

Building a Legislative Framework for Securing Georgia's Strategic Assets¹

Archil Chochia

Department of Law
Tallinn University of Technology
Ehitajate tee 5
Tallinn 19086, Estonia
archil.chochia@taltech.ee

Shota Gvineria

Baltic Defence College
Riia 12
Tartu 51010, Estonia

Economic Policy Research Center
Paliashvili 85
Tbilisi 0162, Georgia
shota.gvineria@baltdefcol.org

Holger Mölder

Department of Law
Tallinn University of Technology
Ehitajate tee 5
Tallinn 19086, Estonia
holger.molder@taltech.ee

Abstract: The article discusses the importance of modernizing and securing critical infrastructure in Georgia, particularly within the context of its geopolitical position and evolving economic landscape, by building an appropriate legal framework. The article outlines the significant impact of cyberspace on traditional sectors such as energy, transportation, and telecommunications, necessitating a re-evaluation of critical infrastructure in the digital age. Highlighting Georgia's aspirations to align with European

¹ The research was carried out in the framework of the project 'Building a Legislative Framework for Securing Georgia's Strategic Assets,' funded by the Estonian Centre for International Development (ESTDEV) (project no. 116-2021-A).

and Euro-Atlantic structures for enhanced national security and democratization, the study emphasizes the need for regulatory and legislative frameworks that would be compatible with EU standards. Drawing on a comparative analysis between Estonia and Georgia, the research identifies gaps and areas for improvement in Georgia's critical infrastructure protection (CIP) system. Through the examination of Estonia's successful transformation from a Soviet-era environment to a robust EU-compatible CIP system, the study offers recommendations tailored to Georgia's context.

Keywords: *CIP systems, critical infrastructure, Estonia, Georgia, Georgian legal system*

1. Critical infrastructure and its legal protection: An introduction

Critical infrastructure (CI) refers to assets, systems, or their essential components that are crucial for sustaining the key functions necessary for the health, safety, security, economic stability, or social well-being of a population. A disruption or destruction of such an infrastructure would result in significant consequences, impeding the ability to maintain these vital functions and affecting the overall resilience of society (Pursiainen, 2009). Potential threats to these infrastructures include physical and cyber threats, natural disasters, technological failures, human error, and terrorism (Osei-Kyei *et al.*, 2021). Physical threats refer to direct attacks on infrastructure facilities and could involve sabotage, terrorism, or acts of war that physically damage or destroy infrastructure components (Rehak, Hromada & Lovecek, 2020). With the growing reliance of critical infrastructures on information and communication technologies, cyber threats are increasingly susceptible to cyber attacks. These attacks, which might involve hacking, viruses, and other cyber intrusions, have the potential to disrupt service delivery or compromise sensitive data, threatening the operational integrity of these infrastructures (Wilson, 2014). Natural disasters, such as earthquakes, floods, hurricanes, and other severe weather conditions, are events that pose significant risks to infrastructure. These natural events can cause extensive damage to physical structures and disrupt essential services (Kadri, Birregah & Châtelet, 2014). Technological failures, such as breakdowns or malfunctions of critical components, refer to errors within the infrastructure

itself and can lead to cascading effects that compromise the functionality of interconnected systems and services (Pursiainen, 2009). Human errors are the mistakes made during the operation, maintenance, or management of critical infrastructures that can result in disruptions or accidents, impacting the delivery of essential services (Ghafir *et al.*, 2018). Finally, targeted attacks against critical infrastructure, either by terrorist groups or hybrid attacks from hostile countries, are designed to cause maximum disruption and instil fear in the population. These attacks are a major concern, particularly for infrastructures that are symbolic or have a significant impact on national security or public safety (Yao *et al.*, 2020).

To safeguard critical infrastructures from these diverse threats, governments and regulatory bodies have implemented a range of protective measures and frameworks. Regulation plays a crucial role in ensuring the resilience and security of these vital systems. This includes establishing standards and guidelines that dictate the minimum-security measures required to protect infrastructures from physical, cyber, and natural threats (Wiater, 2015; Karabacak, Ozkan Yildirim & Baykal, 2016). At the European Union (EU) level, for example, these are the European Critical Infrastructure (ECI) Directive (Council Directive 2008/114/EC), the Critical Infrastructure Protection (CIP) Framework, the Critical Information Infrastructure Protection (CIIP), and the Network and Information Security (NIS) Directive (Chochliouros *et al.*, 2015). Directive 2008/114/EC establishes a procedure for identifying and designating ECIs across the EU. It initially focused on the energy and transport sectors (Keypour, Kerikmäe & Chochia, 2023), but was open to expansion to other sectors, such as information and communications technology (ICT) (Mazur & Chochia, 2022). The Directive mandates that Member States ensure adequate protection of the designated ECIs, which has an impact on national legislation and regulatory frameworks (Lindström & Olsson, 2009). The EU's CIP framework is designed to enhance the protection capabilities against various hazards across all EU Member States, including developing capabilities to prepare for, protect against, respond to, and recover from disruptions or destruction of critical infrastructure (Bossong, 2014). The CIIP focuses on protecting the ICT systems that are critical infrastructures themselves or that are essential for the operation of other critical infrastructures, involving protection programs and activities by infrastructure owners, operators, and regulatory bodies to maintain performance and minimize recovery time and damages from failures or attacks (Tiirmaa-Klaar, 2016). Finally, the NIS Directive aims to raise the overall level of cybersecurity in the EU by requiring Member States

to boost their national IT security capabilities, improve cooperation, and ensure that operators of essential services and digital service providers take adequate security measures and report serious incidents (Markopoulou, Papakonstantinou & de Hert, 2019).

2. Critical infrastructure in Georgia

Georgia's geopolitical location and its historic connectivity between Eastern and Western markets have always been the driving force behind the country's economic development (Kerikmäe & Chochia, 2016). Georgia's pivotal geostrategic location serves a unique transit function, as a remarkable part of the world's oil production flows through the country's territory via pipeline connections with Armenia, Azerbaijan, Russia, and Turkey (Gvelesiani & Mölder, 2018, pp. 139–140). Also, the emergence of cyberspace as a new economic domain has heavily affected operations in energy, transportation, telecommunications, and other sectors traditionally related to strategic infrastructure, where the digital economy is taking over many strategically important sectors. Accordingly, critical infrastructure is also reshaping in form (Lazari & Tabagua, 2024).

According to the National Security Concept (2011), Georgia aspires to become part of European and Euro-Atlantic structures, which will enable the country to consolidate its democratization process and strengthen its national security. The EU defines critical infrastructures as structures that influence the functioning of the health, safety, security, economic and social well-being of the people, the damage or destruction of which would significantly affect the country (Council Directive 2008/114/EC). This report adopts the EU's official definition of the term:

Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. (Council Directive 2008/114/EC)

The first indispensable step towards modernizing Georgia's CIP system is to introduce regulatory principles and legislative framework for the identification and protection of the country's critical infrastructure,

conforming to EU principles and standards. To this end, from September 1, 2020 to August 31, 2022, TalTech Law School of Tallinn University of Technology, in cooperation with the Economic Policy Research Centre (Georgia) and Tbilisi State University Law School, implemented the project 'Building a Legislative Framework for Securing Georgia's Strategic Assets' (project no. 116-2021-A), funded by the Estonian Centre for International Development (ESTDEV). "Creating a model of governance that provides for the sustainable development of the country's democratic political system" is outlined as one of the main national interests for Georgia in the government's 2030 Development Strategy (n.d.). Moreover, the current Development Strategy of the Government of Georgia specifically highlights the development of infrastructure and full use of its transit potential as the key strategic priority. Securing critical infrastructure and key assets is particularly important for Georgia as the country aspires to be a regional hub with a highly open economic structure and free trade regimes with key economic players, including the EU, China, Turkey, and the Commonwealth of Independent States (CIS) countries. Georgia is still struggling with the modernization and digitalization of its critical infrastructure. The issue of protecting strategic assets has become even more relevant for Georgia being exposed to Russia's hybrid warfare (Mölder *et al.*, 2021; Napetvaridze & Chochia, 2019) and coercion, especially against the backdrop of Russia's unprovoked and illegal aggression against Ukraine.²

The research team examined and assessed national-level conceptual documents on issues of defence and security in Estonia, as well as conceptual documents and legislative and regulatory papers related to defining, managing, and protecting CI. All sections in the conceptual documents as well as in the legislative and regulatory papers that address CIP were used in developing the comparative data framework for the case study analysis. A comparative analysis of the best practices of Estonia and Georgia's policy and legislative framework helped to identify potential gaps and areas for improvement. On the basis of the content and data analysis and given its strong democratic governance, robust CIP system, and commonalities with Georgia in security environment and threat levels, Estonia was chosen as the successful model, having transformed its system from the Soviet-era environment to the EU-compatible CIP system. Consequently, the research team learned from the best practices of Estonia's CIP model and, analyzing contextual similarities and differences, developed adequate recommendations for Georgia.

² On Russia's war against Ukraine and the relevant aspects for Georgian case study, please see Sayapin and Tsybulenko, 2018; Tsybulenko and Kajander, 2021; 2022; Tsybulenko, 2022; Tsybulenko and Platonova, 2022; Tsybulenko and Rinta-Pollari, 2023.

First, the full hierarchy of Estonian conceptual and policy documentation was analyzed to define relevant criteria for the adequate identification of critical infrastructure whose disruption or destruction would have a significant impact on national security. Second, Estonia's legal and regulatory framework was studied to identify specific procedures and requirements for the protection of Estonia's critical infrastructure. Most importantly, a series of interviews were conducted with experts involved in developing and managing Estonia's CIP system from both government and civil society perspectives. This component of research was crucial for understanding the practical aspects of Estonia's CIP system and tailoring Estonia's approaches to the Georgian context.

The project team also carried out a thorough analysis of the existing Georgian CIP policy and legislative frameworks. A number of documents were analyzed and a series of interviews conducted with the representatives of Georgia's executive and legislative bodies responsible for defence and security. Finally, based on the comparative empirical analysis of Georgia's and Estonia's CIP policies and legal frameworks, potential solutions have been proposed for fixing the identified gaps in the current Georgian CIP model.

3. Lessons learned from the Estonian case study

Estonia has developed a vast legislative and regulatory framework that manifests the country's approach to national security, crisis management, and the protection of critical infrastructure and continuity of vital services. In today's turbulent and ever-changing security environment, Estonia is constantly adapting to a wide range of threats and challenges, including extreme weather conditions, an increasing risk of accidents, epidemics, disturbances, migration, and armed attacks with outbreaks of violence, among others. Estonia applies the modern approach of comprehensive national defence, according to which both military and non-military fields must be involved in enabling an efficient national defence, and in order to deal with possible non-military and military security threats, all state institutions and the whole society must be prepared to defend the country. Security threats involving various non-military domains play a major role in the current security picture, which is why successful prevention of crises and conflicts requires countering them with speed and specialization (National Defence Development Plan 2017–2026, 2017, p. 5).

Estonia has been a member of the North-Atlantic Treaty Organization (NATO) since March 29, 2004, and a member of the EU since May 1, 2004. During the pre-accession period as a candidate country, Estonia adopted 31 chapters of the EU's *Acquis Communautaire* and fulfilled the membership criteria set forth by the NATO's Membership Action Plan (MAP). Both international organizations have developed a number of CIP-related policies, which have had a normative, institutional, and organizational impact on the development of the national (domestic) system over the last two decades.

3.1 Relevant conceptual and legal documents

The National Security Concept of Estonia establishes the objectives, principles, and directions of the security policy and will be revised or amended depending on changes in the security environment and the development of measures for ensuring Estonia's security. The Concept was adopted by the Parliament (Riigikogu) in 2017 and amended in 2023 (Parliament of Estonia, 2023). The National Security Concept (2023) constitutes a framework document which forms the basis for the preparation of specific development and action plans.

The National Defence Act establishes a legal framework for an efficient response to threats endangering the country, as a need arises. The Act serves as the basis for the implementation of the national defence architecture.

The Foreign Investment Reliability Assessment Act was adopted by Riigikogu on January 25, 2023. The primary objective of the Act is to screen direct and indirect investments of non-EU investors in strategically sensitive areas (i.e., electricity supply, natural gas supply, liquid fuel supply, ensuring the operability of national and local roads, phone and mobile phone services, data transmission services, digital identification and digital signing, emergency care services, payment and cash circulation services, district heating, water supply and sewerage; national television or radio broadcasting services, and other media services with a turnover of at least 3 million euros; geological exploration; railway, seaports, and aerodromes; supply of military goods and/or dual-use items, or technical assistance related to it, etc.) in Estonia. Similar laws have been passed in Germany, Finland, and Latvia. The Estonian Consumer Protection and Technical Regulatory Authority has the authority to clear investments before transactions.

Most importantly, **the Emergency Act**, passed by Riigikogu on February 8, 2017, lays down the principal frameworks for preparing for and resolving

emergencies and ensuring the continuity of vital services in the event of civil emergencies. According to the definition proposed in the referred Act, an emergency is an event or a chain of events that threatens the life or health of many people, causes major property damage or major environmental damage, and requires rapid coordinated action of several agencies to solve it (Emergency Act, Art. 2(1)). The amendment to the Emergency Act, adopted by Riigikogu on June 2, 2021, established the State's Operation Stockpile to manage the stockpiling and storage of vital goods needed in emergencies (Emergency Act, Art. 18). Several coordinating tasks of the Ministry of the Interior are assigned to the Government and the State Chancellery.

Finally, to reflect the changing dynamics in strategic security environment, the **Civil Crisis and National Defence Act** is expected to be passed by Riigikogu in 2024. It should replace the National Defence Act and does not differentiate between peacetime and wartime, which makes it a less legally binding and more flexible approach. The new Act addresses preparation for crisis situations, emergency situations, state of emergency and martial law, among others, and national crisis resolution under a unified management. It is intended to replace current national defence and emergency situations tasks to prepare for both civil and national defence crises. The government, executive state authorities, providers of vital services, and local governments prepare their own crisis plans based on a nationwide risk analysis (National Risk Analysis, n.d.).

Notably, the legislative initiatives are guided and adhere to good practices. The Guidelines for Ministers and their Advisors to Avoid Conflicts of Interest and the Good Practice in Communicating with Lobbyists for Officials includes a collection of ethical principles for ministers and their advisors, which help avoid the realisation of conflicts of interest. Good practices in communicating with lobbyists increase the transparency and clarity of legislative drafting, making the publishing of at least quarterly reports on meetings with lobbyists mandatory.

4. Regulatory and strategic approach

The term 'critical infrastructure' is not defined in the Estonian legislation; however, the draft of the new Civil Crisis and National Defence Act will divide critical assets and services in two categories: vital services (which assume stronger security requirements) and services with permanent crisis task (which assume softer security requirements) (Latvian Institute of International Affairs, 2021). The combination of the assets and services in both groups, in essence, constitutes Estonia's critical infrastructure list. Based on this draft law, in times of crisis, the government could include additional services into the list and assign temporary crisis task to the companies and individuals that do not have those duties under existing legislation.

According to Estonia's approach, critical infrastructures consist of those physical and information technology facilities, networks, services, and resources whose disruption or destruction significantly impacts the health, safety, security, or economic well-being of citizens or affects the efficient functioning of the national government (Tropp, Hoffmann & Chochia, 2022). Critical infrastructure covers various economic sectors, as well as key services within sectors designated by laws. Some of the critical elements of critical infrastructure sectors are not strictly 'infrastructure,' but are, in fact, networks or supply chains that support the distribution of vital products or services. For example, the supply of food or water in larger urban areas depends on certain key facilities, but also on a complex network of producers, processors, distributors, and retailers (Communication COM(2004) 702).

In the Estonian Emergency Act, the sectors covering the majority of the critical infrastructure and vital services are the following:

- Energy installations and networks: electricity, oil and gas production, storage and processing plants, transmission and distribution systems;
- Communication and information technology: telecommunications, transmission systems, software, hardware and networks, including the internet;
- Finance: banking, securities, and investments;
- Healthcare: hospitals, health and blood supply facilities, laboratories and medicines, search, rescue and ambulance services;
- Food: safety, means of production, wholesale and food industry;
- Water: dams, storage, treatment and nets;

- Transport: airports, ports, intermodal facilities, rail and mass transit networks, traffic control systems;
- Production, storage and transport of dangerous goods: chemical, biological, radiological and nuclear materials;
- Government: critical services, facilities, information networks, resources and national key sites and monuments.

According to the draft of the new Civil Crisis and National Defence Act, a vital service is defined as follows: (a) a service that has an overwhelming impact on the functioning of society, (b) the interruption of which directly threatens the life or health of people or another vital service or the operation of a service of general interest or causes great environmental damage, and (c) the interruption of which has a significant impact on the national economy and national defence. Below is a list of vital services and permanent crisis tasks assigned to providers in each area.

- Operation of payment services: banks;
- Operation of cash circulation and cash handling: banks;
- Provision of district heating: operators have service agreements with local municipalities;
- Ensuring the drivability of local roads: road maintenance companies have service agreements with local municipalities;
- Water supply and sewerage operation: operators have service agreements with local municipalities;
- Provision of food: larger food producers;
- Operation of healthcare services: 20 national/regional/county hospitals, but not all hospitals;
- Electricity supply: the transmission system operator and larger distribution system operators;
- Natural gas supply: the transmission system operator and larger distribution system operators;
- Liquid fuel supply: larger terminals and gas station operators;
- Ensuring the drivability of national roads: road maintenance companies have service agreements with the National Transport Board;
- Operation of telephone services: 3 telecom companies;
- Operation of mobile phone services: 3 telecom companies;
- Operation of the data communication services: 3 telecom companies;
- Operation of airfields: larger airports, international flights;
- Operation of air navigation service: the national air navigation company;
- Operation of public railways: the national railway operator;

- Operation of railway transport: the national railway transport company;
- Operation of ports: larger ports;
- Electronic identification, authentication, and digital signing: eID service operator;
- Provision of medicines: larger operators of drug warehouses;
- Provision of security services: security companies who have service agreements with other vital service providers.

The following plans and processes are put in place to ensure the security of Estonia's vital services:

- The Digital Society Development Plan 2030 outlines the key participants' shared principles, development trends, and operational objectives and lines of action in the field of digital governance, cybersecurity, and connectivity.
- The Transport and Mobility Development Plan for 2021–2035 aims at making the transport system safer and more sustainable and more attuned to the strategic development of mobility.
- The National Energy Sector Development Plan focuses on local renewable energy production and increasing energy efficiency while also ensuring Estonia's energy security.

A two-year revision and discussions of a broad-based expert committee resulted in the draft legislation amending the Local Government Organization Act, one of the central aims of which is to extend the local government's right to self-organize the protection of critical infrastructure. As part of simplifying the process of transferring land to local governments, the government agreed on common land policy principles and initiated the preparations for amending the State Assets Act and the Land Reform Act, which aim to accelerate the process of transferring land and make it more flexible.

5. Critical information infrastructure protection (CIIP)

State information security and cybersecurity form a special dimension within the broader security system for critical infrastructure and vital services. The task of the critical information infrastructure protection (CIIP) is to ensure that the network and information systems important to society operate smoothly. The Information System Authority (RIA) organizes the protection of network and information systems used for the provision of services important for the functioning of society at the national level. In 2009, the RIA established the Department of Critical Information Infrastructure Protection (KIIK) as part of its structure. The task of the department is to create and maintain Estonia's critical information infrastructure protection system.

The main legal instruments of CIIP are the **Cybersecurity Act** and the **Digital Society Development Plan 2030**. Services important for the preservation of social and economic activities are defined in Article 3 of the Cybersecurity Act.

The fundamental principles of the **Estonian Cyber Strategy** are:

- We consider the protection and promotion of the fundamental rights and freedoms on the internet as important as in the physical environment.
- We treat cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis of the country's socioeconomic development. Cybersecurity must support innovation and innovation security.
- We acknowledge that ensuring the security of cryptographic solutions is uniquely important for Estonia, as the entire ecosystem of our digital country is based on it.
- The functioning of the digital state is based on transparency and public trust and to maintain this, we adhere to the principle of open communication by the state.

The distribution of tasks between the public and private sectors is as follows:

The responsibilities of state agencies

- Shaping the ecosystem: legislation, policies, frameworks, and preparation of instructions;
- Providing competent information on current cyber threats and vulnerabilities;

- Involving the private sector in its activities;
- Organizing information events for private enterprises and state agencies;
- Creating and managing an informal network.

The responsibilities of the private sector

- Protecting business processes and systems;
- Providing sustainable services to society;
- Complying with the national requirements and best international practices;
- Participating in cooperation networks with public sector and state agencies.

Besides the general description of functions, there are specific security requirements that providers of vital services identified under the Emergency Act and the Cybersecurity Act are obliged to fulfil in various spheres, such as telecommunications operators, electricity network operators, natural gas operators, and state roads.

Table 1 expounds the sectors that constitute the critical infrastructure and vital services in Estonia, their tasks, and the obligatory requirements they must fulfill to ensure the stable and uninterrupted functioning of their respective sectors.

Table 1. Sectors that constitute the critical infrastructure and vital services in Estonia, their tasks and obligations.

Sector	Services / Tasks	Stakeholders	Requirements / Criteria
Finance	Operation of payment services (the permanent crisis task is to ensure the operation of payment systems).	Banks – Eesti Pank	A credit institution established in Estonia, or a branch of a foreign credit institution established in Estonia, is the vital service provider specified in Article 3 of the Credit Institutions Act, which determines the frames applicable to the vital service providers in the banking domain. The list of the vital services is approved by Eesti Pank (the national bank).
	Operation of cash circulation and cash handling (the permanent crisis task is to issue cash and ensure a sufficient cash reserve).	Banks – Eesti Pank	
Energy	Provision of district heating	Operators have service agreements with local municipalities (the permanent task is to ensure a certain quantity for heat production with the possibility of using reserve fuel, to ensure heat supply for seven days).	A heating provider whose estimated annual production volume is at least 10,000 MWh per network area
	Electricity supply	The state authority transmission system operator and larger distribution system operators	A producer whose power plant has a net capacity exceeding 200 MW; a line owner, whose transmission capacity of the power line crossing the state border exceeds 100 MW; a network operator with more than 5,000 consumers connected to the distribution network.
	Natural gas supply	The transmission system operator and larger distribution system operators	An enterprise that provides transmission services in the gas network; An entrepreneur with more than 1,000 consumers connected to the distribution network.
	Liquid fuel supply	Larger terminals and gas station operators	A fuel seller who has ten or more gas stations and whose gas stations are located in at least three locations in the county. A person holding an excise warehouse license who allows liquid fuel for domestic consumption.

Transport	Ensuring the drivability of local roads	Road maintenance companies have service agreements with local municipalities	
	Ensuring the drivability of national roads	Road maintenance companies have service agreements with the National Transport Board	
	Operation of airfields	Larger airports, international airlines. The civil air traffic service and air navigation service provider in the Tallinn flight information area. The airport operator, which operates Tallinn and Pärnu airports.	A service provider who provides ground service listed in the Annex to Council Directive 96/67/EC handling services, with the exception of catering services, to an airport providing vital services to the operator on the basis of the ground service contract, the permanent crisis task is to ensure the service (Civil Crisis and National Defence Act, Art. 73(15) and (16)).
	Operation of air navigation services	The national air navigation company (the permanent crisis assignment is to ensure service provision in accordance with the Emergency Act (Art. 71)).	An aviation security service provider who ensures the application of aviation security measures on the basis of a contract concluded with an airport operator providing a vital service
	Operation of public railways	The national railway operator (the permanent crisis task of a railway performing public passenger transport is to organize service in accordance with the provisions of subsection 1 of this section).	
	Operation of railway transport	The national railway transport company	A railway infrastructure manager to manage the public railway infrastructure is the vital service provider specified in the Civil Crisis and National Defence Act (Art. 73 (3(17))).
	Operation of ports (the permanent crisis task of the ice-breaking service provider is to ensure ice-breaking during the ice-breaking period in local service area in accordance with the contract concluded with the Transport Board).	The port operator who loads and unloads container and rolling stock in a port used for the provision of a vital service. (Art. 31 of this Act approved on the basis of paragraph 2)	An entrepreneur is a vital service provider as defined in the Civil Crisis and National Defence Act if the interruption or termination of its economic activity will have a significant impact on the population food supply, including in the case of a single industry or food. The port manager is specified in the Civil Crisis and National Defence Act (Art. 73 (3(19))) as provider of a vital service if at least one of the following conditions is met: 1) the operation of its port affects the continuity of another vital service or national defence guarantee; 2) the number of passengers passing through its port constitutes a significant part of international passengers in Estonia; 3) the volume of goods transported through its port constitutes a significant part of ports in Estonia of the total volume of goods transported.

Food and water	Water supply and sewerage operation	The operators have service agreements with local municipalities	
	Provision of food	Large food producing companies	The fields of food supply security are defined as: 1) production of cereal, bakery, or pasta products; 2) keeping animals for the purpose of meat or milk production; 3) meat handling; 4) milk handling; 5) food retail trade
Healthcare	Operation of healthcare services	National/regional/county hospitals—20 selected hospitals (not all hospitals)	
	Provision of medicines	Larger operators of drug warehouses—a permanent holder of a license to wholesale pharmaceuticals crisis task	
Communications and information	Operation of telephone services	3 larger telecom companies	
	Operation of mobile phone services	3 larger telecom companies	
	Operation of data and electronic communication services (the permanent crisis task is to ensure at least one radio and television program in Estonian and one in Russian with round-the-clock production and access to a communications company).	The broadcasting network service is an electronic communication provided via a broadcasting network to make media services available to the public	Broadcasters that ensure round-the-clock production and access to web-based news in Estonian to a communications company; Broadcasters that ensure readiness for transmission of radio programs, specified in point 2 of this paragraph, to the communication network of the communication company providing broadcasting network service from at least three locations, including from at least two locations outside Tallinn, and access to a communications company to online news from at least two locations, including one location outside of Tallinn.
Digital governance	Electronic identification, authentication, and digital signing	The eID service operator	
Other	Security service provision	Security companies, who have service agreements with a vital service provider.	A security company that permanently provides security services to a vital service provider to ensure the continuity of the service, or one with whom the provision of the security service is a vital service to ensure business continuity, agreed upon in the business continuity plan of the vital service provider, is the vital service provider specified in the Civil Crisis and National Defence Act (Art. 73 (3 (2))).

6. Critical infrastructure protection system in Georgia

At present, the main regulatory acts addressing issues related to national security and defence in Georgia are: 'On Defence of Georgia,' 'On Defence Planning,' 'On Civil Security,' 'On the State Security Service of Georgia,' 'On the Rules for Planning and Coordination of National Security Policy,' and Laws of Georgia 'On Information Security.' Three main problems have been identified as key areas where Georgia needs to be insistent in order to adapt its CIP system to the needs of the modern security environment.

First, critical infrastructure is not adequately identified, protected, or even defined in the national legislation. Due to the uncertainty stemming from the lack of regulations, there is a high risk that politically motivated direct foreign investments from unfriendly countries could gain control over some strategic assets. In order to mitigate risks and encourage further assurances for the access of reliable investors, it is crucial for Georgia to develop a system of requirements and standards that would be compatible with relevant EU practices. This would facilitate the establishment of democratic policies and a legal framework that generate more opportunities for the flow of direct foreign investments, businesses, and innovation.

Second, in Georgia, as in most Western democratic countries, the majority of critically important services are located in the private sector. These strategic fields include energy and water supply, the banking and financial sector, food safety, chemical and military industries, the medical sector, and others. Consequently, the private sector is intensively involved in the maintenance of critical infrastructure. However, contrary to the Western models, only state-owned assets currently qualify as critical infrastructure objects in Georgia. The current Georgian legislation ignores the fact that private businesses own and manage critical infrastructure assets, whose proper functioning is vital for the state and society.

Third, the national security concept of Georgia recognizes that the security of cyberspace and the protection of electronic information is very important for the country: "As information technologies rapidly evolve, critical infrastructure is becoming increasingly dependent on them. Therefore, combating cybercrime and protecting against cyber attacks is very important to the national interests of Georgia" (National Security Concept, 2023). Therefore, the paradigm for identifying critical infrastructure should be fundamentally reviewed and brought in line with Georgia's Europeanization agenda.

7. Information security

The critical information infrastructure is the most successfully developed aspect of Georgia's CIP system and is regulated by the Law of Georgia 'On Information Security.' The Law defines the rights and obligations of the public and private sectors in the field of information security protection, as well as the state control mechanisms for the implementation of the information security policy.

The Law of Georgia 'On Information Security' includes the definition of a 'critical information system entity' and defines it as an organization whose continuous operation of the information system is important for the defence and/or economic security of the country, the maintenance of state governance and/or public life. Three categories of critical information systems entities are distinguished:

- Subjects of *the first category* include state bodies, institutions, legal entities under public law, state enterprises, whose continuous operation of the information system is important for the defence and/or economic security of the country, for the maintenance of state power and/or public life;
- Subjects of *the second category* include electronic communications companies, whose continuous operation of the information system is important for the defence and/or economic security of the country, for the maintenance of the state government and/or public life;
- Subjects of *the third category* include legal entities of private law, which are not electronic communication companies, but whose continuous operation of the information system is important for the defence and/or economic security of the country, for the maintenance of the state government and/or public life.

The specific list of entities belonging to the above categories is approved by Resolution no. 646 of the Government of Georgia, dated December 31, 2021.

According to the Law of Georgia 'On Information Security,' all categories of information system entities are obliged to appoint an information security manager. (The minimum standards for the information security manager of critical information systems entities of the first and second categories are established by the Decree of the Head of the Operational-Technical Agency of the State Security Service of Georgia no. 12 of May 3, 2022.) The manager must meet the following requirements: (a) have at least three years

of working experience in information technology, management or project management; (b) have the International Organization for Standardization (ISO), the British Institute for Standardization (BSI), the Information Systems Audit and Control Association (ISACA), a valid certificate in the field of information security issued by the International Consortium for Information Systems Security Certification (ISC) or SANS (GIAC) Institute; and (c) must have access to state secrets.

The main duties of the information security manager are: daily monitoring of the fulfillment of information security policy requirements; describing informational assets and their access; preparing internal documentation of information security policy; collecting information about information security incidents and monitoring the response to them; reporting on information security issues and other administrative/organizational activities; organizing and conducting general and sectoral information security trainings; other duties determined by the subject of the critical information system.

In addition, the first and second category entities are coordinated by the Operational-Technical Agency of the State of Georgia, while the third category entities are coordinated by the Digital Governance Agency of the Ministry of Justice.

According to the law 'On Information Security,' the subject of the critical information system is obliged to adopt the rules of internal use of information security, which serve to enforce the provisions of this law and determine the information security policy of the organization. The law 'On Information Security' regulates the procedure for identifying and reporting a computer incident (an actual or potential violation of the information security policy).

The subject of a critical information system performs the identification of a computer incident, which includes the study and description of, and response to this incident. The identification of a computer incident of the first or second category in the subject of a critical information system is immediately reported to the Computer Incident Support Group of the Operational-Technical Agency, the identification of a critical information system of the third category in the subject—to the Computer Incident Assistance Group of the Digital Government Agency, and the identification of a subject of the critical information system in the field of defence is reported to the Computer Incident Response Team of the Cybersecurity Bureau. The entity of the critical information system implements emergency measures, if necessary, to store and protect information about the computer incident.

The Computer Incident Support Group investigates, describes, and responds to a computer incident. After studying the incident, the Computer Incident Assistance Group develops and submits mandatory instructions to the subject of the critical information system. The mandatory instructions for execution may not include the obligation to access the network sensor of the subject of the second or third category of a critical information system or the information asset, information system and/or subject included in the information infrastructure of the subject of the second or third category of the critical information system. The subject of the critical information system is obliged to respond to the mandatory instructions and take appropriate measures within a reasonable period of time. Subjects of critical information systems of the first and second categories submit information about the implemented measures to the Computer Incident Support Group of the Operational-Technical Agency, subjects of critical information systems of the third category—to the Computer Incident Assistance Group of the Digital Government Agency, and the subjects of critical information systems in the field of defence—to the Computer Incident Response Team of the Cybersecurity Bureau.

Also, the minimum information security requirements for the subjects of critical information systems of the first and second categories are established by the Order no. 35 of December 21, 2021, of the head of the Operational-Technical Agency of Georgia.

According to the above “requirements,” an information security management system (ISMS) should be developed, consisting of policies, procedures, guidelines, related resources, and activities that the organization manages collectively to protect its information assets. An ISMS is a systematic approach to establishing, enforcing, managing, monitoring, reviewing, maintaining, and improving an organization’s information security. The ISMS is based on the organization’s risk assessment and risk acceptance criteria, which are developed for the effective treatment and management of risks. Analyzing the requirements to protect information assets and applying appropriate controls to protect these information assets contributes to the effective implementation of an information security management system.

To implement, monitor, maintain, and improve an ISMS, the organization must (a) define information assets and information security requirements related to them; (b) assess information security risks and carry out information security risk management; (c) select and implement appropriate controls in order to manage unacceptable risks; and (d) monitor, maintain,

and improve the effectiveness of controls related to information assets of the organization.

For the ISMS to continuously and effectively protect the organization's information assets, it is necessary to carry out the above activities on a permanent basis to be able to identify changes in risks, organization strategy, or business tasks.

The organization must define and use the information security risk assessment process, which (a) defines information security risk criteria, including risk acceptance criteria and information security risk assessment criteria; (b) ensures that the repeatable procedure for assessing information security risks produces consistent, valid, and comparable results; (c) determines information security risks; (d) analyzes information security risks; and (e) evaluates information security risks. The organization shall maintain documented information about the information security risk assessment process.

8. Conclusions and policy recommendations

Based on the analysis of Estonia's CIP system and the gap analysis of Georgia's CIP system, the Estonian model could serve as the best practice for building a modern CIP model in Georgia, following a four-step approach: (1) identifying the critical infrastructure sectors and vital services; (2) identifying and analyzing the main threats to critical infrastructure; (3) mapping the key stakeholders per sector/service; and (4) defining the functions and responsibilities of stakeholders.

1) Identifying the critical infrastructure sectors and vital services

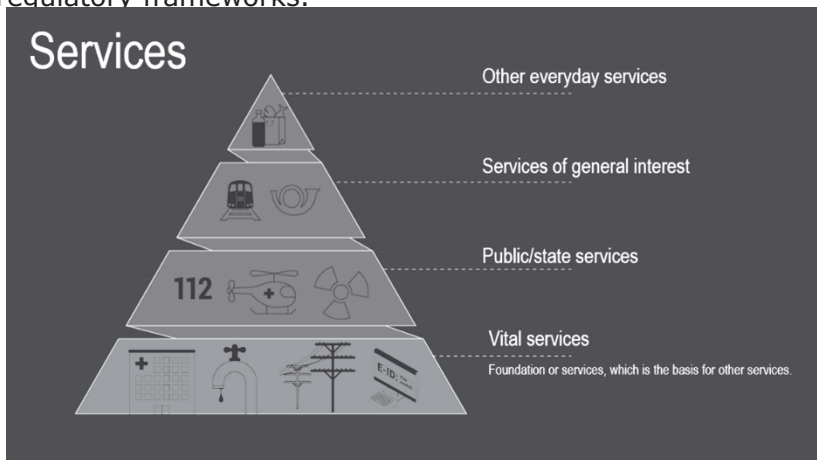
From the outset, Georgia needs to identify some vital components of its CIP system based on modern EU-compatible approaches. As Estonia's experience shows, Georgia, being a small import-oriented county with limited natural resources, could benefit from the concept of sector-by-sector approach. Following the Estonian model, Georgia could define components of its critical infrastructure as follows: critical infrastructures consist of those physical and information technology facilities, networks, services, and resources whose disruption or destruction significantly impacts the health, safety, security, or economic well-being of citizens or affects the efficient functioning of national governments. Based on Estonia's logic,

vital services are those foundational services that provide the basis for all the other critically important basic services in the country. In Estonia's case, those services include healthcare, water and electricity distribution, and electronic systems providing government services to the population. There can be no single list of vital services that could apply to all countries. Accordingly, Georgia should develop its own list based on the structure of its economy and social construct as well as on the levels of population's dependency on various digital and physical services. The general criteria to be used for selecting vital services in Georgia could be borrowed from Estonia's legislation accordingly.

A vital service is a service

- which has an overwhelming impact on the functioning of society;
- the interruption of which directly threatens the life or health of people or another vital service or the operation of a service of general interest or causes great environmental damage;
- the interruption of which has a significant impact on the national economy and national defence.

Figure 1. Estonia's categorization of services under its legislative and regulatory frameworks.



Source: Compiled by the authors.

The Estonian model does not clearly define the term critical infrastructure nor critical infrastructure sectors. However, since Georgia is taking its first steps in developing its CIP system, it might be useful to first identify the sectors that are of strategic importance for the country (e.g., energy,

telecommunications, transportation, banking, healthcare, food and water, etc.) and then gradually identify the vital services inside those critical sectors. This approach will facilitate the inclusion of professional circles within various sectors into the discussion and the development of the legislative and regulatory frameworks. Such an approach would allow for an inclusive process, which, in turn, may foster effective cooperation and coordination across the sectors.

2) Identifying and analyzing the main threats to critical infrastructure

In a highly interconnected and interdependent world, the emergence of new domains has heavily affected and increased the risks of operations in all sectors of strategic importance for national security. The issue of protecting critical infrastructure is even more relevant for Georgia, which is exposed to military, political, and economic tools of malign influence, as well as various tools of hybrid warfare. As the threats and risks to Georgia's CI are broad in nature, it is highly recommended that Georgia adopts an all-hazards approach and draws its CIP considerations from the regularly updated comprehensive National Threat Assessment Document. Notably, the current version of the National Threat Assessment Document was updated as early as in 2015. In the case of Estonia, military threats and threats related to power and communication outages are of primary concern, as their impact would affect all or the majority of Estonian population. Estonia conducts a yearly assessment of the threats and develops annual CIP and crisis management plans accordingly. Similarly, Georgia should develop a corresponding system that would consider the threat landscape and base the CIP consideration on the specific context and factors affecting Georgia's national security.

Figure 2 shows how Estonia maps its various sectors and services based on the number of the country's population likely to be affected by disturbances in that particular sphere.

3) Mapping the key stakeholders per sector/service

In both Estonia and Georgia, most of the strategic assets are dispersed through different sectors of the private sector, with only the limited amount of critical infrastructure still under the government ownership. Accordingly, the proper identification of key state and non-state stakeholders within each sector is vitally important. In the case of Estonia, the criteria of selecting companies providing vital services is based on a thorough assessment of their impact on the proper functioning of the state and societal functions at

a local or national level. One of the main criteria is the scale of disturbances in the sector, counting the number of customers that will be affected in case of service disruption of particular companies. It is critical that all those stakeholders are invited to contribute to the process of developing a legislative and regulatory document as early as possible. This open and inclusive process can deliver mutually beneficial outcomes for both public and private stakeholders, generating full confidence and a sense of ownership and responsibility among all involved parties.

Figure 3 shows the vital services where stakeholders are identified in Estonia's case (15–21 services will be added to the next addition to Estonia's Emergency Act).

4) Defining the functions and responsibilities between stakeholders

After identifying the sectors of critical infrastructure, defining the vital services, and mapping the key stakeholders, a vitally important step is to develop a workable pattern of relationships and distribution of the responsibilities and coordination among the key stakeholders across public and private actors. The approaches and organizing principles applied in Georgia's critical information infrastructure protection system could serve as a good starting point for developing legislation and regulatory frameworks in in other critical infrastructure sectors.

The relationships between the stakeholders representing different sectors are complex and require thorough planning and coordination mechanisms. The private sector often does not appreciate directives from government agencies on how they should handle their security arrangements. This is a very delicate issue and can only be solved through regular contacts with various involved industries and raising their awareness on the threats to their operations and infrastructure. Another important aspect of the public private cooperation on CIP is the sharing of sensitive and classified information. While it is not always possible for government institutions to share classified materials and intelligence information with the private sector, it is vitally important to develop credible mechanisms for exchanging information on the threats and risks between the sectors. Table 1 on page 284, elaborated by the project team, aims to explain the logic of cross sector relationships and give a flavor of the responsibilities of key stakeholders in the case of Estonia. This table could serve as a useful basis for adapting Estonia's experience in Georgia's specific contexts.

Finally, due to the lack of legal protection mechanisms, Georgia faces an elevated risk of politically motivated direct foreign investments and adversarial actors gaining control over CI. It is critically important for Georgia to adopt legislation limiting the ownership and management of strategic assets by the foreign parties that might have political motivations to exert malign influences on the country's policy choices and decision-making systems. Thus, it is highly recommended for Georgia to adopt an FDI screening model based on Estonia's experience of applying the Foreign Investment Reliability Assessment Act.

Dr. **Archil Chochia** is a senior researcher at TalTech Law School of Tallinn University of Technology. Dr. Chochia obtained his doctoral degree from TalTech in 2013. His academic publications include *Political and Legal Perspectives of the EU Eastern Partnership Policy* (Springer, 2016), *Brexit: History, Reasoning and Perspectives* (Springer, 2018), and *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighbourhood* (Springer, 2021). Archil is a senior fellow of the Weinstein International Foundation.

Ambassador **Shota Gvineria** is a lecturer at the Baltic Defence College in Tartu and a Senior Fellow in Economic Policy Research Centre. Shota Gvineria has worked with the security question for the past 20 years in various positions. He has been a Deputy Secretary at National Security Council of Georgia (2017–2018), Ambassador at Large at NATO & Security Policy at the Ministry of Foreign Affairs (2016–2017), he has been head of the NATO Division at MFA of Georgia (2008–2009) and has worked in various positions at the Politico-Military Department at MFA of Georgia (2001–2008). Shota Gvineria was a foreign policy advisor to the Minister of Defence of Georgia (2015–2016) and director of the European Affairs Department at MFA of Georgia (2009–2010).

Dr. **Holger Mölder** is an associate professor of international relations at Tallinn University of Technology and, in his research, focuses on various international security issues, political cultures, influence and information operations, and cognitive warfare. He has a PhD from the University of Tartu (2010) in political sciences. Before joining TalTech, he worked for nearly 20 years for the Estonian Ministry of Defence and the Estonian Military Academy. His recent works include co-editing *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighbourhood* (Springer, 2021), *Producing Cultural Change in Political Communities* (Springer, 2023), and the article 'The Prospects of Strategic Imagination in Explaining International Security Challenges' in *Quality & Quantity* (2022).

References

- 2030 Development Strategy (n.d.), Government of Georgia. Retrieved from https://www.gov.ge/files/428_85680_321942_khedva-2030-saqarthvelos-ganvitharebis-strategia-1.pdf [accessed 3 May 2024]
- Bossong, R.** (2014), 'The European Programme for the Protection of Critical Infrastructures—Meta-governing a New Security Problem?' *European Security*, vol. 23, no. 2, pp. 210–226. <https://doi.org/10.1080/09662839.2013.856307>
- Chochliouros, I. P.; Spiliopoulou, A. S.; Stephanakis, I. M.; Arvanitosis, D. N.; Sfakianakis, E.; Belesiotti, M.; Georgiadou, E. & Mitsopoulou, N.** (2015), 'Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also Focusing upon the Cloud Perspective,' in *Proceedings of the 16th International Conference on Engineering Applications of Neural Networks (INNS)*, pp. 1–10. <https://doi.org/10.1145/2797143.2797146>
- Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the Fight Against Terrorism, Brussels, COM(2004) 702, 20.10.2004.
- Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *OJ L 345/75*, 23.12.2008.
- Cybersecurity Act (2018), Küberturvalisuse seadus, *Riigi Teataja*, RT I, 22.05.2018, 1.
- Description and Continuity Requirements for the Provision of Essential Telephone, Mobile Telephony and Data Services Act (2021), Elutähtsa telefoni-, mobiiltelefon- ja andmesideteenuse kirjeldus ja toimepidevuse nõuded [in Estonian], *Riigi Teataja*, RT I, 26.02.2021, 17.
- Description of Essential Service and Continuity Requirements for Electricity Supply Act (2018), Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektriga varustamisel [in Estonian], *Riigi Teataja*, RT I, 03.07.2018, 20.
- Description of the Essential Service and Continuity Requirements for Natural Gas Supply Act (2018), Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded maagaasiga varustamisel [in Estonian], *Riigi Teataja*, RT I, 03.07.2018, 19
- Description of the Vital Service and Continuity Requirements for Ensuring the Navigability of the National Road Network Act (2018), Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded riigitee sõidetavuse tagamisel [in Estonian], *Riigi Teataja*, RT I, 12.01.2018, 6.
- Emergency Act (2017), Hädaolukorra seadus [in Estonian], *Riigi Teataja*, RT I, 03.03.2017, 1.

- Foreign Investment Reliability Assessment Act (2023), Välisinvesteeringu usaldusväärsuse hindamise seadus [in Estonian], *Riigi Teataja*, RT I, 10.02.2023, 3.
- Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S. & Baker, T.** (2018), 'Security Threats to Critical Infrastructure: The Human Factor,' *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4986–5002. <https://doi.org/10.1007/s11227-018-2337-2>
- Gvelesiani, L. & Mölder, H.** (2018), 'Maintaining the Security Dilemma in the South Caucasus: Russia's Geostrategic Interests in Georgia,' *Sõjateadlane (Estonian Journal of Military Studies)*, vol. 7, pp. 137–157.
- Kadri, F.; Birregah, B. & Châtelet, E.** (2014), 'The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-Based Study,' *Journal of Homeland Security and Emergency Management*, vol. 11, no. 2, pp. 217–241. <https://doi.org/10.1515/jhsem-2012-0077>
- Karabacak, B.; Ozkan Yildirim, S. & Baykal, N.** (2016), 'Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey,' *Computer Law & Security Review*, vol. 32, no. 3, pp. 526–539. <https://doi.org/10.1016/j.clsr.2016.02.005>
- Kerikmäe, T. & Chochia, A.**, eds. (2016), *Political and Legal Perspectives of the EU Eastern Partnership Policy*, Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-27383-9>
- Keypour, J.; Kerikmäe, T. & Chochia, A.** (2023), 'Critical Legal Insight into the EU's Hydrogen Strategy,' in J. Simões, F. J. Leandro, E. C. de Sousa & R. Oberoi (eds.) *Changing the Paradigm of Energy Geopolitics: Security, Resources, and Pathways in Light of Global Challenges*, New York: Peter Lang Publishing, pp. 377–401. <https://doi.org/10.3726/b18776>
- Latvian Institute of International Affairs (2021), *Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication*. Retrieved from <https://liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944> [accessed 8 May 2024]
- Lazari, A. & Tabagua, N.** (2024), *Critical Infrastructure Security and Resilience in Georgia: State of Play and Future Prospects*, Policy and Management Consulting Group. Retrieved from https://pmcg-i.com/app/uploads/2024/04/CISR-Policy-in-Georgia-2024_Final.pdf [accessed 2 May 2024]
- Lindström, M. & Olsson, S.** (2009), 'The European Programme for Critical Infrastructure Protection,' in S. Olsson (ed.) *Crisis Management in the European Union: Cooperation in the Face of Emergencies*, Cham: Springer, pp. 37–59. https://doi.org/10.1007/978-3-642-00697-5_3

- Markopoulou, D.; Papakonstantinou, V. & de Hert, P.** (2019), 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation,' *Computer Law & Security Review*, vol. 35, no. 6, art. 105336. <https://doi.org/10.1016/j.clsr.2019.06.007>
- Mazur, V. & Chochia, A.** (2022), 'Definition and Regulation as an Effective Measure to Fight Fake News in the European Union,' *European Studies: The Review of European Law, Economics and Politics*, vol. 9, no. 1, pp. 15–40. <https://doi.org/10.2478/eustu-2022-0001>
- Mölder, H.; Sazonov, V.; Chochia, A. & Kerikmäe, T.** (2021), *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighborhood*, Cham: Springer. <https://doi.org/10.1007/978-3-030-73955-3>
- Napetvaridze, V. & Chochia, A.** (2019), 'Cybersecurity in the Making—Policy and Law: A Case Study of Georgia,' *International and Comparative Law Review*, vol. 19, no. 2, pp. 155–180. <https://doi.org/10.2478/iclr-2019-0019>
- National Defence Development Plan 2017–2026 (2017), [Riigikaitse arengukava], Republic of Estonia Government Office, p. 5. Retrieved from https://kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/rkak_2017_2026_avalik_osa.pdf [accessed 8 May 2024]
- National Risk Analysis (n.d.), Republic of Estonia Government Office. Retrieved from <https://riigikantselei.ee/en/national-risk-analysis> [accessed 8 May 2024]
- National Security Concept (2011), National Security Council of Georgia. Retrieved from <https://nsc.gov.ge/en/CONCEPTUAL-DOCUMENTS/National-Security-Concept> [accessed 20 Apr 2024]
- National Security Concept (2023), Republic of Estonia Government Office. Retrieved from [https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT003B6B36/\\$file/Eesti%20julgeolekupoliitika%20alused_eng_22.02.2023.pdf](https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT003B6B36/$file/Eesti%20julgeolekupoliitika%20alused_eng_22.02.2023.pdf) [accessed 8 May 2024]
- National Threat Assessment Document of Georgia (n.d.), National Security Council of Georgia. Retrieved from <https://nsc.gov.ge/en/CONCEPTUAL-DOCUMENTS/Threat-Assessment-Document> [accessed 20 Apr 2024]
- Osei-Kyei, R.; Tam, V.; Ma, M. & Mashiri, F.** (2021), 'Critical Review of the Threats Affecting the Building of Critical Infrastructure Resilience,' *International Journal of Disaster Risk Reduction*, vol. 60, art. 102316. <https://doi.org/10.1016/j.ijdrr.2021.102316>
- Parliament of Estonia (2023), 'The Riigikogu Discussed the Updated National Security Concept,' 6 February. Retrieved from <https://www.riigikogu.ee/en/sitting-reviews/the-riigikogu-discussed-the-updated-national-security-concept/> [accessed 8 May 2024]
- Pursiainen, C.** (2009), 'The Challenges for European Critical Infrastructure Protection,' *Journal of European Integration*, vol. 31, no. 6, pp. 721–739. <https://doi.org/10.1080/07036330903199846>

- Rehak, D.; Hromada, M. & Lovecek, T.** (2020), 'Personnel Threats in the Electric Power Critical Infrastructure Sector and Their Effect on Dependent Sectors: Overview in the Czech Republic,' *Safety Science*, vol. 127, art. 104698. <https://doi.org/10.1016/j.ssci.2020.104698>
- Sayapin, S. & Tsybulenko, E.**, eds. (2018), *The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum*, Cham: Springer. <https://doi.org/10.1007/978-94-6265-222-4>
- Tiirmaa-Klaar, H.** (2016), 'Building National Cyber Resilience and Protecting Critical Information Infrastructure,' *Journal of Cyber Policy*, vol. 1, no. 1, pp. 94–106. <https://doi.org/10.1080/23738871.2016.1165716>
- Tropp, E.-M.; Hoffmann, T. & Chochia, A.** (2022), 'Open Data: A Stepchild in e-Estonia's Data Management Strategy?' *TalTech Journal of European Studies*, vol. 12, no. 1, pp. 123–144. <https://doi.org/10.2478/bjes-2022-0006>
- Tsybulenko, E.** (2022), 'Blinding Laser Weapons,' in S. Sayapin, R. Atadjanov, U. Kadam, G. Kemp, N. Zambrana-Tévar & N. Quénivet (eds.) *International Conflict and Security Law*, The Hague: T.M.C. Asser Press / Springer, pp. 367–378. https://doi.org/10.1007/978-94-6265-515-7_16
- Tsybulenko, E. & Kajander, A.** (2021), 'The Hybrid Arsenal of Russia's War Against the Democratic World,' in H. Mölder, V. Sazonov, A. Chochia & T. Kerikmäe (eds.) *The Russian Federation in Global Knowledge Warfare. Contributions to International Relations*, Cham: Springer, pp. 173–194. https://doi.org/10.1007/978-3-030-73955-3_9
- Tsybulenko, E. & Kajander, A.** (2022), 'Customary International Humanitarian Law and Article 36 of Additional Protocol I to the Geneva Conventions: A Stopgap Regulator of Autonomous Weapons Systems?' *TalTech Journal of European Studies*, vol. 12, no. 2, pp. 87–112. <https://doi.org/10.2478/bjes-2022-0013>
- Tsybulenko, E. & Platonova, A.** (2022), 'Legal Instruments of the Shanghai Cooperation Organisation: A Case of Missed Opportunities?' in S. Sayapin & R. Burnashev (eds.) *Central Asian Yearbook of International Law and International Relations*, vol. 1, The Hague: Eleven, pp. 244–257.
- Tsybulenko, E. & Rinta-Pollari, H.** (2023), 'Legal Challenges in Prosecuting the Crime of Aggression in the Russo-Ukrainian War,' *Review of Central and East European Law*, vol. 48, nos. 3–4, pp. 319–350. <https://doi.org/10.1163/15730352-bja10087>
- Wiater, P.** (2015), 'On the Notion of "Partnership" in Critical Infrastructure Protection,' *European Journal of Risk Regulation*, vol. 6, no. 2, pp. 255–262. <https://doi.org/10.1017/S1867299X00004554>
- Wilson, C.** (2014), 'Cyber Threats to Critical Information Infrastructure,' in T. M. Chen, L. Jarvis & S. Macdonald (eds.) *Cyberterrorism: Understanding*,

Assessment, and Response, New York: Springer, pp. 123–136.

https://doi.org/10.1007/978-1-4939-0962-9_7

Yao, X.; Wei, H.-H.; Shohet, I. M. & Skibniewski, M. J. (2020), 'Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation,' *Applied Sciences*, vol. 10, no. 20, art. 20.

<https://doi.org/10.3390/app10207162>

