow-invasion-nato-entry/

Poushter, Jacob – Huang, Christine – Clancy, Laura (2022): Spotlight on Poland: Negative Views of Russia Surge, but Ratings for U.S., NATO, EU Improve. *Pew Research Center,* 22 June 2022. Online: www.pewresearch.org/global/2022/06/22/spotlight-on-poland-negative-views-of-russia-surge-but-ratings-for-u-s-nato-eu-improve/

Radio Free Europe – Radio Liberty (2019): Orban Defends Hungary's Good Relations with Russia. *Radio Free Europe – Radio Liberty,* 30 October 2019. Online: www.rferl.org/a/putin-to-visit-eu-nation-hungary-as-russian-presence-grows/30243531.html

Reuters (2022): U.S. Treasury to End 1979 Treaty with Global Minimum Tax Holdout Hungary. *Reuters,* 9 July 2022. Online: www.reuters.com/world/europe/us-treasury-end-1979-treaty-with-global-minimum-tax-holdout-hungary-2022-07-08/

Reuters (2024): Hungary's Orban Says Russia Stands to Gain as 'Irrational' West Loses Power. *Reuters,* 27 July 2024. Online: www.reuters.com/world/europe/hungarys-orban-says-russia-stands-gain-irrational-west-loses-power-2024-07-27/

Rošteková, Maria – Roulet, Gilles (2014): The Visegrád Group – A Model to Follow? *Politeja,* 11(2(28), 181–194. Online: https://doi.org/10.12797/Politeja.11.2014.28.08

Sebena, Martin (2024): Collateral Damage: Slovakia Caught in the China–EU Crossfire. *The Diplomat,* 31 May 2024. Online: https://thediplomat.com/2024/05/collateral-damage-slovakia-caught-in-the-china-eu-crossfire/

Security Strategy of the Czech Republic 2023. Online: https://mzv.gov.cz/file/5161068/Security_Strategy_of_the_Czech_Republic_2023.pdf

Security Strategy of the Slovak Republic 2021. Online: www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf

Szandelszky, Béla (2024): Hungary and China Sign Strategic Cooperation Agreement during Visit by Chinese President Xi. *The Associated Press,* 10 May 2024. Online: https://apnews.com/article/chinas-xi-welcomed-hungary-talks-orban-0719880a351a5ef0763ae6a623a7798b

Than, Krisztina (2023): US Tightens Conditions of Visa Waiver Program for Hungary. *Reuters,* 1 August 2023. Online: www.reuters.com/world/us-tightens-conditions-visa-waiver-program-hungary-2023-08-01/

Törő, Csaba – Butler, Eamonn – Grúber, Károly (2014): Visegrád: The Evolving Pattern of Coordination and Partnership after EU Enlargement. *Europe–Asia Studies,* 66(3), 364–393. Online: https://doi.org/10.1080/09668136.2013.855392

Trading Economics (2023a): *The Czech Republic's Imports by Country.* Online: https://tradingeconomics.com/czech-republic/imports-by-country

Trading Economics (2023b): *Slovakia's Imports by Country.* Online: https://tradingeconomics.com/slovakia/imports-by-country

Treaty Establishing Friendly Relations Between the United States and Hungary (1922). *The American Journal of International Law,* 16(1), 13–16. Online: https://doi.org/10.2307/2212938

Troianovski, Anton – Higgins, Andrew (2024): Viktor Orban Meets Vladimir Putin, Dismaying E.U. *The New York Times,* 5 July 2024. Online: www.nytimes.com/2024/07/05/world/europe/orban-putin-meeting-russia-hungary.html

U.S. Department of Defense (2024a): Defense Security Cooperation Agency, Foreign Military Financing. Online: www.dsca.mil/foreign-military-financing-fmf

U.S. Department of Defense (2024b): Security Cooperation Agency, International Military Education and Training. Online: www.dsca.mil/international-military-education-training-imet

U.S. Department of State (2021a): *U.S. Relations with Hungary.* Bilateral Relations Fact Sheet. *Bureau of European and Eurasian Affairs,* 6 April 2021. Online: www.state.gov/u-s-relations-with-hungary/

U.S. Department of State (2021b): *U.S. Relations with Poland.* Bilateral Relations Fact Sheet. *Bureau of European and Eurasian Affairs*, 20 January 2021. Online: www.state.gov/u-s-relations-with-poland/

U.S. Department of State (2024a): Joint Statement on U.S.–Poland Strategic Dialogue. *U.S. Department of State,* 22 April 2024. Online: www.state.gov/joint-statement-on-u-s-poland-strategic-dialogue/

U.S. Department of State (2024b): Office of Global Programs and Initiatives, Security Forces Capacity Building Division, Global Defense Reform Program. Online: www.state.gov/key-topics-office-of-global-programs-and-initiatives/#sfcb

U.S. Department of State (s. a.): *Integrated Country Strategies.* Foreign Assistance Resource Library. Online: www.state.gov/integrated-country-strategies/

U.S. Department of the Treasury (2022): United States' Notification of Termination of 1979 Tax Convention with Hungary. *Press Release*, 15 July 2022. Online: https://home.treasury.gov/news/press-releases/jy0872

Zachar, Pavol (2022): Slovakia Approves Defense Military Treaty with US. *The Associated Press*, 9 February 2022. Online: https://apnews.com/article/russia-ukraine-business-europe-slovakia-bratislava-07dfd58fd47d672db840eb37583d8376

Zemánek, Ladislav (2023): Czech Republic Economy Briefing: Czech–Chinese Economic Relations in Challenging Times. *China–CEE Institute Weekly Briefing*, 61(2), 1–4. Online: https://china-cee.eu/2023/04/25/czech-republic-economy-briefing-czech-chinese-economic-relations-in-challenging-times/

AARMS Vol. 23, No. 3 (2024) 61–88.

10.32565/aarms.2024.3.4

The Special Legal Order and the Renewed Strategies and Normative Framework of Security and Defence Policies in Hungary

Sándor MÓRÉ[1] – György Péter SZILVÁSY[2]

Recent years have brought challenges of arguably unprecedented number and scale to the global security and defence policy environment of states and international organisations. It is probably enough to mention, among many other crises, the Russian–Ukrainian conflict, the Covid–19 pandemic, the internationalisation of terrorism, the increased migratory pressure on Europe, as well as climate change or the emerging threats in cyberspace. Both international and national legislators are looking for new types of responses to these novel forms of challenges. Accordingly, in recent years, Hungary has started to build a new legal environment for defence and security. In our study, we will first consider the strategic framework of this new legal framework, followed by a description of the amended special legal order rules of the Fundamental Law and the new laws that implement the renewed organisation of the comprehensive defence and security system. The future of the subject at hand is unfortunately bleak; yet it may be somewhat clearer if the responses to international conflicts and other threats are underpinned by active preparation.

Keywords: *defence and security regulation, defence law, special legal order, national security and military strategy, security and defence policy*

Introduction

It is undeniable that the past decade has presented the world with challenges that it has probably never faced before – at least not of this nature or on this scale. The global security environment is facing extraordinary challenges, including the Russian–Ukrainian conflict, the migratory pressures affecting Europe to a significant extent, the Covid-19 pandemic or, more recently, the renewed flare-up of the Armenian–Azeri and Hamas–Israeli conflicts.

There is no question that within this field of security policy, Hungary must also seek new answers to the challenges. As part of this, large-scale changes have taken place in recent years, both at the level of government strategies and at the level of the Constitution and the laws and regulations, which has essentially been a continuous legislative task for

[1] Károli Gáspár University of the Reformed Church, Faculty of Law, e-mail: more.sandor@kre.hu

[2] Ludovika University of Public Service, Faculty of Law Enforcement, e-mail: szilvasy.gyorgy.peter@uni-nke.hu

both the Parliament and the Government. Among other things, the constitutional legislation on the special legal order and the system of rules on defence have been renewed, and a new law on the coordination of defence and security measures was passed. In connection with these factors, a number of implementing regulations have been adopted in the government's legislative sphere. It is also notable that the framework for the renewed legal norms is laid down in plans and strategies set out in government decisions.

Given the limitations of space, in this paper the legal framework will be presented as an overview that seeks to provide new responses to the novel security challenges. We will also discuss the constitutional and legislative changes and the normative strategic frameworks that underpin them in various respects. Further, we will summarise and concisely assess the normative provisions.

The National Security Strategy

In 2020, the Government of Hungary adopted the *National Security Strategy* entitled "Secure Hungary in a Volatile World" [Government Decision 1163/2020 (IV. 21.)]. As can be seen, the Strategy was prepared before the current situation of the Russian–Ukrainian conflict (although with the developments in Crimea in mind). Nevertheless, the experiences of the pandemic were already present and considered.

It is important to point out at the outset that the Strategy was published in the form of a normative government decision.[3] This means that it was not adopted as legislation but as a so-called *public law regulatory instrument.* Public law regulatory instruments essentially contain provisions and expectations concerning the organisation, operation, activities and action programmes of public bodies.[4] Their binding power does not apply to everything, only to the issuing body and any subordinate body (in this case, the Government, ministries and subordinate bodies of the public administration), and are therefore considered to be *internal acts*.[5] A public law regulatory instrument may not be contrary to the law.[6]

1. The National Security Strategy starts out by identifying the current global *security policy factors* that pose significant challenges: the emerging multipolar world order, the drive to redesign the rules governing the relations of international actors, the changing layout of security challenges, and global challenges such as the accelerating climate and demographic change, the closely related illegal and mass migration, the depletion of

[3] Since 2020, the Government has adopted a large number of sectoral strategies (e.g. health, public education, construction, tourism, space, agglomeration rail, anti-corruption, and so on) following the completion of the comprehensive public administration development strategies. On the importance of governmental strategic planning, see e.g. Sántha 2023: 154–160. It is noted here that the obligation to draw up both the National Security Strategy and the National Military Strategy is created by point 17 of Parliamentary Decision 94/1998 (XII. 29.) *on the Principles of the Security and Defence Policy of the Republic of Hungary.* The source of law status of the Parliamentary Decision is otherwise identical to that of the Government Decisions in that it is also *a normative decision*, i.e. *a public law regulatory instrument.*

[4] See Chapter VI of Act CXXX of 2010 on Legislation.

[5] This is also reflected in the technicality that, unlike legislation, public law regulatory instruments are not promulgated but *published.* On *internal acts* see Jakab 2007: 116–118; Jakab 2016: 147–148.

[6] Article 24 (1) of Act CXXX of 2010 on Legislation.

natural resources, and the society-shaping effects of the technological revolution. The Strategy *aims* to maintain and strengthen Hungary's current level of security and, in doing so, ensure the country's continued development in a volatile world. The aim is to make Hungary one of the safest states in Europe and the world by 2030 by maintaining a high level of public security (internal security) and building a modern military force (external security).

2. The Strategy uses several general formulations that point to *obligations* deriving from Hungary's Fundamental Law and our international and EU obligations (e.g. the protection of national sovereignty, security as a fundamental value, the protection of democracy and the rule of law, legal certainty, an independent judiciary, international peace and security, the requirement of international law for the peaceful settlement of disputes, responsibility for Hungarians beyond the borders, and so forth). Special mention should be made of our country's NATO membership, a fundamental condition for security. The Strategy attaches great importance to our EU membership, of course, and to the formation of the Visegrád Group (V4), but also to the effective functioning of the Organisation for Security and Cooperation in Europe and the Council of Europe.

3. Among the *fundamental characteristics of our country,* the Strategy underlines that the political system is stable and the public security situation is balanced. At the same time, the country's size and position in the world economy, as well as its limited defence capabilities make it clear that it can respond to fundamental security challenges primarily through international cooperation and as a member of alliance systems. This is all the more significant given that Hungary's geostrategic position means that it faces a particularly large number of security challenges from Europe's southern and eastern neighbours. An important element of our country's position is that we must protect a long strand so forth of the external borders of the Schengen area, to which the physical border closure and appropriate staffing will actively contribute. The Hungarian Defence Forces, with their increased numbers and continuously improved equipment, also have a key role to play in guaranteeing our defence and security. In addition, the Strategy naturally underlines the importance of law enforcement, counterterrorism and disaster management. In this context, it is particularly important to highlight the urgent requirements for civil protection, defence management, the protection of critical infrastructure and the safe use of technologies related to radioactive materials. The need to increase resilience against hybrid attacks (e.g. information and cyber warfare) cannot be neglected.

4. The Strategy also identifies *Hungary's economic position* as an important factor. The limited natural resources of Hungary, its high dependence on imports and the possibility of a significant shortage of energy resources (especially natural gas) may pose serious challenges and threats to a stable economy. The only non-renewable energy resource mentionable is coal, of which there is still a significant amount underground. It is also important to highlight Hungary's strong position in agriculture: the domestic food supply is stable, food safety is high, and imports of genetically modified crops are banned. Still, the significance of global climate change cannot be underestimated; it could also affect our current stable drinking water base.

5. *Population decline* and the ageing of Hungarian society pose a significant challenge. To counter this, the country is making strong efforts to promote childbearing, while

according to the latest reports, never before in Hungary have so few children been born in a month as in June 2024.[7] It also aims to improve the quality of public and higher education and to stabilise its position in international scientific and technological competition.

6. The Strategy deals extensively with *Hungary's security environment* and the risks that continue to threaten the currently stable security situation. The following shall be highlighted:

- climate change, extreme weather events, overpopulation in Africa and Asia and mass migration
- the population decline and ageing society of the European continent
- the shrinking availability of global resources
- religious fundamentalism
- cross-border terrorism utilising novel techniques and tools, as well as the proliferation of weapons of mass destruction
- organised crime becoming transnational
- the technological revolution (digitalisation, 5G, space technology) and the related vulnerabilities of electronic information systems
- the complexity and rapid spread of crises
- asymmetric and hybrid warfare
- the precarious security situation in the Western Balkans
- the emergence of pandemics
- strategies to influence political, economic and social processes sponsored by state and non-state actors
- the proliferation of cryptocurrencies that are not yet properly regulated by law
- increasing urbanisation

These massive and complex processes foreshadow the emergence of a new world order. The economic, social, demographic and environmental transformations, which are huge, rapid and often very difficult to follow, require careful preparation and complex responses. Linked to this is Hungary's failure to develop robust strategic offensive capabilities, while attaching great importance to arms control and disarmament efforts.

7. The Strategy devotes great attention to the representation of *Hungary's fundamental interests*. In this context, it emphasises the promotion of *national security interests* as a starting point. Naturally, the country considers the preservation of its sovereignty, territorial integrity and constitutional order, the guarantee of its citizens' security, the stability of the country, its sustainable economic, social and cultural development, and the enforcement of human rights and fundamental freedoms as its primary security interests. Furthermore, the maintenance of international peace, security, stability and cooperation, the promotion of democratic principles and sustainable development and the strengthening of Euro-Atlantic and European security structures are noted to be in the national security interest.

[7] KSH 2024.

For our country, one of the most important interests and values is the responsibility we bear for Hungarians living beyond our borders. In this context, the possibility for people to stay in their homeland and the assistance provided locally are given special attention. Hungary has an interest in a strong and stable Ukraine, but also in protecting the rights of the Hungarian community in Transcarpathia. In the period since the adoption of the Strategy, due to known unfortunate events, Hungary has provided assistance to a large number of refugees from Ukraine.

For Hungary, the stability of the Euro-Atlantic and European areas, especially the Central European region and the neighbouring countries, is of paramount importance. The position of the Balkan and Eastern European countries is also of vital importance. From a geographical, ecological, historical and cultural point of view, the Carpathian Basin as a natural area is also of great significance to us.

At the same time, our security interests are also affected by developments further afield concerning the security situation in the Middle East, North Africa, the Sahel and Central Asia. In the time since the adoption of the Strategy, the renewed and intensified conflicts in the Middle East region are a particular cause for concern and a growing security risk.

Our membership of international organisations (UN, NATO, EU, OSCE, the Council of Europe) serves the stability of our country's security and defence policy; maintaining and developing the V4 cooperation is a priority national interest. The Strategy envisages the future of the European Union as an association of sovereign nation states, not a federation. Particular attention should be paid to the battle against terrorism in all its forms. Considering our energy supply, the strengthening of energy security, decarbonisation (with a focus on the role of nuclear energy), the diversification of energy supply and the reduction of the need for imports are fundamental Hungarian objectives. As indicated earlier, Hungary's coal reserves could, temporarily, strengthen its position, especially in electricity generation.

The Strategy sets out in detail the framework for our cooperation with some countries that bear particular significance. Specifically, it describes our relations with Germany, Poland, the United States, Italy, France and Turkey as well as the security policy and, where appropriate, the geostrategic importance of these countries. It also highlights the importance of the post-Soviet space, the Middle East, certain Asian, African and Latin American states and regional organisations in terms of foreign trade and investment. The Strategy also specifically addresses the growing global roles of Russia and China. In view of the military aggression launched against Ukraine in the period following the adoption of the Strategy, a review of these aspects of the Strategy may be timely. However, the document already recognises the significant risk of Russia's tensions with NATO and the EU in 2020.

The Strategy highlights the importance of improving Hungary's position in science and technology, as we aim to be at the forefront of the world in this respect.[8] High-quality research and innovation, modernised public education, vocational training and higher

[8] In this context, it is worth pointing out that in 2023, two scientists of Hungarian origin were awarded the Nobel Prize.

education all play a key role in this.[9] In terms of security, higher education for military, law enforcement and public administration,[10] as well as the IT sector, merit special attention.

The protection of natural resources, in particular water sources, drinking water and arable land is of strategic importance to Hungary's security interests in the face of the adverse effects of climate change. Cooperation on water security with countries in shared river basins is also a priority,[11] as the effects of pollution in other countries, for example along the Danube or the Tisza, have a major impact on Hungary.

8. Based on the above, the Strategy identifies the following *priority security risks:*

- mass illegal migration
- the possibility of an unexpected armed attack
- coordinated diplomatic, intelligence and information operations conducted against the stability of Hungary
- cyberattacks
- acts of terror
- efforts violating national sovereignty or the significant deterioration or collapse of Hungarian communities beyond the borders, which may lead to mass displacement from the homeland (here again, we can refer to the escalating Russian–Ukrainian conflict)
- a demographic situation that is becoming critical
- international economic crisis
- energy exposure
- serious and lasting instability in our region, possibly in some neighbouring countries
- the rise of organised crime
- use of weapons of mass destruction, attack with nuclear, radiological, biological or chemical agents
- industrial disasters with a regional impact
- epidemics
- major floods and inland floodings or other natural disasters (drought, heat and cold waves, storms, fires)
- persistent water scarcity, drying soil and erosion, and the destruction of vegetation

9. The Strategy sets out Hungary's *strategic objectives in the field of security,* which include the following. The *primary objective* is to strengthen the effectiveness and resilience of national measures as well as the strength of national cooperation in order to ensure security. The prevention, management and response to identified challenges

[9] The "Public Education Indicator System 2023" presents the current state and trends of public education through various indicators. The study highlights that after 2018, the share of expenditure in GDP has increased significantly on average in several Central and Eastern European countries (the Czech Republic, Slovakia, Estonia and, in 2020, Lithuania) and in Western Europe. In contrast, the share of GDP allocated to public education in Hungary remained stable after 2014 (Varga 2024).

[10] Currently, in Hungary, these three areas are managed by a joint higher education institution, the Ludovika University of Public Service. The University has a Faculty of Public Governance and International Studies, a Faculty of Military Science and Officer Training and a Faculty of Law Enforcement.

[11] The higher education provider for water engineering in Hungary is also the abovementioned University, which has its own Faculty of Water Sciences.

is primarily a national responsibility, which is *the responsibility of the Government,* in cooperation with society. The primary basis for security is a solid social, economic and financial structure and a sustainable and flexible system of preventive and protective measures at the national level, including the targeted development of the armed forces and law enforcement agencies (the police, the penitentiary, the national security services, the disaster management and, for its law enforcement functions, the State Tax and Customs Administration). The ability to respond independently at the national level to threats from beyond our borders is vital. It is in the interest of society as a whole to shape and develop the citizens' patriotism, sense of national responsibility and security-conscious mindset. In addition to raising the general levels of the citizens' knowledge on these topics, the training of young people in disaster management, national defence education and the preparation of volunteer reservists play a key role in this process. Hungary's strategic objective is to develop, by 2030, the national resilience, deterrence, defence, crisis management and coordination capabilities that are a prerequisite for the stability and security necessary for the development of the nation in a volatile international environment. According to the Strategy, Hungary's high level of public security, even by international standards, must be maintained and further improved.

The Strategy states that Hungary must ensure the protection of the fundamental rights of Hungarians living beyond its borders. The document has already referred to this earlier, as we have indicated, this can be linked to the reception and care of refugees from Ukraine by providing them with accommodation, as well as work and study opportunities.

Among the strategic objectives, the development of the defence industry and the armed forces is naturally emphasised. This includes, among other things, supporting enterprises in the defence industry, procuring as many products as possible from domestic sources which would be needed for defence, supporting defence research, development and innovation, as well as integrating the domestic knowledge base into the development of the defence industry.

The additional reinforcement of our cooperation within international organisations is also a key objective of the Strategy. In this context, the "collective self-defence" arrangements [Article 5 of the North Atlantic Treaty[12] based on Article 42 (7) of the Treaty on European Union[13]], arms control, disarmament, compliance with and monitoring of non-proliferation regimes, and the Euro-Atlantic and EU integration of neighbouring regions are particularly important. The development of Hungary's bilateral and regional security and defence cooperation frameworks and Hungary's substantive contribution to global development are also high up on the agenda. Among the environmental aspects also set out above, the Strategy makes clear that one of the critical conditions for sustainable social and economic development and the prevention of natural disasters is the mitigation of the effects of climate change, as well as the promotion of environmentally conscious and low-carbon lifestyles in order to reduce the economy's fossil fuel demand.

[12] For a detailed analysis of the article, including a historical retrospective, see Sulyok 2002: 99–136.

[13] For the elements of the Union's common security and defence policy related to this rule see Pünkösty 2023: 443–448.

10. The Strategy summarises, in a repeated and "awareness-raising" way, the *comprehensive tasks and tools* that will make it possible to achieve the objectives. It states that Hungary intends to promote the achievement of its strategic security objectives through predictable, proactive, and value and interest-based foreign, security and defence policy. Furthermore, through the maintenance of adequate self-sufficiency of national armed forces and law enforcement, economic and foreign trade instruments, and finally through effective strategy government communication. According to the Strategy, the Hungarian Government is committed to providing adequate resources for the fulfilment of its tasks.

The document lays emphasis on making the Hungarian Defence Forces able to avert possible armed aggression against the country, both independently and through cooperation in the context of alliances. This requires well-equipped and well-trained defence forces and interoperable capabilities. The defence forces are also responsible for assisting with the consequences of disasters. It is important that defence capabilities are serviced by a defence industry with sufficient capacity.

According to the Strategy, Hungary intends to continue to participate in addressing the management and root causes of crises in the Western Balkans, the Middle East, Africa, Central Asia and other regions with security implications, as well as in any stabilisation and reconstruction processes.

The protection of women and children is a priority in international crisis management. A related objective of the Strategy is to ensure the protection of educational institutions, including IT record-keeping and data systems. The design and delivery of humanitarian aid is equally important.

The Strategy points out that one of the most topical tasks is to coordinate the activities of the bodies responsible for the external and internal security of the state (armed forces, law enforcement agencies and civil authorities). In line with this, coordination and cooperation between foreign affairs, defence, law enforcement, national security, judicial, economic and financial affairs, public health and epidemiology, food safety, disaster management and civil crisis management bodies shall be continued and strengthened.[14] Increased action to combat mass, uncontrolled and illegal migration and trafficking of human beings is of the utmost importance, as is the fight against terrorism and organised crime.

With regard to economic aspects, the Strategy emphasises that the pursuit of a growth and export-oriented economic policy that ensures fiscal balance is closely linked to the economic and social stability of Hungary, and thus to its ability to assert its security policy interests. Industrial development, employment expansion, and the reduction of underground economy and corruption are important tools in this respect. Likewise, efforts to broaden the possibilities for importing natural gas, to ensure the sustainability of the energy mix, to expand the Paks nuclear power plant and to preserve coal assets also bear great significance.

To address the demographic challenge, the Strategy proposes a family policy that promotes responsible parenthood, aims to improve the health of citizens, and mechanises certain production processes as well as reinforcing them with the use of artificial

[14] One of the most important legal instruments is Act XCIII of 2021, which will be discussed in more detail later.

intelligence. The aim is to reduce economic disparities between the country's regions while maintaining social security and providing adequate child protection in order to achieve social inclusion.

The document also pays close attention to addressing challenges, risks and threats within cyberspace. Ensuring the smooth functioning of critical information infrastructures and the development of the cyber defence and cyber operations forces are of particular importance in this context. Further development of the skills of the national security services and close cooperation with allied forces performing similar tasks are essential as well. It is also paramount, according to the document, that Hungary pays special attention to the development of the space sector in terms of innovation, which can give the country considerable leverage in international relations.

Moreover, the Strategy points out that health security is prioritised, especially in light of the recent pandemic. If necessary, the use of military force could be considered (for crisis response, evacuation, quarantine, running military hospitals, and so forth). Great importance should also be attached to the areas of vaccine and pharmaceutical production and the sustainability of healthcare systems.

In order to ensure environmental security, the document identifies as indispensable the increased protection of water and land resources and their intrinsically linked ecosystems, alongside the preservation of biodiversity, the conditions for providing the population with healthy drinking water and non-GMO food, the improvement of air quality, the reduction of carbon dioxide emissions and the enhanced preparedness of public health, veterinary and phytosanitary services.

11. Finally, the Strategy provides guidance to public and governmental bodies on the expectations for the delivery of tasks in line with the document.

Public authorities should continuously assess the issues of national and international security and the threats in their respective fields and take the necessary steps to prevent and address them. Their security-related activities should be consistent with the Strategy, and ministries should also strive for this consistency when developing their own sectoral strategies.

In the event of a significant change in Hungary's security environment or other relevant circumstances, the Strategy will be reviewed.

The National Military Strategy

The National Military Strategy is another key governmental planning document of Hungarian security and defence policy which was adopted by the Government in 2021, also in the form of a normative government decision [Government Resolution 1393/2021 (VI. 24.)]. Given that its legal source is identical to that of the National Security Strategy, the same characteristics apply to this Strategy (its form is that of a *public law regulatory instrument*, i.e. an *internal act*).

While the National Security Strategy can be seen as a comprehensive, general document, the Military Strategy can be understood *as a sectoral (sub)strategy,* which is closely related to the development of the armed forces, the military aspects of the security environment and, of course, the vision for the future Hungarian Defence Forces. Since by its very nature it is in a sense an "implementation" of the first strategy, it is closely in line with it and in many cases repeats its formulations.[15] The Military Strategy is therefore presented here only briefly and in summary.

At the core of the Strategy is the *Zrínyi Defence and Military Development Programme* launched by the Hungarian Government in 2016, which aims to develop a military force that increases security for Hungarian citizens and the military-industrial capacities needed to sustain it. The renewed Hungarian Defence Forces will develop and organise their capabilities in line with the government's defence policy considerations, ensuring the protection of the country's sovereignty and territorial integrity, as well as its citizens and interests. The aim of the military development is to significantly strengthen Hungary's military self-reliance, which is essential not only for its self-defence and deterrence capabilities but also to remain an effective contributor to regional, European and transatlantic security efforts.

The Strategy naturally gives special attention to our membership in NATO but stresses that *national self-reliance* is a fundamental condition for collective defence and effective alliance cooperation. Hungary's *strategic objective* is to build its national Defence Forces by 2030, which as a member of NATO and one of the region's leading military forces, will be capable of guaranteeing the country's security, the deterrence of potential aggression, the support of collective defence against military and non-military threats and challenges, and the fulfilment of responsibilities arising from its membership of the Alliance and the European Union. The Zrínyi Programme provides the framework for this.

According to the document, the country's security is ensured by mutually complementary pillars:

- a modern national defence force complemented by the defence systems of regional cooperation
- the collective defence provided by NATO
- the EU's common security and defence policy
- the UN and OSCE cooperation forums

The Strategy points out that fostering security is a long-term task, and the defence of the country is built on complex and interdependent security elements which are military, economic, political, social, environmental, and cyber and information dimensional in nature. Today's state and non-state threats and challenges can occur across the full spectrum of these security dimensions in various combinations, and defence cannot be treated in isolation from other areas of security. Addressing security challenges goes beyond the remit of individual specialist ministries and requires *holistic governmental cooperation.* At the same time, military capabilities will continue to play a key role in the implementation of national defence tasks. In view of the above, the scope of the Strategy *covers all activities and organisations in the defence sector that are involved in the defence of the country* and in providing capabilities related to our alliance commitments. However, *it provides guidance primarily to the Hungarian Defence Forces.*

[15] On the relationship between the Strategies see Farkas–Till 2022: 21–22.

1. The Strategy examines in detail the security challenges our country faces in the *operational environment* of the 21st century. Overall, the document is pessimistic: the global and European security environment is characterised by instability and unpredictability. Crises in distant regions could have a short-term impact on Hungary's security, increasing the number and range of threats and challenges which Hungary faces. Overall, the global security situation is deteriorating. The shifting balance of power is accompanied by a renewed intensification of great power rivalries and an increased risk of confrontation. In the 21st century, while the purpose of war remains unchanged, the theatres, forms and methods of war are expanding and changing, and its characteristics are increasingly extending to non-military dimensions of security (e.g. *hybrid* warfare or the use of *proxy forces*).

Radical changes are also taking place in the technological sphere. The spread of artificially intelligent robots, revolutionary drone technology, human–robot collaborative military tasking, automated decision-making technologies, military applications of 3D printing, cyberspace operations and directed energy weapons, and military hardware with high-precision and autonomous strike measurement capabilities are fundamentally changing the rules and procedures of warfare.

In modern wars, the concept of "victory" has changed, since the attacking party does not need to occupy the enemy's territory or destroy their army, forces or economic potential in order to achieve a political goal. To achieve victory, it may be sufficient to attack the enemy's centres of state and administrative leadership or vital infrastructures in order to block the functioning of communication systems, to make the political leadership incapable of action, and to strike at the enemy's command and control objects in terms of military forces and military infrastructure, and thus gain total control over the target country. *Outer space* is also the new venue for the deployment of the latest technologies, which gives the major powers in particular a significant competitive advantage, even during times of peace.

2. The Strategy also takes into account the *threats and challenges* that the Hungarian Defence Forces may face. It states that, although the likelihood of an unexpected armed attack by another state against our country is low, the Hungarian Defence Forces must at all times be able to deter an armed attack, even independently. This may be necessary until the arrival of allied forces, or, in the event of an armed attack, to defend the country's independence, territorial integrity, borders, citizens and material assets. Interested state actors may also use *information technology* to cripple or obstruct the command-and-control system of the Hungarian Defence Forces. Moreover, there would be some small probability, but also unforeseeable consequences, of an attack with weapons of mass destruction (including nuclear missile systems), in which the use of the capabilities of the Hungarian Defence Forces would be unavoidable.

In the 21st century, risks from *non-state actors* are becoming increasingly common. In this context, the rise of radical ideologies and terrorism, even within Europe, poses an increased threat. Illegal migration on a massive scale is also a major challenge, which the Defence Forces are actively supporting law enforcement agencies to counter.

The rapid spread and serious consequences of the coronavirus pandemic have shown that the armed forces can play a significant role in managing a crisis of this nature, especially with their high level of organisation, capabilities and extensive logistical infrastructure. The important role of the armed forces in disaster management (both industrial and natural) should be emphasised.

3. In terms of Hungary's *defence capabilities,* the Strategy points out that in the period following the regime change (1989–1990), the level of resources spent on military forces decreased significantly, the life of military technology systems, which were typically Soviet-made, expired, and capacities of the defence industry were degraded. The objectives of the Zrínyi Programme have led to significant changes in the processes set out above, including the development of military systems and infrastructure, the acceleration of holistic governmental decision-making, as well as the development of national resilience and security awareness among citizens. The emergence of a committed and competent workforce with high-quality education, training and continuous professional development, based on targeted knowledge elements, and with adequate physical fitness and mental resilience, is a notable challenge as well, and essential for the successful operation of modern forces.

Hungary's specific geographic location places it at the threshold between the eastern and southern threats identified by NATO, as well as the continental theatres of war in Northern, Eastern and Southern Europe, and its central position allows it to function as a military backbone, procession route, and area for reception, concentration, redeployment and training. In addition to the large-scale cooperation already mentioned (NATO, EU, and so forth), the regional cooperation forums (e.g. V4, Central European Defence Cooperation, Central European Multi-National Command, and so forth) also bear great significance.

4. The Strategy asks the following question: What will *the future of defence* look like? The answers are numerous. Generally speaking, the Hungarian Defence Forces must become a sustainable force that meets the requirements of the times and is modernised in its approach, organisational culture and military technology. It must be well organised, it must respect and cherish national traditions, and it has to be deployed effectively both on its own and within a federal and EU framework. It must also be able to strengthen its capabilities with a reserve system. It must have modern, well-trained and equipped soldiers, as well as flexible, adaptable, effectively deployable and sustainable military capabilities to carry out its domestic and international tasks. The development and maintenance of an adequate and continuously renewable national defence industry is essential for modern forces.

In the case of threats, mainly from state actors, the Strategy recognises the concept of *deterrence* as well as *protection.* A strong national force capable of responding autonomously will in itself provide the *deterrent force* to address the objectives and risks of a potential attack by an adversary of comparable size and potential, and, if an attack is launched, to *defend* the territory and sovereignty of the country with *armed forces.*

The Strategy emphasises that defence is a national issue and that resources and the *coordination* of efforts must be developed at all levels of all organisations of government and public administration. Although the armed defence of the country can only be achieved through the activities of the Hungarian Defence Forces, the nature of the challenges requires the preparation of the whole nation and the strengthening of national *resilience* in the complex system of defence. This also includes the further development of public administration, the economy, social organisations, as well as individuals in times of peace, as the security of the country can only be ensured by the combined existence and cooperation of all these elements. In order to organise the defence of the country in accordance with these principles, an effective *defence management system* must be put in place, in the spirit of a holistic governmental approach. Strengthening the resilience of the Hungarian national economy and the capacities of the national defence industry will serve to enhance resilience. The Hungarian Defence Forces must be able to counter conventional and hybrid threats, enhance national resilience through their military capabilities, guard critical system elements and certain installations of the defence sector requiring increased protection, and support and cooperate with civil and law enforcement agencies. The military intelligence and counterintelligence body, the Military National Security Service, has a special role to play in this area.[16] However, there is also a civilian component to resilience. *Civilian preparedness* is a task comprising part of the national defence system, aimed at ensuring the continuity of governance (administration) and the services provided by vital system elements, as well as securing civilian resources to support the Hungarian Defence Forces and NATO military forces. The coordination between the civil and military aspects of civil preparedness tasks in order to strengthen and develop national resilience is carried out within the system of *defence administration,* which therefore needs to be developed in a manner capable of effectively carrying out the tasks arising from these requirements.

It is an obvious and clear requirement that our country and the Defence Forces should continue to be active and stable participants in *international cooperation.* As mentioned earlier, maintaining and enhancing the capability and readiness to cooperate with allied and EU forces, security and defence organisations is a priority. Of particular relevance in this context is the implementation of commitments under the Permanent Structured Cooperation[17] of the EU Common Security and Defence Policy.

The Strategy also addresses the *civilian component* in detail. It addresses not only the *soldiers* serving in the Defence Forces but also the *civilians* performing service in aid of defence duties. In addition to ensuring a stable and predictable military career, the recruitment, retention, career development and development of the benefits system are also major challenges. In order to guarantee resource replenishment for the Defence Forces, the Strategy sets as a task an effective patriotic and defence education, and the dissemination of relevant basic knowledge to a broader range of society through the institutions of public education, vocational training and higher education.

5. Based on the above, the Strategy also discusses the characteristics of the *modernised Hungarian Defence Forces.* The Hungarian Defence Forces are the primary pillar of guaranteeing the sovereignty and territorial integrity of our country. Accordingly, the Armed Forces carry out their tasks to the standards of the times, as stipulated in the Fundamental Law and the general legal framework. It guarantees Hungary's security and sovereignty through credible deterrence based on its national capabilities, on the one hand, and within the framework of the alliance system, on the other. The *future's Hungarian*

[16] For a detailed regulation of the tasks and competences of the Service see Articles 6–7 of Act CXXV of 1995 on National Security Services.

[17] In short, PESCO.

Army is a modern, highly mobile and responsive organisation, capable of continuous development, adaptation and renewal.

In terms of personnel, the Defence Forces are made up not only of professional and contracted soldiers but also of civilians and so-called *reservists* who support their activities. The Strategy foresees the creation of a Hungarian Defence Force prepared to carry out its tasks independently but also while integrated in the system of alliances, through the planned implementation of comprehensive *improvements* to the capabilities required for defence. It is also notable that making progress in national resilience, which is also integrated into the NATO Crisis Response System, can maintain a high level of the citizens' sense of security and preparedness for elements involved in crisis response.

The Strategy points out that the warfare of the present and the future goes beyond the boundaries of *armed conflict in the traditional sense.* With the expansion of operational space, in addition to classical land and air forces, the electromagnetic, cyberspace and space forces play an increasing role in gaining and maintaining operational superiority, both in deterrence and during times of crisis or armed confrontation. This will require the coordinated development of *new operational spaces*, such as electromagnetic, cyberspace and space assets, in addition to the capabilities of classical forces. The new Hungarian forces are capable of conducting both traditional symmetric and asymmetric warfare, even when faced with irregular forces or an adversary with superior capabilities. To this end, the Strategy includes development concepts for land, air and cyber forces, as well as for support capabilities (e.g. logistics and health). Military tasks will be complemented by a so-called *volunteer area protection force.*

The document under scrutiny envisages force development through the active advancement of command and control, combat support and service, as well as capabilities of adaptation and transformation, and complementary national and hinterland defence. One of the most important components of the latter is the staffing of an ever-expanding so-called *Voluntary Reserve System.*

6. The Strategy also includes objectives for the *defence industry.* The maintenance and development of national defence industrial capabilities and the development of autonomous industrial research and innovation for defence are strategic in nature. They aim to enhance the country's defence credibility, resilience and robustness and to reduce significantly its external economic and technological dependence for defence in the short term. The implementation of the Zrínyi Programme will therefore be supported by related *industrial development programmes.* The Hungarian Government shall support the defence sector through economic instruments and incentives, enabling the production and maintenance of modern military equipment on a domestic basis, developing the necessary production capacities, implementing the technological change necessary for the operation and servicing of new equipment, and providing skilled labour. In a broader sense, the Strategy points out that industrial research and innovation for defence has a positive impact on *the technical quality of the whole economy.*

7. The last point of the Strategy examines the *financial basis* for achieving the objectives set. It states that one of the decisive conditions for the development of the armed forces is that the availability and efficient use of resources for the defence sector shall be commensurate with the performance of the national economy. In line with the requirements of NATO

membership, defence spending should reach 2% of GDP by 2024. Adequate proportions of the so-called defence budget are an essential condition for the implementation of the Zrínyi Programme.

Finally, the Strategy indicates that its timeline is essentially longer term, but that it should be reviewed as necessary, at least *every four years* in any case, in light of significant changes in the security environment or in the system of defence management.

Constitutional regulation of the special legal order

The main source of Hungarian law, i.e. our cartel constitution, has only included regulations on the special legal order (also known as the extraordinary legal order, emergency situation, qualified period) since the change of regime in 1989, as the previous system, which could not be considered to have operated under the rule of law, considered it unnecessary to regulate this issue.[18] The constitutional arrangements following the transition to the rule of law regulated the relevant provisions in a scattered manner, largely in relation to state bodies.

The new constitution, Hungary's Fundamental Law, which entered into force in 2012, now has a single, separate chapter dedicated to the rules for the special legal order. While it previously listed a total of six types of cases (state of national crisis, state of emergency, state of danger, terrorist emergency, pre-emptive state of defence and unexpected attack), the ninth and tenth amendments to the Fundamental Law in effect since 1 November 2022 have restructured the rules and reduced the number of cases to three (state of war, state of emergency and state of danger). The main new elements of the current legislation are presented below.[19]

1. *A state of war* may be declared in the following cases:
   – in the event of a declaration of war or threat of war
   – an external armed attack, an act having equivalent effect to an external armed attack and the imminent threat thereof
   – in the case of a covenant to provide collective defence

In effect, therefore, under the term "state of war", Parliament has essentially merged the previous scope of a state of national crisis, a pre-emptive state of defence and unexpected attack (and, in some cases, terrorist emergency). What has not changed is that the declaration of a state of war requires the agreement of two-thirds of all Members of Parliament.[20] A significant modification, however, is that unlike the previous legislation, which provided for the establishment and operation of a so-called *Defence Council* during a state

[18] See e.g. Hoffman–Kádár 2021: 16–17.

[19] The rules of the special legal order to be presented here are contained in Articles 48–56 of the Fundamental Law. It should be noted here that international perspectives on the subject have recently been published in large volumes of studies. See, among others, Nagy–Horváth 2021; Nagy–Horváth 2022; Kelemen et al. 2023: 44–94.

[20] The question of what legal form the "declaration" should take and, in light of this, whether it should be subject to review by the Constitutional Court, is a very interesting one. See Csink 2023: 6–10.

of national crisis (although, fortunately, this was never needed), the current legislation now only gives the Government the power to act, if necessary. According to Hungary's Fundamental Law, during a state of war, the Government exercises the rights delegated to it by Parliament and decides on the deployment of the Hungarian Defence Forces abroad or domestically, on their participation in peacekeeping, on their humanitarian activities in foreign theatres of operations, on their stationing abroad, and on the deployment of foreign armed forces within Hungary or from the territory of Hungary as well as their stationing in Hungary.

2. A *state of emergency* may be declared in the following cases:

– in the case of an act intended to overthrow or subvert the constitutional order or to acquire exclusive power

– in the event of a serious unlawful act that massively endangers the safety of life and property

The rules on the constituent elements of the state of emergency have changed little. A new element is the possibility of so-called "subversive" activities,[21] and the fact that serious acts for the purposes of both categories cannot only be committed by armed persons anymore (the adjective "violent" has been removed from the second category and replaced by "unlawful"). In this way, the constitutional authority has responded to the fact that such offensive conduct can also be carried out in cyberspace, by means of information technology.

The rule that the declaration of a state of emergency requires the agreement of two-thirds of all MPs has not changed. The timeline is also unchanged, except that a state of emergency may be declared for a period of thirty days, which may, however, be extended by a further period of thirty days by a vote of two-thirds of all MPs if the circumstances necessitating the declaration of a state of emergency still exist.

A major amendment, however, is that the President of the Republic no longer has the power to issue decrees in the event of a state of emergency, and the Constitution does not address whether the Hungarian Defence Forces may be used during a state of emergency.

3. There has been a significant change in the reasons for declaring *a state of danger.* Under the current constitutional rules, the Government may declare a state of danger in the event of armed conflict, war or humanitarian disaster in a neighbouring country, or in the event of a serious incident threatening the safety of life and property, in particular a natural disaster or industrial accident, or in order to avert the consequences thereof. Firstly, the reference to the situation in a neighbouring state was not previously included in the Fundamental Law (this changed on 25 May 2022, in view of the escalation of the Russian–Ukrainian conflict), and secondly, the reference to a natural disaster or industrial

[21] The definition of this is not yet known, nor is it defined in the explanatory memorandum of the amendment to the Fundamental Law. See Jakab–Till 2021: 474–475. The new state of emergency legislation may also include some of the elements of the former terrorist emergency. See in this context a detailed analysis of the previous and the new legislation: Horváth 2021b: 133–135.

disaster is not merely exemplary but is regulated as a concrete possible reason for proclamation.[22]

By comparing the expanded cases of the state of danger with the state of war and the national defence crisis (quasi-special legal order),[23] it can be concluded that "danger" appears in all three legal orders. The question arises whether an armed conflict or war in a neighbouring country can justify the introduction of a special or quasi-special legal order in Hungary. It may do so because, on the one hand, a war in a neighbouring country may entail the risk of further spread, and on the other hand, the large number of refugees may place a heavy burden on immigration enforcement agencies, social welfare systems, etc. The demarcation between the two special legal orders can also be seen in the fact that the Fundamental Law uses "imminent danger" in the case of a state of war, which means a qualified "danger". The question also arises as to why it was necessary to broaden the cases of state of danger, as this concept overlaps significantly with that of national defence crisis, although the latter is a peacetime condition for crisis management, not a matter for consideration of a special legal order. Consequently, if there is an "imminent danger" that an armed conflict or war in a neighbouring country will extend to Hungary, then a state of war should be declared, but in our opinion, if the "danger" is not imminent, then it is sufficient to declare a national defence crisis.

An important new guarantee rule is that a state of danger can be declared *for thirty days* but this can be extended by Parliament if the circumstances that led to the declaration persist. The authorisation requires the affirmative vote of two-thirds of the MPs present, not all of them. In contrast to the "original" thirty-day time limit, the extension could in theory last indefinitely subject, of course, to the constitutional rule that the body authorised to declare a special legal order *shall terminate it when the conditions for its proclamation no longer exist.* In reality, however, the extension is prevented by Article 82/A of Act XCIII of 2021 on the Coordination of Defence and Security Activities, which sets the *maximum duration to be 180 days*.[24]

4. Among the *common rules* concerning certain cases of the special legal order, the previous provisions of the Fundamental Law have not changed significantly (e.g. the scope of fundamental rights[25] that may be restricted in relation to the so-called "constitutional minimum", the prohibition of the dissolution of Parliament during a state of war or state of emergency, the powers of the President of the Republic to substitute Parliament, the

[22] In the context of the previous constitutional legislation, the question of whether a pandemic can be equated with a "major disaster" has been the subject of debate in both public and academic circles. See e.g. Szente 2020: 131–133; for a very detailed analysis see Horváth 2021a: 156–159. In relation to the constitutional rules and the regulation of the Disaster Management Act, see also Klein 2020: 220–222; Jakab–Till 2021: 464–465. On the previous legislation of the Fundamental Law see Till 2019.

[23] According to Paragraph (1) of Article 107 of Act CXL of 2021 on Defence and the Hungarian Defence Forces, a national defence crisis may be declared in view of the effects of a crisis in a state neighbouring Hungary, which requires military management and directly threatens Hungary's security in the event of an external armed attack or a threat of an external armed attack equivalent in its effect to an external armed attack, or in order to prepare for the fulfilment of military obligations in connection with NATO and EU membership.

[24] Since May 2022, a state of danger has been maintained with reference to the Russian–Ukrainian conflict. At the time of writing, the Parliament had already adopted a new authorisation allowing the extension of the state of danger until 23 May 2024.

[25] See in this context Sabjanics 2022: 8–9.

automatic expiry of decrees issued during the special legal order when the special legal order ceases to exist, and so forth). Something that may be considered a radical change is that during all three cases of a special legal order, *the Government* has substantive rights and obligations to act, in particular the possibility to issue decrees with the force of law. Thus, as indicated above, the opportunities for issuing decrees that did not exist under the previous constitutional rules during the "normal" legal order (as regards the Defence Council and the President of the Republic), which were (in theory) possible during the state of emergency and extraordinary circumstances, have been removed.

This designation of the Government as a centre of power with broad powers is also accompanied by *increased responsibility* as a guarantee in the Fundamental Law. Among other things, the Government is obliged to take all measures to ensure the continued functioning of Parliament and the Constitutional Court in times of special legal order. During the period of special legal order, the Government is obliged to inform the President of the Republic, the Speaker of Parliament and the Parliamentary Standing Committee, endowed with the relevant powers and responsibilities of Parliament, of the decree issued under the rules governing the special legal order. Furthermore, a special new rule is that *the Parliament may repeal a decree* issued by the Government under the rules governing the special legal order during the special legal order. A repealed decree may not be reissued by the Government with the same content unless justified by a significant change in circumstances, in which case the Government must keep the abovementioned bodies informed.

Act on the Coordination of Defence and Security Activities

One of the most important legislative acts of the 2018–2022 parliamentary term is *Act XCIII of 2021 on the Coordination of Defence and Security Activities* (hereinafter: AoCDSA).[26] The Act is based on the National Security Strategy and includes a number of provisions that previously appeared in the laws on defence (sometimes partially in other laws, e.g. on disaster management).

1. The *explanatory memorandum* to the proposed law highlights that since 2013, the security environment in Europe has changed dynamically. The Arab Spring, the massive wave of illegal migration, the conflicts in Ukraine and the hybrid events that preceded them, the terrorist attacks in Europe and the development of cybercrime opportunities resulting from the evolution of information technology, among others, have marked an epochal change, but the successive threats in our region have led the legislator to react on a case-by-case basis, in parallel with the management of specific crises. The altered security environment has made it necessary to *step up cooperation between armed bodies and organisations,* on the one hand, and to strengthen the capacity for preparedness and response for defence and security purposes in non-armed activities, on the other.

[26] For a brief and overarching presentation of the law see e.g. Kádár 2022: 8–10. An extensive analysis of the historical antecedents of the Act and of the Ninth Amendment to the Fundamental Law is provided in Farkas–Kelemen 2022: 4–40. The law is presented in detail, chapter by chapter in Kádár 2023: Chapters III–XV.

Through the new law, the legislator has complemented the sectoral operation of the previous law with a framework for effective cooperation replacing the sectoral delimitation and the *holistic coordination of the government*, making it a priority area to strengthen the preparedness and security awareness of society, as well as to make the standard legal crisis management and the special legal order regulation more effective. The Ninth and Tenth Amendments to the Fundamental Law and the AoCDSA have laid the foundations for the reform of defence and security upon which the coordinated development of the various sectors, in light of the foreseeable changes in technology and the security environment, can be built in the coming years.

To this end, the Act draws on the country's historical background, the regulatory and crisis management experience of recent years, the increasingly comprehensive approach to national security in the transatlantic region, NATO's efforts to develop national resilience, and the academic analyses of these issues both in Hungary and abroad. The aim of the Act is therefore to establish and consolidate a *comprehensive approach* to the protection of Hungary and the security of the nation through leaving sectoral specificities intact and maintaining the system of sectoral governance, but enhancing the coordination of crisis management operations, modernising crisis management regulations and improving the preparedness and security awareness of non-state actors. The explanatory memorandum also states that the ability to adapt rapidly to circumstances that often change over a short period of time is a prerequisite for effective crisis management. With this in mind, the drafting of the AoCDSA has also placed due emphasis on securing the conditions necessary for adaptiveness at both individual and societal levels.

2. The Act declares, as a matter of principle, that the defence and security of Hungary is a *national matter* upon which the survival and development of the nation and the enforcement of community and individual rights are based. Therefore, the legal provisions relating to the maintenance and development of the defence and security of the Hungarian nation shall be determined in light of this Act. As such, it makes it clear that the AoCDSA should be regarded as a type of "framework" law whenever the legislator adopts new legislation on defence and security issues (this is reflected, *inter alia*, in the Defence Act currently in force).

According to the law, the unified management of the above and the promotion of a modern security concept in this context, as well as the coordination of the operation and utilisation of the organisations, capabilities and resources involved in this, *are tasks for the State*. The three pillars of the enforcement of the stated requirements and, where necessary, of the armed defence of Hungary are as follows:

- the defence system and the Hungarian Defence Forces
- law enforcement and law enforcement agencies (the police, the National Tax and Customs Administration, the penitentiary system and the professional disaster management agency)
- the national security services[27]

[27] There are currently one military (the Military National Security Service) and four civilian national security services operating in Hungary. The civilian services are: the Office for the Protection of the Constitution, the Information Office, the National Security Service and the National Information Centre.

All (civil) public authorities[28] are obliged to cooperate with these bodies in order to meet the above requirements which are of a principled nature.

The law devotes a separate sub-chapter to the "Principles". In this context, the emphasis should be placed on the priority of *Community-wide security,* the requirement for *coordinated action* and the *proportionality of any restriction of rights.*

3. In recent decades, a common regulatory subject of defence laws has been the discussion of the so-called system of *basic defence obligations.* The general regulation of these has been taken over by the AoCDSA. It is important to point out that the relevant regulatory system has multiple levels: the Constitution provides the basis,[29] while certain detailed provisions remain regulated by the Defence Act. The obligations of defence and security are as follows:

- military service, armed or unarmed (during a state of war)
- civil defence obligations
- compulsory national defence work (during a state of war)
- economic and material service obligations
- the obligation to notify for defence and security purposes

It is worth emphasising that under the Fundamental Law:

- military service is compulsory only for *men of Hungarian nationality who are of age and reside in Hungary*
- the obligation to work in the field of national defence and the civil defence obligation *applies only to Hungarian citizens of full age resident in Hungary* (including women), while
- economic and material service obligations apply to *everyone* (not just individuals but also organisations)

However, the AoCDSA also stipulates that *only one of the obligations* of military service, civil defence and national defence may be imposed on one natural person within one period. Another rule of guarantee which bears significance is that administrative decisions and measures relating to the fulfilment of the obligations of defence and security under the Act may be challenged by means of an *administrative* appeal or *administrative lawsuit.*

Three of the defence and security obligations are regulated in detail in the Act, as the other two (obligations that may be imposed during a state of war) are regulated in detail in the Defence Act. The obligations are briefly described here.

a) The objectives of the civil defence obligation in times of armed conflict and disaster:

– the protection of human life
– the protection of material goods necessary for human subsistence

[28] According to the interpretative provision of the AoCDSA, the term "administrative body" is to be understood only to mean state administrative bodies under the control of the Government (i.e. excluding certain bodies with autonomous legal status and local self-governments, which are excluded from the control of the Government).

[29] Paragraph (3) of Article XXXI of the Fundamental Law deals with military service, (4) deals with the obligation to perform national defence services, (5) deals with civil defence service and (6) deals with economic and material service.

- promoting the preservation of material security
- performance of humanitarian tasks

The sub-obligations of the civil defence obligation are the obligation to provide information, the obligation to report, the obligation to participate and the obligation to provide service. The *mayor* usually acts in matters relating to these obligations.

b) The *purpose of the economic and material service obligation* is to provide the material and service conditions for the performance of tasks directly related to the defence and security of the country, as defined by law, from non-state sources if they cannot be provided in any other way. As indicated above, this service obligation may be imposed not only on natural persons but also on organisations (primarily companies).

This obligation can be very broad. It may involve, for example, the temporary transfer of immovable or movable property, the creation of reserves and stocks, the suspension of exports of foreign currency or precious metals, the restructuring of a production plant, the provision of data, and so forth.

The decision to use this service is made by the "claiming authority". This authority may be the Government or a Minister, the chairman of the regional defence committee, the mayor, the head of the sectoral administration responsible for defence and security administration, or, in the event of war, the commander of the military organisation. If the person or body concerned suffers a financial loss as a result of the performance of the service, he or she may, as a general rule, be *compensated for* that loss.

c) The essence of the *duty to report for defence and security purposes* is that, in the event of certain acts or circumstances occurring which are specified by law, the person who becomes aware of them is obliged to report them to the specified bodies. These include, for example, acts likely to cause serious and violent disturbance to public order or public security, as well as imminent threats thereto, and disasters. Notification can be made to a number of bodies, including the police, defence organisations, disaster prevention services, metropolitan and county government offices and local self-government offices.

4. The AoCDSA also covers a number of other topics, including planning for defence and security, preparation and mobilisation of the national economy for defence, the system of national resilience, the alert system for defence and security, the verification and control of obligations, the so-called coordinated defence action, and the rules for national participation in NATO and EU crisis management systems. These will not be described in detail here, but the specificities of the *defence and security management system* will be discussed. In recent decades, the rules relating to this were also laid down in the Defence Acts.

The AoCDSA emphasises the role of the Parliament, the President of the Republic, the Government and the ministers responsible for the management of certain public administration sectors, as well as the role of defence and security organisations in the top-level management of defence and security activities. Simultaneously, a large number of other state organisations are involved in the performance of defence and security tasks (e.g. state administration bodies under the control of the Government, local self-governments, courts and prosecutors' offices, healthcare-related, educational, cultural and scientific institutions, the national news agency, transport, communications and information technology bodies, the state post office, the Hungarian National Bank, utility service providers, and so forth).

In a narrower sense, the law deals with *the organisation of the defence and security management system.* The purpose of the system of defence and security management can be summarised as follows:

- coordinating the activities and development of all bodies and organisations involved in maintaining and developing the defence and security of the country and the nation
- providing governmental direction to the bodies involved in the preparation for coordinated defence action
- the transmission of government guidance to the bodies involved in preparing for the operation of the special legal order
- preparing for and coordinating the exercise of cross-sectoral responsibilities
- the professional management of cross-sectoral activities, as defined by law
- carrying out checks related to defence and security activities and the preparations for them

It is observable that the law attaches particular importance to *coordination tasks.*

The organisational system is organised into three levels: *the central, the regional* and *the local bodies* of defence and security administration. The central body is designated by decree by the Government and is currently the *Defence Administrative Office.*[30] The Office is a central administration, under the authority of a Minister and headed by a Director-General. The regional and local bodies are known as Regional and *Local Defence Committees.* In contrast to the central body, which was created in 2022, the system of defence committees already existed in previous decades. In these special administrative bodies, which have a specific legal status, there is both civilian representation (within the regional state administration and local self-government administration) and military and law enforcement administration. In addition to their coordinative role, the Regional Defence Committees have the power to order the use of certain services, to order the evacuation of the population in certain urgent cases and to deploy civil protection organisations. The Local Defence Committees are also primarily coordinative bodies, but may also take measures in certain cases, for example, to redeploy and mobilise the personnel and equipment needed for protection. It is also worth mentioning that the law specifically assigns a number of tasks to *mayors* in this regard.

5. Regarding the Hungarian administrative system for sanctions, it is worth mentioning that the AoCDSA considers the breach of certain obligations defined in the Act *a breach of the rules,* which entails administrative authority proceedings to be conducted by the governmental authority. The government agency may impose *protection and security fines* in the event of a finding of noncompliance.

6. Finally, in connection with the Act, we would like to convey the fact that the *preparation* for special legal orders, which were also regulated in the Defence Acts, and the *operation* and the range of *extraordinary measures* that may be introduced during these periods, are also regulated in the AoCDSA. In this area, the law basically regulates in general terms the measures which the Government may introduce by decree, including

[30] See Government Decree 337/2022 (IX. 7.) on the Defence Administrative Office.

the framework for the restriction of fundamental rights. In the latter context, it is worth mentioning that the restriction of rights is only possible for a specific purpose, subject to the requirements of necessity and proportionality.

In case of government decrees issued in the context of a special legal order, *publication in the Official Gazette* is not obligatory for operational reasons. On the day of signature, these decrees may be published free of charge on the news programmes of so-called linear broadcasters, in daily newspapers, on Internet news portals and even by means of a notice. If for any reason this should be impeded, the law provides that the publication must be carried out as extensively as possible using the technical means of law enforcement agencies and the armed forces.

The Defence Act

When considering the 2018–2022 parliamentary term, we also need to touch upon *Act CXL of 2021 on Defence and the Hungarian Defence Forces* (The Defence Act), which concerns the system of rules related to the development of the defence and security system established in relation to the new approach. This Act, in addition to the two strategies described above, also draws from and adapts to the rules of the AoCDSA. For the purposes of this study, we will restrict ourselves to a brief presentation of the rules of the Act, primarily those of a management, administration and organisational nature.

1. The explanatory memorandum to the proposal of the Defence Act highlights that the new Act revises the sustainable elements of the previous Defence Act adopted in 2011 by adapting them to the expectations and requirements of the times, and, bearing in mind the Ninth Amendment to the Fundamental Law, clarifies the special legal order rules, defining certain former special legal order tasks as peacetime tasks. As a result of the changed security policy environment, new rules are introduced particularly in the section concerning the tasks of the Defence Forces, which share the requirement that decisions must be made in a timely manner. The compulsion to comply with the requirement to react in a timely manner is a recurrent feature of the new rules of the Act, with repercussions that affect the regulation of the powers of management. In view of the above, the new law aims to *reform the institutional system for National Defence as a whole* in line with the defence and security institutional system's reform.

2. As in the case of previous laws on defence, the Defence Act states that defence is *a national matter.* According to the Act, Hungary relies on its own strength, including the resources of its national economy, the preparedness and determination of the Hungarian Defence Forces, the cooperation of law enforcement agencies, national security services and other bodies, the patriotic commitment and sacrifice of its citizens in defence of the homeland, and the cooperation and assistance of the allied states and their armed forces in maintaining and developing its defence and allied military capabilities.

3. In the field of *defence management*, the Act, similarly to previous defence Acts, names the Parliament, the President of the Republic, the Government and its members (in particular the Minister responsible for defence), and other bodies involved. It is important

to underline that the activities of the Chief of the General Staff, who is in charge of the Defence Forces, are directed by the Minister responsible for defence.[31]

4. As we have already pointed out, the provisions referred to in previous legislation as *national defence obligations* have been split into two. Some of them have been included in the AoCDSA as obligations of defence and security. However, the Defence Act retains the name "national defence obligations" and regulates the *military obligation* as the first of these.

The military service obligation during a state of war consists of the constitutional (armed or unarmed) military service obligation alongside additional obligations (reporting, providing information and participation). The purpose of *armed military service* is to carry out national defence and allied military tasks and, to this end, to train and prepare conscripts for military tasks and to strengthen the defence capabilities of the Defence Forces. The purpose of *unarmed military service* is to participate in and provide the necessary training for the unarmed tasks of the Defence Forces without the use of weapons and to ensure and support the armed tasks of the Defence Forces. An application for unarmed military service may be submitted to the head of the military administration and central data-processing body of the armed forces. As in previous decades, the exemption from military service is governed by the institution of the so-called "waiver". The persons designated by the body involved in managing the waivers are entered on the waiver register and may not be summoned by the military administration for a place of service outside of their employment duties.

The national defence work obligation is also a form of national defence obligation. Under the Act, the person liable is required to perform physical or mental work in the workplace assigned to him or her, in accordance with his or her abilities and state of health, in the context of a permanent or temporary national defence work obligation, in order to maintain and restore the functioning of the country.

5. It is worth mentioning that, as does the AoCDSA, the Defence Act allows the Government Office, within the framework of an official procedure, to impose a so-called *national defence fine* in the case of a violation of certain obligations listed above.

6. The law also defines the legal status of the Hungarian Defence Forces, also on the basis of a "model" in place for several decades now. The Hungarian Defence Forces are an *armed force* under *civilian control*, operating under a system of dependency, based on volunteerism in times of peace and on volunteerism and general military duty in times of war, and are organised by the Defence General Staff and the Defence organisations under its subordination. Some defence organisations also perform military administrative functions as defined by law. The Defence Forces perform their functions with or without the right to use arms, within the scope defined by law.[32]

The *Defence General Staff* is the leading body responsible for the planning, organisation and military activities of the Defence Forces at the highest level. This body is headed by

[31] Pursuant to Paragraph (1) of Article 112 of Government Decree 182/2022 (V. 24.) on the Duties and Powers of the Members of the Government, this is the *Minister of Defence*, at the time of writing.

[32] For a detailed analysis of the "cooperative" type of tasks of the Defence Forces see Till 2023: 4–14.

the Chief of the General Staff[33] and, with certain exceptions, directs the Defence Forces organisations. Otherwise, the defence organisations are headed by *commanders*.

The military administration is a two-tier organisation: it comprises a central military administration as well as regional military administrations. The central body is the military administrative and central data processing body of the Defence Forces;[34] the regional bodies are the military supplementary and recruiting centres and offices.[35]

In addition to the military (and other personnel), the Defence Forces also have *reserve personnel*. Maintaining the *voluntary reserve system* is an obligation under the Fundamental Law. The reserve personnel include voluntary reservists, defence personnel who volunteer for military service during the period of compulsory military service, trained conscripts and untrained conscripts.

The law specifically mentions the *military police* when detailing "certain security measures". The purpose of the military police is to maintain military order and discipline and to provide police security for the activities of defence organisations, as well as to perform the law enforcement tasks specified in the law. The law provides the military police with special powers, which are very similar to those of professional police officers. Also in a similar way, appeals *(complaints)* can be made against an action taken by a military policeman, which is decided by the Chief of the General Staff in an administrative procedure.[36]

The most serious use of force available to the military is the use of firearms. The law regulates in detail the possible cases, conditions and methods of using firearms (similarly to the use of firearms by members of law enforcement agencies). However, other less severe uses of force (e.g. physical force, truncheons, tear gas canisters, tasers, or handcuffs) may also be used. Complaints may also be lodged with the Chief of the General Staff regarding the use of force by the military. Civilian persons may also request that their complaint be examined by the Commissioner for Fundamental Rights in the first instance if the use of force infringes their fundamental rights.

7. Finally, it should be noted that, in certain cases where there is a situation affecting national defence and threatening the security of the country, but no special legal order is promulgated, the Government is empowered to introduce special measures. In such cases, the Government may declare a *state of national defence emergency*. In the absence of such a decision, immediate government measures must also be taken to avert an *unexpected attack* on the country. These regulatory elements also have a longstanding history.[37]

[33] Former name: Commander of the Hungarian Defence Forces.

[34] At the time of writing, according to Article 17 of Government Decree 614/2022 (XII. 29.) on the implementation of certain provisions of the Defence Act, this body is the Military Administration and Central Registry of the Hungarian Defence Forces.

[35] According to Articles 18–19 of the above Decree, there are seven military training and recruitment centres and twenty military training and recruitment offices covering the country's territory. In addition, *recruiting points* may also operate to support the tasks of these bodies.

[36] On the role and importance of the military police see e.g. Buzás 2019: 36–48.

[37] In the 2011 Defence Act, it was still possible to declare a "state of national defence emergency". For an analysis see Kádár–Hoffman 2021: 6–7. In the context of the regulations on crisis management within national defence see Puskás 2023: 8–9.

Summary and conclusions

The objectives of the renewed legal environment presented in the study are clear: the legislator seeks to provide a well-founded and clear response to the new types of security challenges.[38] The plans for the convergence of military and law enforcement activities and the potential exploitation of synergies are primarily reflected in the new system of defence and security regulation, but it is too early to assess them as of yet.[39] However, it is to be hoped that the new type of security and defence system will not have to be applied in a real situation, especially in the event of an armed attack. However, the global processes, conflicts and crises outlined in the introduction, and the situations described in the outlined strategies, which are increasingly impacting our world today, do not bode well, even for the near future.[40] As the saying goes: "It is better to be safe than sorry." However, we could also quote the Roman proverb: "Si vis pacem, para bellum."[41] Whereas until the war in Yugoslavia, wars in Europe were only to be found in the pages of textbooks or news reports from distant countries, today they are a nearby reality. Although our NATO and EU membership represent major security potential, a well-prepared and capable military and internal security organisation is also essential for the defence of sovereignty and statehood. The NATO framework and the defence of every single European country work on the basis of a multinational framework. This framework creates the necessary elements to defend any parts of NATO, and a capable Hungarian military is important primarily because it is also one (but of course significant) element of the puzzle of our common defence structure. In other words: strong national contribution helps defend sovereignty, not by actual military force, but as a tool of national interest assertion.

References

Buzás, Gábor (2019): Rendészet – katonai rendészet. *Katonai Jogi és Hadijogi Szemle*, 7(2), 25–50. Online: https://epa.oszk.hu/02500/02511/00009/pdf/EPA02511_katonai_jogi_szemle_2018_2_025-050.pdf

Csink, Lóránt (2023): A különleges jogrend bevezetésének alkotmányjogi megközelítése. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, (3), 4–13.

[38] Of course, the new laws are now accompanied by a significant number of implementing regulations. It is not within the scope of this study to describe them.

[39] However, we refer to the thoughts of Géza Finszter, who in our opinion convincingly demonstrates that confusing the use of *physical violence* with the use of military and police force (e.g. in terms of the firepower of the weapons used, the prioritisation or marginalisation of the safety of life and property, the treatment of hostile aggressors) can have serious consequences. See Finszter 2018: 29–33; see also Hautzinger 2023: 16–17.

[40] This pessimistic tone is supported, among other things, by the study which describes and analyses the current mass of challenges, risks and threats that significantly influence the future in almost 50 pages: Juhász–Petruska 2022: 4–46.

[41] As underlined by Pál Kádár: crisis management and special legal order operations should be prepared in the greatest possible depth and thoroughness *during a crisis-free period.* See Kádár 2022: 16.

Farkas, Ádám – Kelemen, Roland (2022): Az Alaptörvény kilencedik módosítása, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény megalkotásának történelmi előzményei. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* (37), 4–40. Online: http://hdl.handle.net/20.500.12944/21563

Farkas, Ádám – Till, Szabolcs Péter (2022): A honvédelem közjogi szabályozásának megújítását indokló körülmények áttekintése. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* (26), 4–37.

Finszter, Géza (2018): *Rendészettan.* Budapest: Dialóg Campus.

Hautzinger, Zoltán (2023): A rendészet védelmi és biztonsági funkciói. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* (10), 4–17.

Hoffman, István – Kádár, Pál (2021): A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai I. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* (2), 4–39.

Horváth, Attila (2021a): A 2020-as Covid-veszélyhelyzet alkotmányjogi szemmel. In Nagy, Zoltán – Horváth, Attila (eds.): *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest: Mádl Ferenc Institute, 149–173. Online: https://doi.org/10.47079/2021.nzha.kulon.4_6

Horváth, Attila (2021b): A különleges jogrend fejlődése Magyarországon a kilencedik Alaptörvény-módosítás tükrében. In Nagy, Zoltán – Horváth, Attila (eds.): *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest: Mádl Ferenc Institute, 122–148. Online: https://doi.org/10.47079/2021.nzha.kulon.4_5

Jakab, András – Till, Szabolcs (2021): A különleges jogrend. In Trócsányi, László – Schanda, Balázs – Csink, Lóránt (eds): *Bevezetés az alkotmányjogba* (8. kiadás). Budapest: HVG–ORAC, 437–484.

Jakab, András (2007): *A magyar jogrendszer szerkezete.* Budapest–Pécs: Dialóg Campus.

Jakab, András (2016): A jogforrási rendszer. In Trócsányi, László – Schanda, Balázs (eds.): *Bevezetés az alkotmányjogba* (5. kiadás). Budapest: HVG–ORAC, 121–179.

Juhász, István – Petruska, Ferenc (2022): A védelmi-biztonsági szabályozási reformot indukáló biztonsági környezet-változás elemeinek beazonosítása, szakmai értékelése. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* (32), 4–46.

Kádár, Pál (2022): Gondolatok a védelmi-biztonsági szabályozás reformjának egyes kérdéseiről. *Honvédségi Szemle,* 150(1), 3–19. Online: https://doi.org/10.35926/HSZ.2022.1.1

Kádár, Pál ed. (2023): *A védelmi és biztonsági szabályozás magyarországi reformja.* Budapest: NKE Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely.

Kádár, Pál – Hoffman, István (2021): A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai: a „kvázi különleges jogrendek" helye és szerepe a magyar közigazgatásban. *Közjogi Szemle,* 14(3), 1–11.

Kelemen, Roland – Petruska, Ferenc – Spitzer, Jenő – Vikman, László (2023): Nemzetközi minták vizsgálata az összehangolt válságkezelésre, az arra való felkészülésre és a különleges jogrendi szabályozásra. In Kádár, Pál (ed.): *A védelmi és biztonsági szabályozás magyarországi reformja.* Budapest: NKE Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, 44–94. Online: http://hdl.handle.net/20.500.12944/21560

KLEIN, Tamás (2020): A veszélyhelyzeti jogalkotás alkotmányos alapjai, különös tekintettel a véleménynyilvánítás különleges jogrendi korlátozhatóságára. *Glossa Iuridica*, 7(különszám), 211–234.

KSH (2024): *Gyorstájékoztató.* Hungarian Central Statistical Office. Online: www.ksh.hu/gyorstajekoztatok/nep/nep2406.html

NAGY, Zoltán – HORVÁTH, Attila eds. (2021): *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest: Mádl Ferenc Institute. Online: https://doi.org/10.47079/2021.nzha.kulon.4

NAGY, Zoltán – HORVÁTH, Attila eds. (2022): *Emergency Powers in Central and Eastern Europe.* Budapest–Miskolc: Mádl Ferenc Institute. Online: https://doi.org/10.47079/2022.znah.epicaee.1

PÜNKÖSTY, András (2023): A közös kül- és biztonságpolitika. In SZABÓ, Marcel – GYENEY, Laura – LÁNCOS, Petra Lea – PÜNKÖSTY, András (eds.): *Az Európai Unió jogának alapjai.* Budapest: Pázmány Press, 431–448.

PUSKÁS, Anna (2023): Az új honvédelmi törvény és a védelmi és biztonsági szabályozás reformjának összefüggései. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, (7), 4–14.

VARGA, Júlia (2024): *A közoktatás indikátorrendszere 2023.* HUN–REN Közgazdaság- és Regionális Tudományi Kutatóközpont. Online: https://kti.krtk.hu/wp-content/uploads/2024/05/Indikatorkotet_2023.pdf

SABJANICS, István (2022): Az Alaptörvény kilencedik módosításának államigazgatási vonatkozásai a különleges jogrendet illetően. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, (9), 4–14.

SÁNTHA, György (2023): *A menedzselt állam.* Budapest: Pázmány Press.

SULYOK, Gábor (2002): Az egyéni vagy kollektív önvédelem joga az Észak-atlanti Szerződés 5. cikkének tükrében. *Állam- és Jogtudomány*, 43(1–2), 99–136. Online: https://szakcikkadatbazis.hu/doc/4067451

SZENTE, Zoltán (2020): A 2020. március 11-én kihirdetett veszélyhelyzet alkotmányossági problémái. *Állam- és Jogtudomány*, 61(3), 115–139.

TILL, Szabolcs (2019): A különleges jogrend. In JAKAB, András – FEKETE, Balázs (eds.): *Internetes Jogtudományi Enciklopédia.* Online: https://ijoten.hu/szocikk/kulonleges-jogrend

TILL, Szabolcs Péter (2023): A Magyar Honvédség feladatrendszerének újraszabályozása az új honvédelmi törvény tükrében, *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, (6), 4–14.

10.32565/aarms.2024.3.5

Institutionalised Tools for Addressing the Climate Crisis in Cape Coast, Ghana

Ama Kissiwah BOATENG[1]

The climate crisis presents significant challenges for many African cities, impacting their economies, ecosystems and the livelihoods of their inhabitants. This paper explores into the various tools and techniques that local government administrations are employing to adapt to these challenges. Using Cape Coast Metropolitan Assembly in Ghana as a case study, a combination of focus group discussions and informal interviews was held with key stakeholders. The findings revealed a multifaceted narrative of vulnerability and adaptation, highlighting the importance of education and capacity building in institutionalising effective climate governance. Ongoing engagement with stakeholders is also considered crucial for refining existing strategies and discovering innovative solutions that address the unique challenges posed by climate change in the region.The paper concludes that incorporating informal practices often deeply rooted in local culture can enhance formal policy initiatives. This integration fosters a more comprehensive and effective approach to climate governance at the sub-national level.

Keywords: *climate crisis, institutionalised tools, local government, Cape Coast, Ghana*

Introduction

The rapid urbanisation of Africa is one of the continent's most significant socio-economic transformations, evidenced by an annual growth rate of about 3.6% from 2005 to 2015.[2] This trend is projected to accelerate, with estimates suggesting that urbanisation levels may surpass 60% by 2050.[3] The African Development Bank emphasises that much of this growth is being driven by the expansion of small towns and intermediary cities, raising urgent concerns about urban climate resilience.[4]

As urban areas continue to grow and expand, they become more vulnerable to the unpredictable nature of climate variability and the increasing frequency of extreme weather events.[5] Over the past thirty years, extensive research and analyses have been

[1] PhD candidate, Ludovika University of Public Service.
[2] UN-Habitat 2020.
[3] UN DESA 2019.
[4] ADB 2016.
[5] IPCC 2023.

conducted, primarily focusing on climate adaptation policies and plans in well-established, larger developed cities.[6] For instance, Salvia et al. (2021) analysed 327 cities in the EU with a Climate Change Adaptation Plan, Reckien et al. (2018) analysed 885 across the EU28 and Otto et al. (2021) found that 104 of the largest cities in Germany have climate change mitigation plans.[7]

Over the last three decades, extensive research and analyses have been conducted, primarily focusing on climate adaptation policies and plans (CAPS) in well-established, larger developed cities. This body of work seeks to understand how cities are preparing for the impacts of climate change, and it emphasises the necessity for effective strategies to reduce vulnerability and enhance resilience. For instance, climate change mitigation plans of the 103 largest cities in Germany were examined, and it was essential to know that cities are not only reducing their carbon footprints but are also equipped to handle the immediate effects of climate variability.

Their research indicated a growing acknowledgement among urban decision-makers of the need for comprehensive strategies that not only address the mitigation of greenhouse gas emissions but also integrate resilience measures to prepare for climate-related risks. This dual approach is essential in ensuring that cities are not only reducing their carbon footprints but are also equipped to handle the immediate effects of climate variability.

However, there is a noticeable gap when it comes to the rapidly urbanising cities.[8] These cities, often characterised by their burgeoning populations, are facing unique challenges related to climate change that demand urgent attention.[9] The lack of comprehensive studies on these regions highlights the need for tailored climate adaptation plans that recognise the specific vulnerabilities and resource constraints these cities encounter.[10] As the world becomes more urbanised, the call for equitable solutions that account for the diverse realities of all cities, both developed and developing, becomes important.[11]

To this end, the notion of institutionalised tools and mechanisms is central to this paper. These tools can be framed as systematic actions undertaken by local governments to integrate climate governance into their urban management practices, extending beyond policy formulation.[12] Existing research has largely neglected how municipalities in developing countries can proactively adapt to climate challenges through the institutionalisation process.

Studies surrounding the institutionalisation of climate change emphasise the importance of incorporating climate adaptation strategies into routine decision-making within urban environments.[13] Ostrom's Institutional Analysis and Development (IAD) framework serves as a valuable lens for understanding this dynamic. The IAD framework aids actors in achieving their objectives in confronting societal problems, and it frames

[6] Araos et al. 2016.

[7] Otto et al. 2021.

[8] Fila et al. 2023.

[9] Birkmann 2016.

[10] Hoppe 2019.

[11] Fila et al. 2023.

[12] Olazabal et al. 2024.

[13] Patterson–Huitema 2019.

organisations as entities governed by a set of rules, constraints and patterns of interaction that define their structure.[14]

Despite the challenges local administrations face concerning urban climate change governance, there are opportunities to institutionalise existing tools and techniques that can reinforce climate adaptation efforts.[15] This paper offers a detailed exploration of Ghana's Cape CoastMetropolis, focusing on the tools and techniques successfully integrated into the local government system address the climate crisis. It presents a model that other urban areas facing similar challenges can follow.

Ghana, like many developing nations, deals with governance and socio-economic challenges that complicate its response to the climate crisis.[16] Despite over thirty years of climate change governance at the national level, there remains a lack of robust adaptation efforts at the local administration level.[17] This gap raises questions about how cities can integrate climate resilience into their governance frameworks.

Methodology

This research incorporated qualitative methods, particularly focus group discussions and informal interviews with various stakeholders, including local government officials, community leaders and residents in Cape Coast. This approach enabled a comprehensive understanding of local attitudes toward climate change adaptation and the tools being utilised.

Selection of the case study

This paper focuses on Cape Coast, a city exemplifying the challenges and vulnerabilities faced by rapidly urbanising municipalities in Ghana. Cape Coast is uniquely positioned as one of the most susceptible cities to climate change, attributed largely to its significant exposure to excessive flooding and coastal erosion. The Metropolis, steeped in historical significance, is characterised by a burgeoning population that reached an estimated 189,925 inhabitants according to Ghana's 2021 Population and Housing Census.[18]

Geographically, the city is located along the southern border of the Gulf of Guinea, benefiting from a tropical savanna climate that includes two extended wet seasons; the heavier rainfall period extends from March to July, while a lighter wet season occurs from September to November. Additionally, the climate features two shorter dry periods in January–February and August.

[14] Ostrom 2005; 2011.
[15] Valdivieso et al. 2017.
[16] Adu-Boateng 2015.
[17] Musah-Surugu et al. 2019.
[18] Institute for Health Metrics and Evaluation 2021.

Over the years, extensive human activities, including farming, charcoal production and bushfires, have significantly altered the region's original dense scrub vegetation, resulting in secondary vegetation that is less dense compared to the interior forest areas. The rapid urban expansion, spurred by the burgeoning population and associated socio-economic activities, poses further challenges to the local ecological balance.

Cape Coast's economy is dynamic and heavily reliant on fishing, trade, tourism and various hospitality-related ventures. However, this economic growth comes at a notable cost, as competition for land between agricultural use and housing development leads to substantial negative impacts on the natural environment. Alarmingly, the Ghana Statistical Service (GSS) reports a rapid depletion of the city's vegetation cover, exacerbating vulnerabilities related to climate change.

Inundation from increased flooding has severely damaged infrastructure and disrupted both residential and commercial enterprises, contributing to water pollution and exacerbating land erosion. Coastal communities serve as case studies of this threat, often experiencing destructive flooding leading to building collapses during heavy downpours.

Extreme weather conditions have adversely affected sectors such as agriculture and fisheries, leading to diminished marine ecosystems and fish supplies, and even the extinction of certain fish species. Collectively, these factors translate to critical management challenges that hinder the sustainable development of the municipality and the responsible use of its water resources.

Given this context, Cape Coast presents an insightful case study for examining local administrative responses to the climate crisis, particularly focusing on the institutional processes shaping climate adaptation strategies.

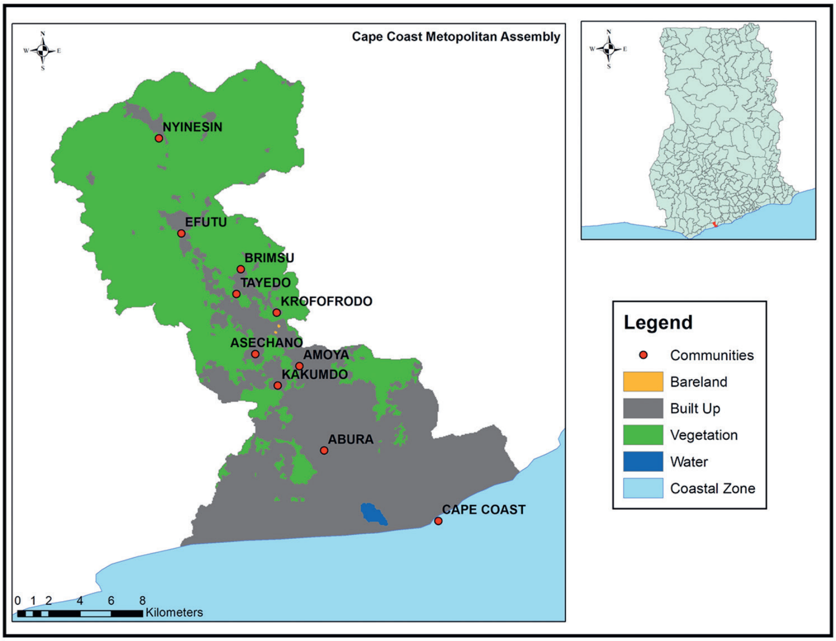

Figure 1: Location map of the study area

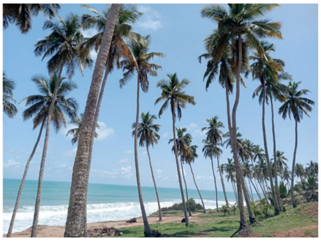

Figure 2: Palm trees are planted along the Cape Coast beach

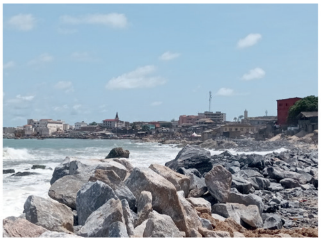

Figure 3: Construction of a sea defence wall to prevent coastal erosion

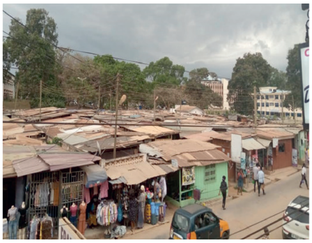

Figure 4: Growth of Informal Settlements in the Cape Coast Metropolis

Source: compiled by the author

Data collection and analysis

This research employed a case study approach to thoroughly understand the dynamics at play within Cape Coast. Key data were gathered through focus group discussions and informal conversations with stakeholders involved in urban development within the city. The objective was to gain insights into their perspectives regarding vulnerabilities to climate change, the effectiveness of ongoing adaptation efforts, and the tools and practices currently being utilised to institutionalise climate governance.

To facilitate a comprehensive dialogue, a stakeholder workshop was convened in May 2022, which attracted approximately twenty-seven participants from various governmental and non-governmental organisations actively engaged in climate action initiatives. The workshop served as a vital platform for discussing the climate vulnerabilities of the Metropolis, fostering collaborative discourse on the emerging instruments and mechanisms essential for advancing climate policy and governance within the locality.

These interactions provided critical insights into community knowledge, existing practices and potential areas for improvement. Informal interviews further enriched the data, contributing personal narratives and localised insights that highlighted the cultural dimensions of the climate response.

Before conducting the workshop, a meticulous stakeholder mapping exercise was performed to ensure an equitable representation of both governmental and non-governmental entities in the participation pool. An expert sampling technique guided the selection of stakeholders, focusing on their roles and responsibilities within their organisations. These strategic selection criteria emphasised the importance of knowledge depth, ensuring that at least two officials from each sampled organisation were included to facilitate robust discussions.

During the workshop, participants were divided into five diverse teams, allowing for a balance of expertise and perspectives. Each group addressed key issues relevant to the overarching subject of climate governance, which encouraged a more nuanced debate surrounding the core challenges. Additionally, informal conversations with various officials were conducted post-workshop to complement the insights gathered during the event, elucidating how different governance mechanisms operate in practice.

Results

The analysis identified some tools institutionalised by Cape Coast's local government to address the climate crisis.

Medium-term development plans

The absence of a robust local-level climate policy or action plan in the Cape Coast Metropolian Assembly hinders effective adaptation and mitigation efforts and risks exacerbating existing vulnerabilities. Studies have indicated that the overwhelming focus on national interests often neglects local adaptations for fostering climate resilience. The integration of climate change adaptation into the operations of the Cape Coast Metropolitan Assembly is increasingly recognised as essential, particularly in the absence of explicit local climate policies.

In this regard, the focus group discussions highlighted that the formulation of a medium-term development plan is a key strategy in this context. These plans serve not only as a guide for local governments but also align with broader national priorities and regulatory frameworks established by the National Development Planning Commission (NDPC). In Ghana, local governments are mandated to create and submit these medium-term development strategies, which must explicitly consider the need for resilience against potential climate-related risks and challenges. This requirement emphasises the proactive role that local authorities play in ensuring that their development frameworks are robust enough to withstand the impacts of climate change, such as extreme weather events, rising sea levels and other environmental stresses.

The informal interviews conducted with various stakeholders also revealed that the medium-term development plan offers a vital opportunity to frame local priorities and needs accurately. This is particularly important as some national policy directives may not fully address the unique circumstances and challenges faced by specific local jurisdictions. By adopting a tailored approach, local authorities can better respond to the pressing climate issues that impact their communities, ensuring that the measures implemented are relevant and effective.

The identification of these priorities reflects a comprehensive understanding of the specific climate challenges faced by local jurisdictions. By addressing these concerns, medium-term development plans can significantly contribute to both environmental sustainability and socio-economic development. Ultimately, this holistic approach not only enhances the resilience of communities but also improves the overall quality of life for residents through increased economic opportunities and improved environmental conditions.

Environmental impact assessments

Environmental permitting is a critical tool for managing climate change impacts in urban settings. This mechanism allows local governments to systematically evaluate the potential environmental impacts of proposed development projects before they are approved. By implementing Environmental Impact Assessments (EIAs), authorities are provided with a structured approach to identify, assess and mitigate negative environmental effects, ensuring that urban development aligns with sustainability objectives. The Ghana Environmental Protection Agency (EPA) plays a pivotal role in overseeing this process, ensuring compliance with national environmental standards.

Some crucial regional offices play pivotal roles in supporting project developers in urban areas, with the Environmental Protection Agency (EPA) and the Land Use and Spatial Planning Authority (LUSPA) being noteworthy examples. The EPA conducts environmental impact assessments (EIAs) for various projects, ensuring compliance with environmental regulations. This encompasses a range of development activities, such as the establishment of tourist attractions, hotel facilities, manufacturing plants, fuel and gas stations, and mining operations. The goal is to ensure that such developments do not significantly harm the environment or violate existing laws.

Meanwhile, LUSPA is responsible for the issuance of building permits, with a focus on promoting sustainable and economically viable human settlement development. Their activities ensure that planning adheres to sound environmental principles. Additionally, LUSPA provides zoning schemes aimed at protecting vulnerable areas from encroachment and climate-related hazards. The authority also has a vital role in regulating physical developments in ecologically sensitive regions, including forests, nature reserves, wetlands and other critical environments.

In Cape Coast, the EIA process is tailored to accommodate both small-scale and large-scale projects. Small-scale initiatives undergo a rigorous screening process designed to evaluate their environmental impacts. The screening results guide the issuance of environmental permits by the EPA. These permits are instrumental in allowing projects to commence while mandating that any environmental deficiencies identified during the assessment are effectively addressed.

For larger projects, particularly those that encounter community opposition, the EPA adopts a more inclusive approach by organising public hearings. These gatherings serve as a platform for community members to voice their concerns and suggestions, fostering a participatory process in decision-making. Notably, the requirement for two-thirds of the panel members to be residents of the local area ensures that the interests and needs of the community are well represented. This not only enhances the legitimacy of the decision-making process but also cultivates a sense of ownership among community members regarding local development projects.

When a project receives approval, the EPA takes proactive measures to communicate the decision widely. This includes sharing details with local authorities and making the information accessible to relevant stakeholders. A critical component of this transparency is the dissemination of a 21-day public notice alongside the final Environmental Impact

Statement (EIS) report. This practice underscores the commitment to community engagement, allowing stakeholders the opportunity to review and comment on the findings and implications of the EIA.

The institutionalisation of the EIA process is paramount for advancing effective climate governance. By establishing robust mechanisms for monitoring and accountability, local governments can systematically track the implementation and outcomes of climate-related actions. Such monitoring is vital for assessing the effectiveness of local climate policies and ensuring that they deliver the intended environmental, social and economic benefits.

Regular reporting is an essential facet of this accountability framework. It not only enhances transparency in governance processes but also builds community trust in local authorities. Engaging the public and local stakeholders in evaluating the success of climate initiatives offers governments invaluable insights, enabling them to adapt and refine practices based on real-world feedback and experiences. This iterative process is crucial in leading to more effective and resilient urban environments that can better withstand the challenges posed by a changing climate.

The integration of climate change considerations into urban planning through regulations, environmental permits and ongoing monitoring is vital for developing sustainable cities. By facilitating a structured EIA process, local governments can ensure that urban development practices contribute positively to environmental resilience, community well-being and sustainable growth. As cities continue to evolve in response to climate change, the role of EIAs and effective community engagement will be instrumental in shaping urban landscapes that are not only resilient but also equitable and environmentally responsible.

Education and capacity building

The findings of this study indicate that education and capacity building are fundamental tools that contribute significantly to the institutionalisation of climate change responses. A critical observation from the research is that while awareness of climate change issues is growing, many stakeholders still lack comprehensive knowledge about the specific measures being implemented at the local level. This gap underlines the need for ongoing educational initiatives to enhance understanding and engagement among community members and officials alike.

Stakeholders emphasised the necessity of ongoing educational initiatives, as some participants expressed a limited understanding of climate change issues and the adaptation strategies being deployed at the local level. Educational programs focused on climate issues have been instrumental in fostering awareness and encouraging community involvement in adaptation strategies. Local workshops and outreach initiatives serve to empower residents with knowledge about climate change and its local implications. The emphasis on strengthening human resources through targeted training programs is critical, given that effective climate governance hinges on a well-informed and proactive leadership base.

Stakeholder responses indicated an increasing awareness of the importance of integrating climate education into urban planning and development processes. Educational initiatives should encompass a wide array of topics, including practical climate adaptation strategies, environmental management and community engagement approaches, which can empower officials and the community at large to navigate the complexities of climate change impacts effectively.

Moreover, ongoing capacity building efforts not only equip stakeholders with the necessary skills but also foster a culture of collaboration and shared responsibility in addressing the climate crisis. Participants noted that when stakeholders are well-informed and trained, they are more likely to contribute meaningfully to discussions and decision-making processes, enhancing the overall resilience of Cape Coast to climate pressures.

Ghana's National Climate Change Adaptation Strategy calls for a multi-sectoral approach to effectively address climate challenges; however, the actual implementation of these strategies must occur at the local government level.[19] The capacity of local government officials must be considered during the process of mainstreaming climate adaptation strategies into existing frameworks. To this end, local governments have initiated various climate change awareness and sensitisation programmes aimed at improving community engagement in climate issues.

For instance, a recent consultative forum on climate change and flooding facilitated by the National Disaster Management Organisation (NADMO) brought together residents and officials to discuss the local implications of climate change. During this event, NADMO officials presented historical shoreline maps, illustrating significant erosion caused by local activities. This presentation had a profound impact on attendees, many of whom were unaware of how their actions contributed to increased flooding risks. The forum was attended by influential religious and community leaders, signalling a collective commitment to addressing these challenges.

Additionally, the research indicates that climate change awareness and sensitisation programmes are regularly conducted for diverse groups, including senior high school students, church congregations, university students and various local communities. These sessions often cover critical topics such as waste management and broader environmental management practices. The National Development Planning Commission (NDPC) has also been cited as a significant player in organising targeted workshops. These workshops aim to equip regional and local officials with essential knowledge, enabling them to support Metropolitan, Municipal and District Assemblies (MMDAS) in embedding climate change adaptation efforts within their medium-term development plans (MTDPS) and annual budgets.

Taboos and indigenous knowledge

Indigenous knowledge and practices, particularly in the form of taboos, have emerged as vital mechanisms for environmental protection. Taboos create strong social norms

[19] Government of Ghana 2012.

that prohibit harmful actions toward specific species, habitats, or natural resources. Often rooted in spiritual beliefs, these cultural norms reinforce the idea that violating such taboos could lead to detrimental consequences not only for individuals but for the entire community. This reliance on cultural norms serves as a complementary approach to regulatory measures and contributes to the preservation of ecosystems.

A poignant example of how local communities adapt to the climate crisis is found within practices observed in the Cape Coast Metropolitan Assemblys. Certain days are designated as fallow periods during which smallholder farmers and fishermen are prohibited from utilising their resources. This practice is based on the belief that these rest periods allow the sea and rivers to naturally replenish, ultimately fostering sustainability and continuity in the ecosystem's functionality. Participants in the research highlighted that such practices are crucial in allowing various ecosystems, including forests, rivers and seas to recuperate, which is essential for long-term environmental conservation.

Another noteworthy adaptive strategy involves the traditional preservation of mangroves and wetlands, with locals believing that spiritual entities inhabit these areas. To protect these crucial resources, traditional prayers are often conducted to appease the gods, thereby ensuring the availability of freshwater critical for local fishermen's livelihoods. Beyond their practical importance, forests and wetlands are often revered as sacred spaces, housing ancestors and deities that have historically supported the community. This intertwining of spiritual beliefs and environmental stewardship enhances cultural identity and encourages a communal commitment to ecological preservation.

In contrast to the typical response of many nations, which often involves erecting hard infrastructure like sea walls to shield against tidal waves and flooding, local communities in the Cape Coast opt for alternative strategies. For instance, they commonly utilise solid waste to create barriers against encroaching tides. This innovative approach reflects a grassroots-level responsiveness to environmental challenges. To further improve these adaptive measures, governments need to enact laws that facilitate the delegation of decision-making authority to local bodies.

The inclusion of local ecological knowledge has proven effective in developing context-specific adaptation strategies. Community members often possess valuable insights regarding agriculture, resource management and disaster preparedness, which can greatly enhance formal climate policies. The findings underscore the importance of an integrated approach to climate governance that incorporates both formal policies and informal practices. The recognition of local knowledge as a legitimate tool in climate adaptation reflects a broader trend towards participatory governance models. By valuing indigenous practices and community input, local governments can enhance their legitimacy and effectiveness in implementing adaptation strategies.

Investing in local capacity and actively engaging local actors in sustainable energy projects can significantly invigorate Ghana's economy. By fostering local ownership and enhancing employment opportunities, these initiatives have the potential to uplift the livelihoods and well-being of countless individuals residing in rural and remote areas across the African continent. Such strategies not only address immediate environmental challenges but also lay the groundwork for sustainable community development and resilience against future climate adversities.

Community engagement with non-governmental and civil society organisations

Addressing the impacts of climate change necessitates a collaborative approach that involves a diverse array of stakeholders, including government entities, non-governmental organisations (NGOs), the private sector and academic institutions. Effective implementation of national climate policies requires concerted efforts from all these parties. Informal discussions with key stakeholders revealed the existence of decentralised ministries, departments and agencies that facilitate this collaboration.

Research participants noted that while this stakeholder network has received recognition at the national level, the model has the potential to be replicated across other municipalities and local governments. It would need to be tailored to fit specific demographic, economic and local conditions concerning climate change mitigation and adaptation efforts.

Partnerships with non-governmental organisations and civil society groups have facilitated the implementation of community-led climate initiatives. These collaborations provide additional resources and expertise, amplifying the impact of local government efforts. Additional evidence of how climate change could be embedded within urban governance can be seen through the strategic maximisation of the impact of non-governmental organisations (NGOs) and civil society organisations (CSOs) at the local level. These entities are instrumental in promoting inclusive and participatory decision-making processes that actively engage local communities, Indigenous groups and a diverse array of stakeholders in the planning, implementing and evaluating climate adaptation policies and programs.

This collaborative approach ensures that local knowledge, needs and perspectives – essential elements that reflect each community's unique context – are effectively integrated into crucial decision-making processes. In discussions held in Wa and Cape Coast, several NGOs shared valuable insights on how such a participatory culture has normalised within their constituencies.

One of the stakeholders illustrated how establishing NGOs has proven to be a robust mechanism for increasing awareness across various crucial areas, such as climate resilience, disaster risk reduction, sanitation issues and overall environmental management. These organisations have played a significant role in educating the public and mobilising community action around these pressing issues. Government officials recognised that the NGOs and CSOs that have established effective partnerships with governmental bodies have overcome typical challenges. Their active involvement in various projects has enhanced community engagement and fostered better communication and collaboration between the government and the local populace.

Furthermore, research participants in Cape Coast noted the emergence of youth-led advocacy organisations that primarily focus on promoting environmental sustainability and community development. These organisations are vital in empowering and equipping young people with the skills and knowledge necessary to advocate for ecological education and sustainable practices. Among these groups, the Green Africa Youth Organization is a recognised actor in the Cape Coast Metropolitan Assembly. This organisation has been working with local communities to address specific groups' vulnerabilities, such as children, youth and women. These groups often bear the brunt of climate change impacts, exacerbated by existing social and structural inequalities. By focusing on these initiatives, the Green Africa Youth Organization aims to enhance resilience against climate-related challenges and promote social equity within the community.

Through these interconnected efforts, the role of NGOs and CSOs becomes increasingly vital in shaping urban governance frameworks that prioritise climate change adaptation, promote social inclusion and empower vulnerable populations. Their ongoing commitment to stakeholder engagement and community capacity building underscores the potential for transformative change in addressing the urgent challenges posed by climate change at the urban level.

Discussion and conclusion

In Ghana, the government has formulated and implemented national policies aimed at tackling the pressing effects of climate change. Among these pivotal frameworks are the National Climate Change Policy (NCCP), the National Climate Change Adaptation Strategy (NCCAS) and the National Climate Change Master Plan. These documents are crafted with the intent of guiding the nation's action against climate vulnerabilities. They are put into operation through a governance structure that involves various stakeholders, each with their distinct roles and responsibilities woven into the climate action tapestry.

While Ghana has made commendable progress on the national level, a significant hurdle persists: the lack of dedicated and effective local climate policies.[20] This gap restricts the ability of local authorities to autonomously manage climate challenges, compelling municipalities to seek external funding for most of their initiatives. However, this dependence on national resources creates further complications, especially for long-term projects that require sustainable financing and commitment.

Who are the stakeholders involved?

Given that the effects of climate change are most acutely felt at the local level, municipalities are crucial players in adaptation strategies. Yet, the extent of responsibility and the scope of actions assigned to local authorities differ dramatically from one country to another and even within diverse communities in Ghana itself.

At the heart of Ghana's climate governance framework is the Ministry of Environment, Science, Technology and Innovation (MESTI), headquartered in Accra. MESTI is responsible for formulating and executing the NCCP, benefiting from the technical support provided by the Environmental Protection Agency (EPA). The EPA plays a crucial role in coordinating Ghana's participation in international climate agreements. Although the EPA has its main office in the capital, its reach spans several regional and district offices across the country. Notably, these regional and district offices often lack dedicated climate

[20] Boateng 2023a; 2023b.

change units, which raises pressing concerns regarding their capacity to effectively address the unique climate issues inherent in local settings.

Beyond MESTI and the EPA, a myriad of ministries, departments and agencies (MDAs) have established their climate change units. For instance, the Forestry Commission boasts a Climate Change Unit, while the Energy Commission has divisions dedicated to renewable energy, energy efficiency and climate change matters. Despite these essential roles, there remains a contrast between the levels of engagement and capacity between national and local governments, often leaving local authorities out of crucial climate-related conversations.

Yet, a pattern of institutional fragmentation complicates the landscape of climate governance in Ghana's local government. The absence of a cohesive framework to facilitate inter-agency collaboration exacerbates this issue, forcing governmental bodies to operate in isolation rather than forming synergistic partnerships that could bolster climate resilience. Efficient governance mandates a comprehensive approach, where multiple layers of government and stakeholders cohesively devise and execute climate strategies.

The predominant emphasis on national-level initiatives often overshadows the essential functions of local administrations. The Ministry of Local Government has a role to play in climate issues via the Metropolitan, Municipal and District Assemblies (MMDAs), yet their active participation in the formulation and execution of climate change policies has been markedly limited. Research by Musah-Surugu et al. (2018) underscores the fragmented nature of sub-national governments, which frequently grapple with insufficient leadership and an absence of proactive measures. Many local governments typically engage with climate change projects only when initiated by central government directives, lacking the initiative to spearhead their localised initiatives.

While subnational actors possess vital insights and capacities, their involvement in formulating national policies remains minimal. This reality presents a troubling top-down approach that overlooks the valuable contributions that district-level representatives can offer to national debates. Such restricted participation signifies that local governments may not adequately tackle the unique climate challenges affecting their communities. A more equitable distribution of responsibilities and resources between the national and local spheres could significantly enhance the efficacy of climate response measures throughout Ghana, enabling all stakeholders to play a meaningful role in the nation's climate agenda.

The assumption that local representatives will adequately consult their communities before attending national workshops further amplifies the disconnect between various governance levels. The lines separating national, regional and municipal governance appear increasingly blurred, reflecting a crowded yet ambiguous governance landscape. This ambiguity, paired with overlapping authorities and roles, engenders confusion and, ultimately, hampers effective urban climate action.[21]

Additionally, the findings illuminate a conflict between national policies and indigenous knowledge systems. This tension underscores a broader struggle to harmonise modern scientific methodologies with time-honoured local traditions, which can result in missed

[21] Mitlin–Dodman 2015.

opportunities for incorporating effective climate adaptation strategies.[22] Local chiefs, as traditional custodians of natural resources, play an indispensable role in upholding sustainable practices.[23] However, their knowledge and expertise must be better integrated into formal climate governance frameworks to maximise their potential to foster resilience and sustainability within their communities.

In summary, the case of Cape Coast offers an illustrative example of how effective climate governance can arise from a thoughtful blend of educational initiatives, active community engagement and the meaningful integration of local knowledge. In this context, a deeper and ongoing engagement with stakeholders emerges as a pivotal strategy, essential for refining existing policies and for innovatively addressing the unique challenges that climate change poses to the region.

This narrative points out the perception that while formal top-down policies play a critical role in tackling the complexities of climate change, the power of informal practices deeply rooted in local culture cannot be overlooked. These cultural practices not only complement formal strategies but also enhance their effectiveness, making them vital components of a comprehensive response to climate issues. For cities in developing nations that face similar climate-related adversities, the insights derived from the experience of Cape Coast offer a valuable roadmap for fostering resilience. They encourage a more holistic approach to climate adaptation that is both practical and culturally sensitive.

As we look to the future, local administrations must embrace the institutionalisation of these adaptive tools. Doing so will enhance their capabilities in effectively managing climate risks, ultimately strengthening the community's resilience against the ongoing impacts of climate change. Furthermore, the study accentuates the importance of ensuring that these tools are not only implemented but also sustained in the long term.

As cities like Cape Coast navigate the enduring challenges presented by climate change, the adoption of a pluralistic governance framework becomes increasingly crucial. This framework should encompass a diverse range of methods and perspectives, fostering a more inclusive approach that empowers communities and leverages local knowledge. By doing so, Cape Coast and similar cities can cultivate a robust response to climate change that is both adaptive and sustainable, ensuring a better future for their residents and the environment alike.

Funding

This paper is part of the author's PhD project funded by Prince Albert II of the Monaco Foundation. The contents of this article are solely the author's liability and under no circumstances may be considered a reflection of the position of the Prince Albert II of Monaco Foundation and the IPCC Scholarship.

[22] Pasquini–Shearing 2014.

[23] Frick-Trzebitzky 2017.

Acknowledgements

I want to thank the stakeholders who participated in the fieldwork. I am equally indebted to my Supervisors, Péter Koronváry, PhD of the Ludovika University of Public Service in Hungary and Marta Olazabal, PhD of the Basque Center for Climate Change in Spain, whose insightful comments have improved the quality of this research.

References

ADB (2016): *African Economic Outlook 2016. Sustainable Cities and Structural Transformation.* African Development Bank – OECD – United Nations Development Programme.

Adu-Boateng, Afua (2015): Barriers to Climate Change Policy Responses for Urban Areas: A Study of Tamale Metropolitan Assembly, Ghana. *Current Opinion in Environmental Sustainability,* 13, 49–57. Online: https://doi.org/10.1016/j.cosust.2015.02.001

Araos Malcolm – Berrang-Ford, Lea – Ford, James D. – Austin, Stephanie E. – Biesbroek, Robbert – Lesnikowski, Alexandra (2016): Climate Change Adaptation Planning in Large Cities: A Systematic Global Assessment. *Environmental Science and Policy*, *66*, 375–382. Online: https://doi.org/10.1016/j.envsci.2016.06.009

Birkmann, Joern – Welle, Torsten – Solecki, William – Lwasa, Shuaib – Garschagen, Matthias (2016): Boost Resilience of Small and Mid-Sized Cities. *Nature,* 537(7622), 605–608. Online: https://doi.org/10.1038/537605a

Boateng, Ama K. (2023a): Localising Centralised Climate Policies in Ghana: Insights from 3 Local Governments. *Urban Research & Practice,* 16(3), 470–482. Online: https://doi.org/10.1080/17535069.2022.2129173

Boateng, Ama K. (2023b): Institutionalising Urban Climate Action: Recent Recognitions. *ESJ Humanities,* 19(2). Online: https://doi.org/10.19044/esj.2023.v19n2p146

Fila, Dennis – Fünfgeld, Hartmut – Dahlmann, Heindriken (2023): Climate Change Adaptation with Limited Resources: Adaptive Capacity and Action in Small- and Medium-Sized Municipalities. *Environment, Development and Sustainability,* 26, 5607–5627. Online: https://doi.org/10.1007/s10668-023-02999-3

Frick-Trzebitzky, Fanny (2017): Crafting Adaptive Capacity: Institutional Bricolage in Adaptation to Urban Flooding in Greater Accra. *Water Alternatives,* 10(2), 625–647.

Government of Ghana (2012): *National Climate Change Adaptation Strategy.* Online: www.adaptation-undp.org/sites/default/files/downloads/ghana_national_

Hoppe, Robert (2019): Policy, Governing and Politicality. *EPA. European Policy Analysis,* 5(2), 150–169. Online: https://doi.org/10.1002/epa2.1074

Institute for Health Metrics and Evaluation (2021): *Ghana Population and Housing Census 2021.* Online: https://ghdx.healthdata.org/record/ghana-population-and-housing-census-2021

IPCC (2023): *Climate Change 2022. Impacts, Adaptation and Vulnerability.* Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781009325844

Mitlin, David – Dodman, Diana (2015): The National and Local Politics of Climate Change Adaptation in Zimbabwe. *Climate and Development*, 7(3), 223–234. Online: https://doi.org/10.1080/17565529.2014.934777

Musah-Surugu, Issah J. – Ahenkan, Albert – Bawole, Justice N. (2019): Too Weak to Lead: Motivation, Agenda Setting and Constraints of Local Government to Implement Decentralized Climate Change Adaptation Policy in Ghana. *Environment, Development and Sustainability*, 21(2), 587–607. Online: https://doi.org/10.1007/s10668-017-0049-z

Musah-Surugu, Issah J. – Ahenkan, Albert – Bawole, Justice N. – Darkwah, Antwi S. (2018): Vulnerability Here, There, and Everywhere: What Happened to Ghana's Decentralized Climate Change Adaptation Policy? In Alves, Fátima – Leal Filho, Walter – Azeiteiro, Ulisses (eds.): *Theory and Practice of Climate Adaptation. Climate Change Management.* Cham: Springer, 105–123. Online: https://doi.org/10.1007/978-3-319-72874-2_6

Olazabal, Marta – Amorim-Maia, Ana T. – Alda-Vidal, Cecilia – Goodwin, Sean (2024): What Is Limiting How We Imagine Climate Change Adaptation? *Current Opinion in Environmental Sustainability*, 71. Online: https://doi.org/10.1016/j.cosust.2024.101476

Otto, Antje – Kern, Kristine – Haupt, Wolfgang – Eckersley, Peter – Thieken, Annegret H. (2021): Ranking Local Climate Policy: Assessing the Mitigation and Adaptation Activities of 104 German Cities. *Climatic Change*, 167. Online: https://doi.org/10.1007/s10584-021-03142-9

Ostrom, Elinor (2005): *Understanding Institutional Diversity.* Princeton: Princeton University Press. Online: https://doi.org/10.2307/j.ctt7s7wm

Ostrom, Elinor (2011): Background on the Institutional Analysis and Development Framework. *Policy Studies Journal*, 39(1), 7–27. Online: https://doi.org/10.1111/j.1541-0072.2010.00394.x

Pasquini, Lorena – Shearing, Clifford (2014): Municipalities, Politics, and Climate Change: An Example of the Process of Institutionalizing an Environmental Agenda within Local Government. *The Journal of Environment & Development*, 23(2), 271–296. Online: https://doi.org/10.1177/1070496514525406

Patterson, James J. – Huitema, Dave (2019): Institutional Innovation in Urban Governance: The Case of Climate Change Adaptation. *Journal of Environmental Planning and Management*, 62(3), 374–398. Online: https://doi.org/10.1080/09640568.2018.1510767

Reckien, Diana et al. (2018): How Are Cities Planning to Respond to Climate Change? Assessment of Local Climate Plans from 885 Cities in the EU-28. *Journal of Cleaner Production*, 191. Online: https://doi.org/10.1016/j.jclepro.2018.03.220

Salvia, Monica et al. (2021): Will Climate Mitigation Ambitions Lead to Carbon Neutrality? An Analysis of the Local-level Plans of 327 Cities in the EU. *Renewable and Sustainable Energy Reviews*, 135. Online: https://doi.org/10.1016/j.rser.2020.110253

UN-Habitat (2020): *World Cities Report 2020: The Value of Sustainable Urbanization.* Online: https://unhabitat.org/world-cities-report-2020-the-value-of-sustainable-urbanization

UN DESA (2019): *UN DESA Annual Highlights Report 2019–2020.* Online: www.un.org/en/desa/highlights-report-2019-2020

Valdivieso, Patricio – Andersson, Krister P. – Villena-Roldán, Benjamin (2017): Institutional Drivers of Adaptation in Local Government Decision-Making: Evidence from Chile. *Climatic Change,* 143(1–2),157–171. Online: https://doi.org/10.1007/s10584-017-1961-9

Further reading

Adjaison, Desmond – Amoah, Antwi-Boasiako (2024): Assessing Accra's Climate Action Plan as a Case of Vertical Integration to Achieve Sustainable Development. *Environment, Development and Sustainability*. Online: https://doi.org/10.1007/s10668-024-05341-7

Mubaya, Chipo P. – Mafongoya, Paramu (2017): The Role of Institutions in Managing Local Level Climate Change Adaptation in Semi-Arid Zimbabwe. *Climate Risk Management,* 16, 93–105. Online: https://doi.org/10.1016/j.crm.2017.03.003

Wisner, Ben – Pelling, Mark – Mascarenhas, Adolfo – Holloway, Ailsa – Ndong, Babacar – Faye, Papa – Ribot, Jesse – Simon, David (2015): Small Cities and Towns in Africa: Insights into Adaptation Challenges and Potentials. In Pauleit, Stephan – Coly, Adrien – Fohlmeister, Sandra – Gasparini, Paolo – Jørgensen, Gertrud – Kabisch, Sigrun –Kombe, Wilbard J. – Lindley, Sarah – Simonis, Ingo – Yeshitela, Kumelachew (eds.): *Urban Vulnerability and Climate Change in Africa. A Multidisciplinary Approach.* Cham: Springer, 153–196. Online: https://doi.org/10.1007/978-3-319-03982-4_5

10.32565/aarms.2024.3.6

Hacktivists, Proxy Groups, Cyber Volunteers

The Future of Non-State Actors' Involvement in Military Cyber Operations[1]

Csaba KRASZNAY[2]

This paper explores the involvement of hacktivists, cyber volunteers and proxy groups in military cyber operations, with a particular focus on their roles in the ongoing Russian–Ukrainian war. The research aims to analyse the participation of these non-state actors, their legal implications, and how their involvement could influence the strategic, operational and tactical practices of small and medium-sized NATO member states, such as Hungary. Drawing from case studies, literature review and in-depth interviews with Hungarian military intelligence and public administration leaders, the paper formulates two hypotheses: 1. Hacktivist groups, unless integrated into a state's cyber strategy, hinder tactical objectives and raise significant international legal concerns; and 2. Such groups pose a strategic threat to small NATO countries, including Hungary. The findings emphasise the necessity for NATO states to consider how to engage and regulate cyber volunteers effectively, while minimising the risks posed by hacktivist and proxy groups. Additionally, the research underscores the lack of a unified legal framework governing the use of these non-state actors, which complicates their regulation and control in cyberspace conflicts. The paper concludes with recommendations for how NATO states can leverage the openness of civilians to participate in cyber defence while maintaining legal and operational oversight, supporting the involvement of various cyber groups within the framework of international law.

Keywords: *proxy groups, hacktivists, cyber volunteers, cyber warfare*

[1] This paper was supported by the Bolyai János Research Scholarship of the Hungarian Academy of Sciences.

[2] Ludovika University of Public Service, Department of Cybersecurity, e-mail: krasznay.csaba@uni-nke.hu

Introduction

One of the key issues of the Russian–Ukrainian war from the point of view of military science is the use of cyberspace as the fifth operational domain by the warring parties. At the time of the outbreak of the war, a significant number of military experts believed that cyber operations would be crucial to achieving success, given that Russia had been building its capabilities in this direction since the early 2000s and that the operational objectives were to bring Ukraine to its knees as quickly as possible with as little physical destruction as possible. The procedural methods developed in hybrid operations in cyberspace would have served this objective perfectly. However, the successful military defence of Ukraine has set a different direction for this war, and the focus of military research has shifted to the analysis of events in physical space. But this does not mean that cyberspace operations are not present in less spectacular ways in the course of the confrontations and that elements of operations that had not been encountered in practice before are not present.

Since the early 2000s, the literature has addressed the question of how hackers in a war situation can participate in the defence of their country or in offensive operations against other countries, even if they are citizens of a non-belligerent party. This research topic became particularly topical in 2007, when a cyberspace operation was launched against Estonia. The state-of-the-art of the findings on non-belligerent parties, with the contribution of eminent scholars of international law, was the Tallinn Manual 2.0, published in 2017, the relevant points of which will be quoted below. Since the outbreak of the Russian–Ukrainian war in 2022, however, there are a number of events that can be analysed in practice, which are referred to in the Tallinn Manual 2.0 in theory. After the creation of the Ukrainian IT Army, Healey and Grinberg (2022) warned that support for such irregular groups was both contrary to international law and to the practices issued by the UN and accepted by all member states. While this research attitude persists, a number of questions have been raised about the detail. It is worth mentioning, for example, the study of Thøgersen (2023) examining how hackers supporting the Ukrainian IT Army who do not live in Ukraine should be viewed by the countries from which they conduct their operations. She concludes that the relevant points of international law are quite controversial, and that their interpretation requires that as many states as possible express their views on them. A similar conclusion is reached by Chan and Khaw (2024), who examine nation-state behaviour in cyberspace from the perspective of customary international law. The conclusion of their study is that international law needs to become more interdisciplinary, less nation-state-centred and more adaptable to the challenges of the modern age. Smith and Dean (2023) analyse the activities of irregular cyberspace participants, and their findings are very similar. They also raise the research question of whether these groups are automatically considered enemy combatants by virtue of their participation, and how should the use of commercial IT products and services in conflict be classified? Ashdown (2024) analyses how military and civilian cooperation in sharing cyber intelligence can be achieved. In his view, this will happen organically, as it has happened in other operational domains. The conclusion of many articles on the subject is therefore typically that, until nation states clearly state their views on the involvement of non-belligerent groups, there is a theoretical framework and high-level positions, but no legal consensus on the details.

The high-level objective of this research is to monitor and analyse the cyber operations of Russia and Ukraine, as well as their supporting external parties, and to draw lessons that can be usefully incorporated into the strategic, operational and tactical practices of a small or medium-sized NATO member state. In this particular research, it is examined how belligerents and their supporters in the Russian–Ukrainian war have involved cyber volunteers, hacktivists and other proxy groups in the conduct of military cyber operations and the feasibility of this approach in Hungary as a NATO member state, considering the possibilities offered by national and international law. The paper's aim is not to give a legal analysis, but rather to make proposals from an organisational, cooperative point of view for military and civilian cooperation in the chosen field. For motivation, the last sentences of Ashdown (2024: 323) can be quoted: "However, the value of historical study may be as much in examining the process by which multiple actors collectively (but not always cooperatively) defined those new domains and their roles within them. In doing so, those actors redefined themselves – they 'bent themselves out of shape together'. It is precisely such a process of redefinition that will play out as militaries and private sector actors learn how to collaborate in the production, sharing, and use of cyber intelligence. The choice facing these organizations is whether to pursue coherence and bend, or cling to unity and break."

The first hypothesis is that the involvement of hacktivist groups in offensive military operations hinders rather than helps to achieve tactical objectives, besides raising serious international legal issues, unless they are tasked and directed by military leadership as cyber volunteers. The second hypothesis is that hacktivist groups pose a strategic threat to all small and medium-sized NATO member states like Hungary, even though they have so far been little perceived as such. To support the first hypothesis, case studies are presented, that are available in open sources in addition to a literature review. In selecting the case studies, those cases were chosen that are representative of the activities of the selected groups. The use of open sources is necessary because the "fog of war" is very significant in an active conflict, making it very difficult to find scientifically credible sources. Therefore, the study will rely on sources that are considered trusted in the cybersecurity and military fields, and are considered primary sources. In support of the second hypothesis, in-depth interviews were conducted with Hungarian military, intelligence, public administration and critical infrastructure defence leaders and commanders whose primary responsibility is to lead and coordinate the national cyber defence. In selecting the interviewees, the primary criterion was to interview experts who, by virtue of their position, are primarily responsible for the military and civilian cyber defence of Hungary, as well as for the cyber defence of critical infrastructures that are crucial for the Hungarian economy. In total, 14 interviews were conducted, online, between December 2023 and February 2024. The anonymity of the respondents is important due to their position. This research was supervised by senior researchers from the Institute for Cybersecurity at the Ludovika University of Public Service, and they confirmed that the selected pool of interviewees is representative. The questionnaire included a number of questions that will be published in other papers, but some of them were specifically designed to gauge respondents' attitudes towards non-state cyberspace actors.

Conceptual and legal background

Clarifying the conceptual background is essential for the implementation of the research. In this paper, those persons and groups are mentioned that are identified as non-state actors in the Tallinn Manual 2.0. According to Rule 33: "International law regulates cyber operations by non-State actors only in limited cases."[3] In this context, the category of Civilians under Rule 91 includes the subjects listed in the study, saying that "civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate".[4] For ease of identification, the groups referred to in the study are classified according to the criteria proposed by Jason Healey in 2012 and refined by Healey and Grinberg (2022). The author has set up the following relationship between state and non-state actors:

1. State-prohibited: The national government will help stop the third-party attack.
2. State-prohibited-but-inadequate: The national government is cooperative but unable to stop the third-party attack.
3. State-ignored: The national government knows about the third-party attacks but is unwilling to take any official action.
4. State-encouraged: Third parties control and conduct the attack, but the national government encourages them as a matter of policy.
5. State-shaped: Third parties control and conduct the attack, but the state provides some support.
6. State-coordinated: The national government coordinates third-party attackers such as by "suggesting" operational details.
7. State-ordered: The national government directs third-party proxies to conduct the attack on its behalf.
8. State-rogue-conducted: Out-of-control elements of cyber forces of the national government conduct the attack.
9. State-executed: The national government conducts the attack using cyber forces under its direct control.
10. State-integrated: The national government attacks using integrated third-party proxies and government cyber forces.

In this study, some key terms are used. First of all, the role of proxy groups is examined. According to Michael N. Schmitt and Liis Vihul, proxy groups in cyberspace are defined as non-state actors acting under the instructions of a state or controlling or directing the actions of a non-state actor, unless the state actor oversteps its authority and influences the

[3] Schmitt 2017: 174.
[4] Schmitt 2017: 413.

non-state actors. Thus, if a state intelligence service influences a hacker, cybercriminal group, loose, informal group, corporation, or even a terrorist, or insurgent group, we can speak of a proxy operation. The point is that while all of this needs to be judged on a case-by-case basis, there should be a clear governance link between the state and the non-state actor.[5] They belong to the State-coordinated and the State-ordered categories.

Moreover, the work hacktivism is also appearing in the paper. There are many sources to explain this term, but it is worth going back to the source, which defines hacktivism as the empowerment of people to make the world aware of injustices and violations of human rights. In other words, to organise the flow of information worldwide, without restrictions or censorship. The word hacktivism comes from Omega and the concept was described by Count Zero. Oxblood Ruffin (2010) added: "Using technology to improve human rights across electronic media." All three were members of the hacker group Cult of the Dead Cow (cDc), and the term itself emerged in the mid-1990s when cDc was also very active in public life.

Hacktivism is made by hacktivists who engage in hacktivism. However, since the 1990s we have seen so many different forms of hacktivism that it is worthwhile to think more broadly about the participants! This is how Tim Jordan and Paul Taylor describe the phenomenon in their book on hacktivism:

> "Hacktivism is the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaching out of cyberspace utilising virtual powers to mould offline life. Social movements and popular protest are integral parts of twenty-first-century societies. Hacktivism is activism gone electronic."[6]

A hacktivist is therefore someone who takes part in a cyberspace action organised around a political ideology that has an impact on the physical world. Hacktivist groups belong to the State-prohibited-but-inadequate and State-ignored categories in this study.

As a subgroup, patriotic hackers are a very important group of hacktivists for military cyber operations. In her book on hacktivism, Athina Karatzogianni describes patriotic hackers as those who fight for the purity of their nation through the clever use of online media. Paradoxically, nationalism as a political ideology appears behind classic hacktivist actions, exploiting the internet as a global media.[7] They belong to the State-encouraged and the State-coordinated categories.

When patriotic hackers officially carry out their activities under state control, they become cyber volunteers. They can be either in the State-executed or the State-integrated categories. Rain Ottis defines this term this way:

[5] Schmitt–Vihul 2014.

[6] Jordan–Taylor 2014: 1.

[7] Karatzogianni 2015: 22.

> "People who participate in the cyber militia of their own free will. They do not get paid for their activities, nor do they have a contractual obligation to the militia. They have the right to choose their level of commitment and to leave the militia, if and when they wish. Therefore, volunteer soldiers who join a government-run cyber attack unit are not considered a cyber militia."[8]

The toolbox of hacktivist actions is not nearly as complex as what a state actor with excellent operational planning skills could execute. Moreover, the strength of hacktivist groups lies in their visibility, so they have no interest in keeping the operation hidden, and they typically carry out the act in groups, often not knowing each other, even from very different geographical locations. Conspiracy is therefore not necessarily the goal. Thus, as summarised by Marco Romagna, a hacktivist attack is typically limited to distributed denial of service attacks (DDoS), website defacement and data theft. Occasionally, malicious code may be used, but this has a rather negative resonance in the community.[9]

It is also important to understand the international legislation to the background of this study. Since hacktivists, proxy groups and cyber volunteers have long been present in the academic discourse, there have been numerous studies on how to judge their activities, including in armed conflicts. Perhaps the most important guidance is the clear prohibition of the use of proxy groups in cyberspace operations, as set out in the final report of the United Nations (UN) Group of Governmental Experts (GGE) 2012–2013. The GGE is tasked with reaching a consensus among member states on certain basic cyberspace rules and standards. Paragraph 23 of UN Resolution A/68/98 makes this clear: "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."[10]

The Tallinn Manual, which takes up the international legal interpretation of the use of cyberspace in war, attempts to clarify the rules for the use of proxy groups, hacktivists and cyber volunteers. Rule 17 sets out this requirement most precisely. According to this rule, the activities of non-state actors carrying out cyber operations are attributable to a state when they are acting under the direction of, or under the direction and control of, a state actor and the state actor is aware of and uses the operation for its own purposes.[11]

Rule 69 attempts to define where the boundary of acts that violate international law begins. According to this rule, cyber operations constitute an act of violence if their scale and effect are comparable to non-cyber operations that constitute an act of violence. It is explained that, for example, the mere financing of a hacktivist group does not constitute an act of violence if that group is part of an insurgency against another country.[12] This explains why it can be useful to support in-country hacktivist groups such as Cyberberkut,

[8] Ottis 2011: 34.

[9] Romagna 2019.

[10] United Nations General Assembly 2013: 8.

[11] Schmitt 2017: 94.

[12] Schmitt 2017: 330.

a pro-Russian group within Ukraine that was actively involved in the cyberspace part of the armed conflict in eastern Ukraine before the outbreak of the war in 2022.[13]

Rule 82 further clarifies when a cyberspace operation constitutes an armed conflict and the place of hacktivist groups in it. Armed conflict is defined as hostilities between two states, including actions that involve mere cyber operations. The rule explains that a cyber operation against Estonia in 2007, for example, does not constitute an armed act because there is no evidence that the persons involved were acting under the instructions of a state or that the operation was organised or approved by a state. In addition, it is questionable whether there was any use of weapons at all, i.e. whether the means used constitute cyber weapons. It is therefore clear from the explanation that, although there are many indications of a coordinated operation by intelligence services, the lack of evidence did not allow for an escalation of the response under international law.[14] However, an analysis of the actions carried out during the Russian–Ukrainian war could lead to exact examples of cyber operations that could be interpreted as an armed conflict.

According to Rule 95, in an armed conflict, a person should be considered a civilian until it is clearly established that he or she is not a civilian. In the case of a hacktivist, it is therefore particularly difficult to take any countermeasures as long as he or she is not directly engaged in hostilities.[15] Under Rule 97, however, direct participation deprives him of civilian status. It is explained that if, for example, a hacktivist tries to attack a military command and control system several times in a row, he remains targetable as long as he continues to attack, not only during the specific attack but also between attacks. In fact, if there is a possibility that he or she will continue attacks after a long pause, the hacktivist may remain a target as long as his or her operational capability is maintained. These rules clearly distinguish the activities of cyber volunteers from those of hacktivists.[16]

Cyber volunteers, hacktivists and proxy groups in the Russian–Ukrainian war

Several members of the open-source intelligence community have been actively following the activities of groups emerging from the Russian–Ukrainian war. Perhaps the best-known such collection can be found at Cyberknow. The CyberTracker's update, released on the second anniversary of the war, identified a total of 125 groups, of which 44 groups supported Ukraine and 81 groups supported Russia. Since the beginning of the war, a total of 380 hacktivist groups have appeared on Cyberknow's lists, but a significant number of these have become inactive over the years.[17] In an analysis also published in February 2024, SecAlliance's Riam Kim-McLeod identifies 34 pro-Russian hacktivist groups that have undertaken more than 4,000 attacks in 2023, often with questionable success. This

[13] Koval 2015.

[14] Schmitt 2017: 379.

[15] Schmitt 2017: 424.

[16] Schmitt 2017: 428.

[17] Cyberknow 2024.

information comes mainly from the groups' Telegram channels.[18] By analysing open sources, it is possible to identify groups that are genuinely hacktivist, that act as proxies and that fit into the category of cyber volunteers.

The hacktivists

Hacktivist groups are independent of the control of state organisations, or at least have no conscious connection with any military or intelligence services. This does not mean, of course, that their operations and actions are not influenced by, or at least not known to, law enforcement agencies, but this indirect link does not cross the boundaries of Rule 17 of the Tallinn Manual. Typical examples include groups operating outside Russia or Ukraine, the best known of which is Anonymous. Anonymous is a decentralised group with a common name and visual elements, but each group defines its own operational objectives. Cyberknow's list includes several groups that define themselves as Anonymous, some of which were active long before the war and some of which were created at the outbreak of the war. Anonymous Romania and AnonGhost are older, Anonymous Italia and AltroAnon are newer. None of the analyses link these groups to either the Ukrainian or their own governments, so it is reasonable to assume that they operate along traditional hacktivist lines.

One of the best examples of Anonymous activity is the March 2022 attack on the servers of the Russian media authority Roskomnadzor. As a result, more than 800 gigabytes of data, including 340,000 files, were uploaded to the Distributed Denial of Secrets (DDoSecrets) site. Although details of the operation are not available, the plot is very typical of Anonymous. After hacking into the Internet server of a politically symbolic organisation (the Russian Internet censorship authority), a lot of data is being uploaded in bulk to a non-governmental leak site, which has previously published information that is embarrassing to the U.S. Government.[19] The target does not seem to be relevant from a military point of view, it may be useful from an intelligence point of view, but it is primarily of political use. A review of collection of the tools Anonymous deployed in 2022 shows that they are not necessarily valuable in supporting military operations, and may even be clearly harmful to countries supporting Ukraine.[20] The list includes the following targets:

- hacking printers
- using Conti Ransomware code
- hijacking Russian servers
- hacking the news
- attacking exposed data
- targeting companies who still do business in Russia
- RoboDial, SMS and email spam
- hacks on key Russian holidays and important date hacks

[18] Kim-McLeod 2024.

[19] Brewster 2022.

[20] Fowler 2022.

However, an interesting anomaly in this series is Anonymous Sudan. This group emerged in early 2023 and its activities coincide to a significant extent with the targets of Russian hybrid operations. In addition, the group has publicly aligned itself with several well-known Russian actors, including Killnet. Statements posted on Telegram also openly support Russian activities. Cyberint's analysis has hypothesised, based on several other small indications, that this group is either a covert counterpart of a Russian intelligence service or part of a well-known Russian cybercriminal group.[21] If this hypothesis is correct, the activity of this group goes beyond hacktivism and should be classified as a proxy group.

The proxies

The category of proxies typically includes groups operating within Russia. The link between Russian intelligence services and patriotic hacker groups is not new. Already during the cyberattack against Estonia, the international press and politics almost immediately identified Russia as the state behind the attack, but the Russian Government then and since then has consistently denied its involvement in the operation. Rain Ottis put the available facts like this in 2008:

> "The Russian government has consistently denied any direct involvement in the cyber attacks that hit Estonia in the spring of 2007. To the author's knowledge, this claim is true. It is remarkable, however, that neither is there any proof of measures taken by the Russian government to mitigate the situation. The lack of cooperation in the Estonian investigation indicates that the Russian government is not interested in identifying the attackers and is therefore, in essence, protecting them. In other words, hostile rhetoric from the political elite motivated people to attack Estonia while nothing was done to stop the attacks. This silent consent, however, can be interpreted as implicit state support because, without fear of retribution, the attackers were free to target Estonian systems."[22]

Ottis adds that information about the execution of the attack was shared among the participants in Russian-language forums. The target, the timing, the method of execution and the ideological motivation were precisely defined. In the end, the attack was carried out by the Nashi ("Ours") youth movement led by Konstantin Goloskokov, who denied having received any instructions from Russian officials.[23] Interestingly, in 2016, Ukrainian security agencies referred to Goloskokov as an officer of the Russian military intelligence service, the GRU, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation.[24]

[21] Cyberint Research Team 2023.
[22] Ottis 2008.
[23] Lowe 2009.
[24] UCMC 2016.

A report by the Russian investigative portal Meduza names Pyotr Levashov as the coordinator of the attack, who "full-time" ran one of the largest unsolicited mail services, Kelihos, until he was arrested in Barcelona in 2017 following an FBI investigation. According to Medusa's sources, Levashov had been cooperating with Russian state agencies since at least 2005 and actively supported some of their operations using Kelihos's infrastructure.[25] In return, he was untouchable, so although the U.S. investigative authorities had already indicted him in 2007, it was impossible to catch him for 10 years.[26]

This operation is very similar to the one performed by the team NoName057(16). An analysis by SecAlliance cited earlier highlights that this team alone was responsible for more than half of the pro-Russian hacktivist attacks in 2023. According to the analysis, its operations are significantly different from those of all other groups, as their operations are continuous, pre-planned, preceded by serious reconnaissance, in an almost military-like order. They engage a wide range of participants through their Telegram channel, whose work is paid for in cryptocurrency, but their source of funding is unknown. Meanwhile, there is not a single person who publicly claims to run the group.[27] The attacks are carried out using a proprietary service DDoSia.[28] One of the group's recognised attacks was launched against the website of the Finnish Parliament when the country announced its accession to NATO. The DDoS attack only caused problems for a short time. This model is very reminiscent of the Nashi story, so although at the time of writing it is not yet possible to prove that it is a proxy group, it is worth watching for new information about the group in the coming years. There is no information on data theft, which is more typical of ransomware groups that are also likely to be collaborating with Russian state agencies. Due to space constraints, the functioning and role of ransomware groups will not be discussed in this paper.

The cyber volunteers

The most obvious cyber volunteer organisation of the groups that have emerged in the war is the Ukrainian IT Army. Unlike other similar organisations, this group was declared to have been created at the call of the Ukrainian Government on 26 February 2022, when the Minister for Digital Transformation, Mykhailo Fedorov called on professionals who wanted to support the Ukrainian cause to join the IT Army, according to Soesanto (2022). The idea itself came from a Ukrainian digital entrepreneur, Yegor Aushev. Telegram, the main communication platform, has hundreds of thousands of subscribers. Based on Smith and Dean's research, a total of 9,547 domain names have been identified as targets in the Telegram channel as of 1 November 2022.[29] The group has been active during the second anniversary of the war, including the successful attack on the Russian Troika system, the fare payment system for public transport in several Russian cities. The successful attack

[25] Turovsky 2018; U.S. Department of Justice 2018.

[26] United States District Court for the District of Alaska 2017.

[27] Antoniuk 2023.

[28] Sekoia TDR et al. 2024.

[29] Smith–Dean 2023.

was announced by the Ministry of Digital Transformation, which clearly indicates that the IT Army is under the control of the Ukrainian Government.[30]

The IT Army is neither part of the Ukrainian army nor the secret service, nevertheless, it is under their control. Its participants support Ukraine's fight but are not under the command of the superiors of the armed organisations, can participate in any operation and can leave the group at any time. No security checks are carried out on members, and the level of operational security during the execution of attacks is nowhere near as high as it would be for a military or intelligence operation. For this reason, operations are designed to be as spectacular as possible, in line with classic hacktivist attacks. While the Estonian Defence League's cyber unit was the forerunner of the IT Army, which is a classic military volunteer reserve unit with the appropriate status and command, the Ukrainian group is an ad hoc organisation that could in time form the nucleus of an Estonian-style solution but is not at that level at present.

Both Soesanto and Smith and Dean point out, however, that the IT Army's operation raises several legal problems. The legal status of cyber volunteers is clear under the Tallinn Manual rules already quoted, as long as they are working in Ukraine. However, it raises several questions if they are carrying out their activities against Russia from the territory of a country that is not a belligerent in this war. In this case, their activities are likely to violate the law of their own country constituting a criminal offence, but there are no reports of active prosecution by the law enforcement agencies of the countries concerned. So unlike the Russian groups, where the state does not assume any apparent association with its own proxy groups, therefore it is very difficult to attribute them, although if it is possible to do so, then a clear violation of international law can be established, the use of cyber volunteers is clarified in international law. They can be considered an insurgent group with all the consequences that entails, except for those who join from other countries, because in their case cybercriminal is the appropriate term, who should be prosecuted ex officio by the authorities of their own country.

Lessons learned for NATO member countries

The experience of the Russian–Ukrainian war has made it necessary for all NATO members to consider what to do with civilians who want to get involved in possible future conflicts. The primary objective is obviously to recruit as many of the best experts as possible into the professional armed forces who can carry out the necessary cyber operations professionally and under appropriate control. The secondary objective is to recruit as many people as possible into the voluntary reserve system who can be available in a trained and controlled manner, in the Estonian model, in the event of a conflict. However, the groups analysed in this study should be handled with care.

Hacktivists, and patriotic hackers within them, are typically difficult to control, their activities often falling under the categories of computer crimes in the national criminal code, following their emotions rather than instructions. It is easy to imagine that their worldview

[30] Fornusek 2024.

is unacceptable to their governments. They cannot be trusted; therefore, it is difficult to share the necessary operational information with them. Typically, they are involved in offensive operations from several countries, which can cause serious international legal and diplomatic problems. It is easy to imagine that their offensive activities could disrupt covert operations conducted by professional intelligence organisations. For this reason, formal contact with hacktivist groups is not recommended. In the meantime, however, it is advisable to exploit the potential of information operations and to influence the activities of these groups in support of the strategic objectives, as long as this does not constitute direct control and does not violate international law.

The use of proxy groups in warfare is clearly prohibited by international law if they carry out acts of violence. In addition, many NATO governments support the Paris Call for Trust and Security in Cyberspace initiative of the French Government, including Principle 8 which explicitly seeks to prevent non-state actors from participating in offensive operations.[31] While there is nothing to prohibit a state from acting as an organising force behind a hacktivist group and thus using it as a proxy, whether in peacetime, hybrid operations, or in war, to the extent that they do not carry out acts of violence, there would be a serious political dilemma and risk in supporting a proxy group alongside existing commitments. For this reason, it is not advisable to pursue this course.

However, based on the Ukrainian experience, supporting cyber volunteers could be an appropriate direction for NATO member states, given that such groups could be a precursor to the voluntary reserve system and then to professional status. In Hungary, discussions have been ongoing since the early 2010s on how to involve civilian professionals in the country's cyber defence. In 2011, the Voluntary Cyber Defence Coalition was founded to bring together interested parties, following the Estonian model. However, in the period since then, it has not been possible to find a legal way for the Hungarian Defence Forces and volunteers to work together. The main obstacle was the creation of a trust-based legal framework, as there was no possibility of establishing a legal relationship with the volunteers that would include the appropriate guarantees for the Hungarian Defence Forces, while the volunteer reserve status was not considered acceptable by the applicants. Since the establishment of the Hungarian Cyber Command within the Hungarian Defence Forces in 2019 and the possibility to recruit professionals even for offensive cyber operations, the involvement of volunteers has become redundant.

However, the experience of the Russian–Ukrainian war shows that a cyber militia outside the organisation and hierarchy of the army, but under the direction and control of the state, may be necessary. For this reason, it is advisable to examine carefully the national regulations relating to the IT Army and to transpose them into the national legal systems of NATO member states. Indeed, surveys in Hungary show that cybersecurity experts are open to participate in military operations. Back in 2010, the openness of young people to become cyber volunteers was assessed. Although the survey is not representative, its respondents were selected from among the attendees of Hungary's most important hacker conference, Hacktivity, so it is indicative of the willingness to cooperate. Of the 187 respondents, 59% said that if their country needed help, they would be available. 55%

[31] Government of France 2018.

of them, meanwhile, had an explicitly negative opinion of the Hungarian Defence Forces.[32] The survey was repeated in 2024 at the University of Pécs, led by Gábor Gyurák, among students who are studying cybersecurity as part of their curricula. Although 14 years have passed between the two surveys, the willingness to support is very similar. 51.6% of the 219 respondents would support Hungarian cyber operations as volunteers. However, the perception of the Hungarian Defence Forces has improved dramatically in the intervening period, with 72.1% of respondents in the new survey having a positive opinion of the military, up from 26% in the previous survey, suggesting that cyber volunteering may, in fact, be the gateway to systemic engagement.[33]

The threat posed by hacktivist groups

So, cooperation with cyber volunteers can be beneficial for military defence, but the question is how big a threat to national security the hacktivist groups pose. The cited SecAlliance research clearly shows that the activity of attack groups in 2023 was primarily directed against countries that are active participants and supporters of the Russian–Ukrainian war. Ukraine is of course in first place with 718 attacks, followed by the Czech Republic with 300, Poland with 298, Sweden with 245 and Germany with 234. At the bottom of the list are Ireland with 2 attacks, Hungary with 5 and Portugal with 6. The low number of attacks may be explained by the lack of interest due to geographical distance, as the two Western countries have small numbers even though Portugal supports Ukraine with tanks and Ireland with trainers, but also by the more sympathetic attitude towards Russia, which is well known in the case of Hungary. This does not mean that the exposure to hacktivist groups in these countries could not change at any time!

Hungary, for example, specifically identifies such groups as a threat to national security in its 2020 National Security Strategy:

> "Technological development and the availability of new technologies are also leading to an increase in the influence of non-state actors that endanger security and are difficult to control within international security policy. They include organised crime syndicates, international terrorist organisations, cybercrime groups, extremist religious communities, private security contractors, certain non-governmental organisations, and other transnational networks. The possible interests and groups behind these organisations may be difficult to identify and could easily serve covert state intentions. This reshapes the security situation of certain regions and makes it confusing and difficult to assess, also representing a challenge for Hungary."[34]

The same is confirmed by a longer series of research launched in 2023 by the cybersecurity research group of the Ludovika University of Public Service, with the aim of providing the scientific basis for the new Hungarian National Cybersecurity Strategy. As part of the

[32] Kovács–Krasznay 2010.
[33] Gyurák 2024.
[34] Government of Hungary 2020.

research series, interviews were conducted with several leaders and commanders who lead cyber defence units in law enforcement and military organisations and are responsible for the cyber defence of critical infrastructures. In total, 8 commanders in national cyber defence and 6 critical infrastructure chief information security officers were interviewed, including some questions on the threat posed by hacktivist groups. The final and detailed results of this research are planned to be published later; however, the original data set is available for further study at the Institute of Cybersecurity of the Ludovika University of Public Service. According to the senior research panel of the Institute, the selection of the subjects represents the focus area in Hungary.

One question of the questionnaire asked respondents to rate Hungary's overall cyberspace exposure on a scale of 1 to 5. The average response was 3.19, i.e. medium exposure, with most respondents explaining that Hungary is currently of little geopolitical interest, with a significant proportion of attacks stemming from its membership of the EU and NATO. The next question asked respondents to name the three most serious threats that Hungary faces from cyberspace. A total of three respondents mentioned the Russian–Ukrainian war as a threat that should be considered from a strategic cyber defence perspective. One respondent directly mentioned the risk of hacktivist groups. Later, they were asked whether they considered hacktivist groups to be a strategic threat to Hungary's cybersecurity. All but one respondent agreed that the new Hungarian cybersecurity strategy should also address the threats posed by such groups. There was also broad agreement that, in general, geopolitical conflicts such as the war between Russia and Ukraine, plus the tension between Israel–Iran or U.S.–China have an impact on the country's cybersecurity.

As the vast majority of respondents have an ex officio right to comment on Hungarian cybersecurity regulations, their unanimous opinion supports my hypothesis that despite the country's apparent less exposure to hacktivist activity, the threat should be taken seriously. The same is true for other NATO member states, e.g. the Irish National Cyber Security Strategy mentions the threat posed by hacktivists to critical infrastructure and public systems, and the Portuguese strategy lists hacktivists among the strategic threats.[35] So, despite the momentary calm, countries' cyber defence organisations need to be ready for situations where large-scale distributed denial of service (DDoS) attacks or data thefts are suddenly launched. As these actions are prepared less covertly, it is not too difficult to obtain information about the attacks, sometimes from open-source intelligence, but this requires conscious monitoring of the hundreds of specific channels.

Conclusions

The two hypotheses of this research were confirmed in the present study. First, hacktivists and proxy groups have become irrevocably involved in armed conflicts. NATO member state adversaries routinely use these groups in their hybrid operations, even in ways that violate international law and are willing to use these groups in wartime as well. NATO

[35] Government of Ireland 2019; Government of Portugal 2019.

member states, including Hungary, see this as a strategic threat, even if they are little affected by the activities of these groups. On the other hand, it was also demonstrated that Western countries and democracies cannot afford to use hacktivists and proxies for several reasons, but learning from the example of Ukraine, it would be a big mistake to waste the openness and ability of thousands of people to participate in the defence of their country. As Sun Tzu wrote in *The Art of War,* "Thus the energy developed by good fighting men is as the momentum of a round stone rolled down a mountain thousands of feet in height. So much on the subject of energy."[36] The organised use of cyber volunteers can show tremendous energy in cyberspace operations without disrupting real covert operations.

Interviews with Hungarian cyber defence leaders have shown that even in Hungary, a NATO member state that is not under attack, hacktivists are taken seriously, and their activities are seen as a strategic threat. In two surveys repeated 14 years apart, we also saw that young non-professional cybersecurity experts are open to participating in cyber volunteering. While neither survey was representative, it is certainly indicative of the responsible leaders in military cyber defence. Further research could be conducted with a similar survey in other countries and a representative survey in Hungary to gauge the views of the roughly 10,000 cybersecurity professionals working in the field. As one of the results of this research, the author and his colleagues will come up with a legislative proposal that would allow the launch of a cyber volunteering scheme in the Hungarian legal environment, within the framework of the forthcoming Hungarian National Cybersecurity Strategy. As Ferenc Kölcsey, the author of Hungary's national anthem, wrote: "Homeland before all else!"

References

Ashdown, Neil (2024): Unity or Coherence: Shaping Future Civil–Military Intelligence Collaboration in the Cyber Domain. In Kwan, Claire – Lindström, Lauri – Giovanelli, Davide – Podiņš, Kārlis – Štrucl, Damjan (eds.): *CyCon 2024: Over the Horizon.* 16th International Conference on Cyber Conflict. Tallinn: NATO CCDCoE, 311–325. Online: https://doi.org/10.23919/CyCon62501.2024.10685631

Antoniuk, Daryna (2023): What's in a NoName? Researchers See a Lone-wolf DDoS Group. *The Record*, 4 September 2023. Online: https://therecord.media/noname-hacking-group-targets-ukraine-and-allies

Brewster, Thomas (2022): An 'Unhappy American' in the Russia–Ukraine Information War Promises a Huge Leak of Data Stolen from the Kremlin's Internet Censor. *Forbes,* 10 March 2022. Online: www.forbes.com/sites/thomasbrewster/2022/03/10/dddosecrets-in-the-russia-ukraine-information-war-promises-a-huge-leak-of-data-stolen-from-the-kremlins-internet-censor/

Chan, Kristy – Khaw, Joseph (2024): Not All Those Who Wander (Over the Horizon) Are Lost: The Applicability of Existing Paradigms of International Law to Cyberspace and the Interpretation of Customary International Law. In Kwan, Claire – Lindström,

[36] Sun Tzu 2006.

Lauri – Giovanelli, Davide – Podiņš, Kārlis – Štrucl, Damjan (eds.): *CyCon 2024: Over the Horizon.* 16th International Conference on Cyber Conflict. Tallinn: NATO CCDCoE, 177–190. Online: https://doi.org/10.23919/CyCon62501.2024.10685595

Cyberint Research Team (2023): *Behind the Mask of Anonymous Sudan: An Analysis.* Online: https://cyberint.com/blog/research/anonymous-sudan-an-analysis/

Cyberknow (2024): *CyberTracker Update 26. Russia–Ukraine War.* Online: https://cyberknow.substack.com/p/cybertracker-update-26-russia-ukraine

Fornusek, Martin (2024): Ministry: Ukrainian Hackers Disrupt Transport Services in Russian Cities. *The Kyiv Independent,* 13 March 2024. Online: https://kyivindependent.com/ministry-ukrainian-hackers-disrupt-payment-system-in-moscow-subway/

Fowler, Jeremiah (2022): *Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks against the Russian Government.* Online: www.websiteplanet.com/blog/anonymous-cyberwarfare-report/

Government of France (2018): *Paris Call for Trust and Security in Cyberspace.* Online: https://pariscall.international/en/principles

Government of Hungary (2020): *Government Resolution 1163/2020 (IV. 21.) on Hungary's National Security Strategy.* Online: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html

Government of Ireland (2019): *National Cyber Security Strategy.* Online: www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

Government of Portugal (2019): *Estratégia Nacional de Segurança do Ciberespaço 2019–2023.* Online: https://files.diariodarepublica.pt/1s/2019/06/10800/0288802895.pdf?lang=EN

Gyurák, Gábor (2024): *A katonai kibertér műveletek lehetséges kapcsolódási pontjai a Pécsi Tudományegyetem kibertérrel kapcsolatos kutatásaihoz.* Nemzetközi Katonai Kibertér Műveleti Konferencia, Szentendre, 7 March 2024.

Healey, Jason – Grinberg, Olivia (2022): *'Patriotic Hacking' Is No Exception.* Online: www.lawfaremedia.org/article/patriotic-hacking-no-exception

Jordan, Tim – Taylor, Paul A. (2004): *Hacktivism and Cyberwars. Rebels with a Cause?* London – New York: Routledge. Online: https://doi.org/10.4324/9780203490037

Karatzogianni, Athina (2015): *Firebrand Waves of Digital Activism 1994–2014. The Rise and Spread of Hacktivism and Cyberconflict.* London: Palgrave Macmillan. Online: https://doi.org/10.1057/9781137317933

Kim-McLeod, Riam (2024): Russia–Ukraine War: Telegram-based Hacktivism in 2023. *SecAlliance,* 27 February 2024. Online: www.secalliance.com/blog/russia-ukraine-war-telegram-based-hacktivism-in-2023

Kovács, László – Krasznay, Csaba (2010): A Digital Mohács. A Cyber Attack Scenario against Hungary. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 3(Special Issue), 49–59.

Koval, Nikolay (2015): Cyber War in Perspective: Russian Aggression against Ukraine. In Geers, Kenneth (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn: NATO CCDCoE, 55–58.

Lowe, Christian (2009): Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters*, 13 March 2009. Online: www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313/

Ottis, Rain (2008): *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: NATO CCDCoE. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Ottis, Rain (2011): *A Systematic Approach to Offensive Volunteer Cyber Militia.* Tallinn: TUT Press.

Romagna, Marco (2019): Hacktivism: Conceptualization, Techniques, and Historical View. In Holt, Thomas J. – Bossler, Adam M. (eds.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Cham: Springer, 1–27. Online: https://doi.org/10.1007/978-3-319-90307-1_34-1

Ruffin, Oxblood (2010): Hacktivism: From Here to There. *Threat Post*, 9 December 2010. Online: https://threatpost.com/hacktivism-here-there-120910/74759/

Sekoia TDR – Amaury G. – Maxime A. (2024): NoName057(16)'s DDoSia Project: 2024 Updates and Behavioural Shifts. *Sekoia*, 1 March 2024. Online: https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

Schmitt, Michael N. ed. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781316822524

Schmitt, Michael N. – Vihul, Liis (2014): Proxy Wars in Cyber Space: The Evolving International Law of Attribution. *Fletcher Security Review,* 1(2), 54–73.

Smith, Margaret W. – Dean, Thomas (2023): The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn: IEEE, 103–119. Online: https://doi.org/10.23919/CyCon58705.2023.10182061

Soesanto, Stefan (2022): The IT Army of Ukraine: Structure, Tasking, and Eco-System. *CSS Cyberdefense Reports*, June 2022. Online: https://doi.org/10.3929/ETHZ-B-000552293

Sun Tzu (2006): *The Art of War.* Minneapolis: Filiquarian Publishing.

Thøgersen, Marie (2023): Obligations of Non-participating States When Hackers on Their Territory Engage in Armed Conflicts. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn: IEEE, 39–54. Online: https://doi.org/10.23919/CyCon58705.2023.10182021

Turovsky, Daniil (2018): "It's Our Time to Serve the Motherland" How Russia's War in Georgia Sparked Moscow's Modern-day Recruitment of Criminal Hackers. *Meduza,* 7 August 2018. Online: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

UCMC (2016): Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations with his Russian Supervisor. *Ukraine Crisis Media Center,* 3 March 2016. Online: https://uacrisis.org/en/40837-sbu-3

United Nations General Assembly (2013): *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98.* New York: United Nations. Online: https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf?token=j2rtp8zdWwLTUkk6bu&fe=true

United States District Court for the District of Alaska (2017): *United States Versus Peter Yuryevich Levashov.* Online: www.justice.gov/opa/press-release/file/956511/dl

U.S. Department of Justice (2018): Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses. *Office of Public Affairs,* 12 September 2018. Online: www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

10.32565/aarms.2024.3.7

Competing Forums for Global Security Dialogue: The Munich Security Conference and the Minsk Conference post 2022

Szabolcs LÓRÁNT[1]

This paper examines the evolution of competing international security dialogue platforms through a comparative analysis of the Munich Security Conference (MSC) and the Minsk Conference (MC) during 2023–2024. Using Emanuel Adler and Michael Barnett's Security Communities framework and Charles Tilly's network configurations concept, it analyses how these forums represent distinct approaches to organising international security dialogue. The study demonstrates how the established MSC and the emerging Minsk Conference develop different institutional practices, governance structures and engagement patterns. While Munich emphasises multilateral engagement within a rules-based framework, Minsk promotes an alternative model centred on state sovereignty and Eurasian integration. This comparison reveals an emerging divide between Western and Eurasian approaches to international security dialogue, indicating a broader transformation in global security relations.

Keywords: *international security, security communities, Munich Security Conference, Minsk Conference, institutional competition, network configurations, multilateral dialogue, global security architecture, security forums, international relations*

Introduction

The global security environment has undergone significant changes in recent years, notably marked by the emergence of competing international security discussion forums. This evolution reflects broader transformations in the global power dynamics, where traditional Western-led frameworks increasingly face alternative structures and perspectives.

The coexistence and parallel development of the Munich Security Conference and the Minsk Conference exemplify this shift, illustrating a growing institutional competition in how international security dialogue is structured and conducted.

[1] Ludovika University of Public Service, Doctoral School of Military Science and Military Engineering, e-mail: lorant.szabolcs@stud.uni-nke.hu

This paper analyses these forums through the lens of institutional competition, examining how they operate as parallel dialogue-based security platforms. Both the Munich Security Conference and the Minsk Conference function as structured international dialogue mechanisms, though they represent competing visions for organising security discussions. This institutional competition manifests in their different approaches to multilateral engagement, regional focus and conceptualisation of international order.

As dialogue-based security platforms, both forums share key institutional characteristics: they function as recurring high-level meetings that facilitate multilateral security discussions, engage diverse international stakeholders and aim to shape global security discourse. This common institutional format enables a comparative analysis of how they develop competing approaches to international security dialogue.

These platforms represent an evolving form of multilateral cooperation that follows what Charles Tilly calls "network configurations" – distinct patterns of how international actors connect and interact.[2] Tilly's framework helps us understand how these forums create distinct patterns of interaction: Munich develops complex multilateral networks with multiple connecting points, while the Minsk builds more hierarchical relationships centred on state-to-state connections.

While traditional institutions rely on fixed structures, these security forums create more flexible networks of relationships. This networked approach, where participants can form various types of connections "across boundaries", may indicate how international cooperation could develop in the future. These forum-based interactions may increasingly supplement (or perhaps replace) traditional institutional structures.

The Security Communities framework provides the analytical structure for examining how these forums develop distinct governance patterns and shape security practices. This theoretical lens helps analyse how dialogue platforms establish shared understandings, build trust networks and develop collective identities. Through this framework, we can observe how network-based cooperation patterns emerge in international security dialogue, potentially indicating new forms of multilateral engagement.

In addition, these forums explicitly position themselves as actors shaping world order. The Munich Security Conference, founded in 1963, emphasises its global role through a Euro-Atlantic perspective, while the Minsk Conference, established in 2023, presents itself as a regional Eurasian platform. Their institutional philosophies reflect distinct cultural-historical traditions: Munich embodies Western multilateral traditions, while Minsk represents Eurasian approaches to international cooperation. Both platforms increasingly engage with Global South perspectives, indicating evolving dynamics in international security dialogue.

The present study examines how the Munich Security Conference and the Minsk Conference function as platforms that shape international security discourse and practices. Drawing on Emanuel Adler and Michael Barnett's (1998) framework for analysing security communities, this paper explores how these forums, while distinct from formal international institutions, serve as venues for the articulation and contestation of competing security perspectives.

[2] Adler–Barnett 1998: 403.

Specifically, it examines how the Munich Security Conference and the Minsk Conference represent and promote different views on global security architecture and what their development in the course of 2023 and 2024 indicates about changing dynamics in global security discussions.

This study identifies three key aspects to address this question:

First, the Munich Security Conference and the Minsk Conference demonstrate distinct security concepts and different approaches to international security. These forums operate similarly to what Adler and Barnett call "loosely coupled security communities" – platforms where participants develop shared understandings about security through regular dialogue and interaction.[3]

Second, the distinct formats of the Munich and Minsk conferences reflect fundamental differences in how they build what the security communities literature identifies as "many-sided and direct relations",[4] with Munich representing established Western frameworks while Minsk offers an alternative Eurasian-centred viewpoint.

Third, the development of the two parallel conferences reflects what Adler and Barnett describe as different "governance structures" that rely on "shared goals and intersubjective meanings" rather than formal enforcement mechanisms.[5]

These observations enable a multi-dimensional analysis of "institutional competition" among these forums. The Munich Security Conference prioritises transatlantic partnerships and the defence of a rules-based international order (RIO) increasingly with the ambition to engage with stakeholders globally. In contrast, the Minsk Conference emphasises Eurasian integration and advocates for an alternative security framework that directly challenges Western paradigms.

Importantly, as Adler and Barnett note, such communities can exist "in the absence of well-developed strategic ties or a formal alliance", but they develop through "tacit and/or formal normative prohibitions against states settling their disputes through military means".[6]

This study employs a comparative analysis of conference materials from 2023–2024, scrutinising both ex-ante materials (pre-conference reports) and ex-post documents (conference outcomes and summaries). This technique seeks to evaluate how different forums recognise security issues, engage participants and promote their unique perspectives on international order.

As global security challenges grow increasingly complex and interrelated, this analysis of rival institutional frameworks provides insights into the future direction of global security discussions and their implications for international order.

[3] Adler–Barnett 1998: 30.

[4] Adler–Barnett 1998: 31.

[5] Adler–Barnett 1998: 35–36.

[6] Adler–Barnett 1998: 35.

Historical context and evolution

The historical development of these forums illustrates how security dialogue platforms evolve through what Adler and Barnett term "phases of development"[7] – from nascent to mature stages of institutional formation.

Development of the Munich Security Conference

The Munich Security Conference was first held in 1963. In its early stages, the Conference served as a platform for Western defence officials and analysts. The primary aim was to align NATO members' defence policies and enhance transatlantic collaboration. During its six-decade span, the MSC has experienced a considerable evolution. It has evolved from a relatively small assembly of defence experts (often dubbed a "transatlantic family meeting") to the prime forum for dialogue on global security policy. The organisational framework of the MSC has become increasingly complex. Currently, it operates through an annual principal conference in February, as well as year-round initiatives like regional conferences, working groups and research initiatives. The conference functions as an independent organisation, adopting a public–private partnership framework, which has considerably expanded the range of its initiatives. Initially, the conference featured close to 60 attendees, primarily from NATO states, but it has now broadened its scope to nearly 1,000 participants from more than 100 countries.

The MSC's framework integrates a variety of stakeholders, bringing together viewpoints from both the private sector and civil society. While maintaining its core mission of strengthening the transatlantic alliance, the MSC has significantly expanded its objectives to include facilitating broader international security dialogues, promoting the rules-based global order and addressing global security challenges.[8]

The Munich Security Conference's evolution from 1963 to the present demonstrates the transformation of a security dialogue platform. Initially a small assembly of NATO defence experts, it has developed into the premier forum for global security policy discussions, expanding from 60 to nearly 1,000 participants from over 100 countries. This evolution reflects what Adler and Barnett identify as the development of "many-sided and direct relations" through increasingly complex institutional frameworks.

Emergence of the Minsk Conference

While the MSC represents the evolution of established Western security frameworks, the Minsk Conference emerged post-2014 as an alternative platform, illustrating how new security dialogue venues can develop in response to changing global dynamics.

[7] Adler–Barnett 1998: 30.
[8] Ischinger et al. 2014.

The Minsk International Security Conference was established in October 2023 to provide a Eurasian forum for security dialogue. While Belarus had previously hosted various international meetings since 2014, this conference marked a formal institutionalisation of its role in regional security discussions. The development has progressed through several critical phases: it transitioned from an emphasis on European security discussions to a more expansive Eurasian security framework, ultimately serving as a counter-platform to Western forums. The conference has further evolved from an initial dialogue platform to a more structured forum for developing alternative security architectures, as evidenced by its formalisation into an annual event with expanding participation from 30 countries in 2023 to over 40 countries and regions in 2024.

The Minsk Conference has its unique institutional characteristics, in particular, its annual high-level conference fundamentally reflects a state-centric approach. It sustains substantial connections with regional security groups, including the Collective Security Treaty Organisation (CSTO), the Shanghai Cooperation Organisation (SCO) and the Eurasian Economic Union (EAEU), while also participating in broader Eurasian projects.

The conference has also demonstrated growing alignment with wider non-Western initiatives, particularly China's Global Security Initiative (GSI), reinforcing its role in shaping alternative security frameworks.

The participation designs exhibit a distinctive orientation: attendees predominantly come from the Commonwealth of Independent States (CIS). Nonetheless, there has been a significant rise in both the size and scope of participation, including greater representation of Asian states and the Global South, along with selected engagement – from the geographic standpoint of Belarus – of Western countries such as Hungary. This broadened scope underscores a significant emphasis on "Global Majority" representation and comprehensive security, which includes military, political, economic and informational dimensions.

The strategic aims of the Minsk Conference present a divergent perspective from its Western counterpart. It advocates for a multipolar international order, contests Western security structures and fosters Eurasian integration. Furthermore, it establishes alternative security narratives, cultivates non-Western alliances and advocates viewpoints of the "Global Majority".

Parallel evolution 2023–2024

The timeframe of 2023–2024 represents an important phase in the development of both forums. The MSC has broadened its global engagement while maintaining a robust emphasis on transatlantic unity. Simultaneously, it has increased its focus on Global South perspectives. The Minsk Conference has at the same time reinforced its alternative security narrative, increased its emphasis on regional collaboration, expanded its participation base and solidified its anti-Western position. The Minsk Conference's transformation from a regional dialogue platform to a structured forum for alternative security architectures demonstrates how dialogue platforms can develop distinct "governance structures" based on different sets of "shared goals and intersubjective meanings".[9]

This comparative historical analysis illustrates the evolution of these forums from basic discussion platforms to a more structured manifestation of different perspectives on international security architecture. Their parallel development suggests broader changes in the global system and a growing challenge to Western-centric security frameworks.

Comparative analysis

While the historical context provides background understanding, this study focused specifically on 2023–2024, as this period offers the clearest evidence of dialogue competition between these forums. This timeframe captures both the Minsk Conference's emergence and Munich's strategic adaptation, providing rich comparative material for analysing competing approaches to security dialogue.

Institutional positioning and core narratives

The fundamental contrast between these forums emerged clearly in their self-positioning. The Minsk Conference established itself as an explicit "Eurasian alternative to the Munich Security Conference", as articulated by the CSTO Secretary General,[10] while Munich maintained its role as "the world's leading forum for debating international security policy".[11] This positioning reflects more than institutional rivalry – it demonstrates contrasting perspectives on how international security should be discussed and managed.

These contrasting institutional positions manifested in their different approaches to dialogue format.

Evolution of dialogue formats

Munich's Approach. The 2023 Munich Conference demonstrated its established multilateral format through unprecedented attendance and extensive bilateral engagement.

The conference facilitated 2,750 official bilateral meetings and hosted the largest bipartisan U.S. Congressional delegation in its history,[12] exemplifying its inclusive multilateral strategy.

The conference's focus on Western unity was evidenced by the first "G7 Foreign Ministers meeting in Munich under Japanese presidency".[13] This approach highlights

[9] Adler–Barnett 1998: 35.
[10] TASS 2024a.
[11] MSC 2023: 24.
[12] MSC 2023: 5, 19.
[13] MSC 2023: 5.

an “inclusive multilateral” strategy, aimed at enhancing current European security frameworks through comprehensive stakeholder participation.

Minsk’s Alternative Model. In contrast, the Minsk Conference developed a more selective, state-centric approach.

The Minsk Conference convened over 150 international attendees from 30 nations who participated in the discussions and approximately 300 delegates from Belarusian and foreign think tanks, and governmental bodies took part in the conference. Its format emphasised governmental participation and regional frameworks, with the Belarusian Foreign Minister, the conference host, articulating a direct challenge to Western frameworks: “West-centricity is a thing of the past, its place is taken by multipolarity.”[14] This argument not only challenges Western frameworks but also indicates the rise of alternative security frameworks, highlighting a profound structural divide in global security dialogue mechanisms. This position sharply challenges the assertions made by numerous participants at the Munich 2023 Conference, who consistently emphasised a rules-based international order grounded in transatlantic cooperation and liberal democratic principles.

The different dialogue formats reflect what Tilly identifies as contrasting network configurations: Munich’s approach creates multiple interconnected relationships (triadic connections), while Minsk’s state-centric model emphasises bilateral relationships (chain configurations).

The forums’ distinct formats evolved further as they adapted to changing global conditions.

Adaptation to global changes

Munich’s Strategic Evolution. Munich’s adaptation shows how established security forums can evolve their practices while maintaining their fundamental principles. Following Adler and Barnett’s concept of maturing security communities, the MSC demonstrates how security platforms can adjust to global changes while preserving their core values and expectations.

The 60th anniversary of the Munich Security Conference in 2024 featured significant developments in scale and scope, gathering nearly 1,000 participants, including 45 heads of state or government, from 109 nations across 60 sessions in the main program. Over half of the speakers were female, and more than a quarter were from the Global South.[15]

The conference theme “Lose–Lose?”, derived from the title of the event’s “scene-setter” report, reflected growing concerns about global fragmentation. Nonetheless, it also cultivated a sense of optimism for achieving outcomes, “seizing silver linings” among “dark clouds”, concentrating on pragmatic crisis management and inclusive dialogue.[16] This illustrates efforts to preserve the consistency of established European security

[14] Belarus MFA 2023a.

[15] Carr–Koenig 2024: 1.

[16] Carr–Koenig 2024: 4.

frameworks while recognising new threats to the current system. The revised strategy was apparent in the immediate response to significant incidents during the summit, such as Navalny's death and the taking of Avdiivka by Russian forces, which prompted urgent discussions and enabled the G7 Foreign Ministers to reiterate their "unwavering resolve to continue to support Ukraine".[17] The Conference also aimed at achieving concrete results, exemplified by "twenty technology firms signing an agreement to jointly prevent deceptive Artificial Intelligence content from interfering with global elections".[18]

Minsk's Alternative Vision. Minsk's emphasis on state sovereignty and regional frameworks illustrates what Adler and Barnett describe as the development of alternative "shared understandings" in security communities. Its approach represents the formation of distinct institutional practices that challenge established security dialogue norms.

The Second Minsk Conference reinforced its distinct approach through emphasis on state sovereignty and regional frameworks. Hungarian Foreign Minister Szijjártó's emphasis on "sovereignty as the key word today" exemplified the forum's alternative narrative approach to security dialogue.[19]

This attitude, demonstrated by various speakers in Minsk, which emphasises state-centric dialogue and regional frameworks, directly contests the post-Cold War European security architecture. This indicates not merely different formats but also conflicting perspectives on the conduct of European security discussions.

The Second Minsk Conference was remarkable for the presentation of divergent viewpoints, exemplified by Serbian Deputy Prime Minister Vulin's assertion that "the absolute lack of international law is the biggest problem in modern conditions".[20]

This sentiment was further reinforced in December 2024, when Russian Foreign Minister Lavrov announced that certain EU countries had expressed interest in the new Eurasian security framework proposed at the Minsk Conference. Lavrov emphasised that "the process of building a new architecture of security is moving forward full steam, and is already based not on the Euro-Atlantic concept". He attributed the need for this new architecture to what he described as the destruction of "indivisible security" proclaimed in the OSCE, "first and foremost, thanks to NATO's reckless eastward expansion".[21]

These divergent adaptations reflected each forum's broader approach to establishing their role in international security dialogue.

Institutional competition and legitimacy building

Both forums developed distinct strategies for building legitimacy. Munich expanded its scope while maintaining focus on European security frameworks, addressing "major challenges that disproportionately affect the Global South". Minsk built legitimacy through institutional coordination with regional organisations and direct challenges to Western

[17] Carr–Koenig 2024: 2.

[18] Carr–Koenig 2024: 4.

[19] Radio Svaboda 2024.

[20] Belarus Segodnya 2024.

[21] TASS 2024b.

paradigms, that is the rules-based international order and multilateral engagement model traditionally promoted by Western institutions.

This contrast is evident in their specific approaches to legitimacy-building. The "institutional rivalry" among the forums was evident in Munich's approach of increasing the range of involvement in the security dialogue, tackling what its organisers recognised as "the superlative number and breadth of crises and challenges".[22] This broadened scope, while keeping the focus on European security frameworks, illustrates Munich's effort to modify its established dialogue structure in response to growing global challenges, all the while preserving the core principles of the post-Cold War security order. This encompassed, among other topics, concentrated discussions on climate, water and food security, and technological problems, emphasising that "major challenges that disproportionately affect the Global South must be tackled".[23]

Minsk's strategy for dialogue and legitimacy is characterised by a focus on state-centric coordination and purposeful selective engagement. This emphasis underscores an important challenge to the Western security dialogue model, as it proposes an alternative framework that prioritises state sovereignty and regional power dynamics over multilateral cooperation. This is illustrated by the forum's organisational composition which underlines the need for governmental involvement, as noted by the Belarusian Foreign Minister who stressed the need for "holding a serious summit of heads of state of the Eurasian countries to discuss the future architecture of Eurasian security".[24]

The legitimacy of the Minsk forum has been supported by institutional coordination, demonstrated by the involvement of other regional organisations, including the CSTO, CICA and SCO. Furthermore, Serbian Deputy Prime Minister Vulin's assertion regarding the "complete absence of international law" and the necessity for "a new moral consensus"[25] further illustrates Minsk's strategy to establish legitimacy by directly challenging Western paradigms.

These different institutional practices demonstrate how Tilly's network configurations manifest in practice: Munich's "multilateral engagement" creates dense networks of interconnected relationships, while Minsk's "selective sovereign" approach builds more structured and hierarchical relationships between participants.

Narrative development and strategic positioning

The institutional competition between these forums manifested not only in their legitimacy-building approaches but also in their evolving narratives from 2023 to 2024.

The narrative development of the forums from 2023 to 2024 demonstrates their differing paths. In 2023, the dialogue in Munich predominantly emphasised robust Western solidarity, exemplified by the expression "as long as it takes" in its backing

[22] Carr–Koenig 2024: 1.
[23] Carr–Koenig 2024: 3.
[24] Belarus MFA 2023b.
[25] Belarus Segodnya 2024.

of Ukraine. This previous position showed a consensus-driven approach to European security, based on transatlantic cooperation and shared democratic principles. In 2024, Munich's discourse transitioned to facing uncertainties and various crises, as illustrated in its debrief paper about Western support for Ukraine amid "symptoms of fatigue and an increasing politicization of military and financial assistance".[26] This change implies not just practical issues but also fundamental questions regarding the sustainability of established European security arrangements in an increasingly multipolar world.

Meanwhile, Minsk changed its narrative focus from regional integration toward a more distinct alternative vision to RIO and a sharpened anti-Western sentiment, also with an increased adoption of the "Global Majority" viewpoints. This is exemplified by the statement of Sergei Lavrov, who explained that the current trend of the formation of a multipolar world order "promotes the democratization of international relations, in which there should be no hegemony of anyone and where the principles of the UN Charter should be observed in a comprehensive and not selective manner […], [and] that Russia's vision of Eurasian security corresponds to the [China's] GSI".[27]

The move from a regional platform to an alternative global dialogue forum, as illustrated by the CSTO Secretary General's clear view of Minsk as an alternative to Munich, poses a significant challenge to established European security frameworks and institutions.

The simultaneous development of these forums exemplifies not only competing institutional structures but also fundamentally divergent concepts of European and global security architecture. Munich aims to preserve and improve current global structures to address emerging challenges, whereas Minsk promotes a different model centred on state sovereignty and regional power relations. This increasing disparity indicates a significant structural divide in the conceptualisation, organisation and governance of international security, with substantial implications for the future of global security dialogue.

Conclusions

This analysis confirms our three key observations regarding the evolution of security dialogue platforms. The contrasting security concepts and approaches of Munich and Minsk demonstrate what Adler and Barnett describe as different types of "governance structures".[28] Munich's structure builds on multilateral engagement and Western institutional norms, guiding participants to work within a rules-based international framework. In contrast, Minsk's structure emphasises state sovereignty and regional power dynamics, encouraging participants to prioritise national interests and Eurasian integration.

The contrast between Munich's promotion of a "rules-based international order" and Minsk's support for "multipolarity" and "Global Majority" perspectives indicates fundamentally differing opinions on the organisation and governance of international security. In addition, they represent more than competing platforms – they exemplify

[26] Carr–Koenig 2024: 4.

[27] Xinhua 2024.

[28] Adler–Barnett 1998: 30.

different ways of constructing what Adler and Barnett term "shared identities, values, and meanings" in international security.

The forums' distinct approaches to security dialogue, particularly regarding European security, reflect fundamental differences in how they build – what the security communities literature identifies as – "many-sided and direct relations".[29] Munich's "inclusive multilateral" model emphasises extensive stakeholder engagement and transnational networks, while Minsk's "selective sovereign" approach prioritises state-level discussions and regional frameworks. This distinction goes beyond format and reflects competing visions of how European security discussions should be structured and maintained.

The parallel evolution of the conferences from 2023 to 2024 demonstrates how they developed different foundational principles to security dialogue. Munich's transformation from Western solidarity to acknowledging diverse global threats, alongside Minsk's development from a regional platform to an alternative global forum, shows how security dialogue platforms develop different sets of "shared goals and intersubjective meanings".[30] This competition between Munich and Minsk reveals how fundamentally different their visions are for organising and conducting international security dialogue.

This study points to emerging research directions regarding Global South/Global Majority influence in international security dialogue. While current demographics show numerical dominance of these regions, complex factors like China's declining fertility rates and aging population suggest future shifts in Global Majority dynamics.[31] The contrasting approaches of Munich and Minsk to Global South engagement reflect broader questions about evolving power distributions in international security discussions. Demographic transitions in key Global Majority countries may significantly impact future security dialogue configurations.

References

Adler, Emanuel – Barnett, Michael eds. (1998): *Security Communities.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9780511598661

Belarus MFA (2023a): Speech by the Minister of Foreign Affairs of Belarus S. Aleinik at the High-level International Conference "Eurasian Security: Reality and Prospects in a Transforming World". *Ministry of Foreign Affairs of the Republic of Belarus,* 26 October 2023. Online: https://mfa.gov.by/press/news_mfa/d7371731881f8f54.html

Belarus MFA (2023b): High-level International Conference "Eurasian Security: Reality and Prospects in a Transforming World". *Ministry of Foreign Affairs of the Republic of Belarus,* 27 October 2023. Online: https://mfa.gov.by/en/press/news_mfa/b96e0b311918963e.html

[29] Adler–Barnett 1998: 31.

[30] Adler–Barnett 1998: 35.

[31] Jiang 2024.

Belarus Segodnya (2024): Serbian Deputy PM: Absolute Lack of International Law Is the Biggest Problem in Modern Conditions. *Belarus Segodnya*, 31 October 2024. Online: www.sb.by/en/serbian-deputy-pm-absolute-lack-of-international-law-is-biggest-problem-in-modern-conditions.html

Carr, Randolf – Koenig, Nicole (2024): *Dark Clouds and Silver Linings. Key Takeaways from the Munich Security Conference 2024.* Debrief Paper, Munich Security Conference. Online: https://doi.org/10.47342/HIQV3321

Ischinger, Wolfgang – Stiftung Münchner Sicherheitskonferenz eds. (2014): *Towards Mutual Security. Fifty Years of Munich Security Conference.* Göttingen: Vandenhoeck & Ruprecht. Online: https://doi.org/10.13109/9783666300547

Jiang, Joyce (2024): China's One-child Policy Hangover: Scarred Women Dismiss Beijing's Pro-birth Agenda. *CNN*, 18 August 2024. Online: www.cnn.com/2024/08/18/china/china-one-child-policy-hangover-intl-hnk/index.html

MSC (2023): *Searching for a Common Vision. A Readout from the Munich Security Conference 2023.* Munich Security Conference. Online: https://doi.org/10.47342/JPRD3642

Radio Svaboda (2024): Сіярта ў Менску загаварыў па-расейску і выказаў спадзеў, што яго не асудзяць у Брусэлі. [Szijjártó spoke in Russian in Minsk and expressed hope that he would not be condemned in Brussels]. Radio Svaboda, 31 October 2024. Online: www.svaboda.org/a/33181768.html

TASS (2024a): Eurasian Security Conference in Minsk to Rival Munich Event – Moscow-led Bloc's Chief. *TASS Russian News Agency*, 1 July 2024. Online: https://tass.com/world/1810651

TASS (2024b): Slovakia, Hungary Intrigued by the Idea of a New Security Architecture for Eurasia – Lavrov. *TASS Russian News Agency*, 5 December 2024. Online: https://tass.com/politics/1882827

Xinhua (2024): Minsk Conference Focuses on Eurasian Security, World Multipolarity. *People's Daily Online*, 1 November 2024. Online: http://en.people.cn/n3/2024/1101/c90000-20236535.html

Contents