PMCG Research

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) POLICY IN GEORGIA:

STATE OF PLAY AND FUTURE PROSPECTS

By Alessandro Lazari and Nana Tabagua

“*By failing to prepare you are preparing to fail*”

Benjamin Franklin

The opinions expressed in this publication are those of the authors, and do not necessarily reflect the views of PMCG or PMC Research.

PMCG | Research

61 Aghmashenebeli Avenue, 4th floor Tbilisi 0102
Phone: + (995) 577 170660
Office@pmcginternational.com
www.pmcg-i.com

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) POLICY IN GEORGIA:

STATE OF PLAY AND FUTURE PROSPECTS

CONTE

CONTENTS

FOREWORD

In an era where critical infrastructure security and resilience (CISR) has become paramount to national security, economic stability, and public safety, nations are increasingly recognizing the importance of bolstering their protective measures and governance models. Georgia stands on the cusp of a significant reform, aimed at enhancing its critical infrastructure security and resilience. This policy paper presents an initial analysis of Georgia's current critical infrastructure protection (CIP) landscape as well as insights from the governance models of two EU Member States, and sets out a potential path forward that could serve to safeguard Georgia's infrastructural assets and align its policies with global best practices.

The critical infrastructure of a nation encompasses a wide range of sectors including energy, water supply, telecommunications, and transportation. These sectors form the backbone of a country's economy and are vital to citizens' livelihoods. As such, the security and resilience of these sectors is not just a matter of national concern but a prerequisite for sustainable development and public well-being. Georgia, situated at a strategic crossroads in the South Caucasus region, faces unique challenges and opportunities in this domain.

This policy paper begins by laying out the current state of CISR in Georgia. In doing so, it provides an analysis of existing legislation, regulatory frameworks, and the operational landscape. This builds a foundation on which to understand the gaps and strengths in Georgia's current approach, and to learn learning from the experiences of others.

Drawing lessons from the EU, which has long been at the forefront of developing advanced and cohesive policies for CIP, this study explores the governance models of two of its Member States. These models offer valuable insights into the integration of cross-sectoral policies, the adoption of efficient and impactful governance models and legislative frameworks, and the fostering of public-private partnerships. They represent not just a set of practices but a vision for a more secure and resilient infrastructure ecosystem.

Moving forward, the study proposes a pathway for Georgia that is both efficient and effective. It emphasizes the need for a holistic approach that encompasses policy reform, public-private interaction, and international cooperation. Its recommendations are designed to not only address immediate vulnerabilities but also to build long-term resilience against a spectrum of threats, ranging from cyberattacks to natural disasters, allowing Georgia to establish a robust basis for CISR.

As Georgia embarks on this important reform, it is imperative that all stakeholders—government agencies, industry leaders, academic institutions, and international partners and donors—collaborate closely. The road ahead is complex and challenging, yet it is also filled with opportunities to redefine Georgia's critical infrastructure to ensure a safer and more resilient future.

This Policy paper aims to contribute to the ongoing discourse on CISR, offering a blend of analysis, comparative insights, and forward-looking recommendations. It is our hope that it will serve as a valuable resource for policymakers, experts, and practitioners alike, as they work together to enhance the security and resilience of Georgia's critical infrastructure.

Alessandro Lazari, Ph.D.
28th of February 2024

GLOSSARY

This glossary contains terms that have been used in this Policy paper as well as other terms prevalently used in the field of CISR.

Definitions from the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection:

RISK ANALYSIS: Consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of the disruption or destruction of critical infrastructure.

PROTECTION: All activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructures in order to deter, mitigate, and neutralize a threat, risk, or vulnerability.

OPERATOR SECURITY PLAN (OSP): A procedure identifying the critical infrastructure assets and which security solutions exist or are being implemented for their protection.

Definitions from the DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC:

CRITICAL ENTITY: A public or private entity which has been identified as such by a Member State. Such an entity provides one or more essential services. Moreover, it operates, and its critical infrastructure is located, on the territory of that Member State. In addition, an incident would have significant disruptive effects on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors that depend on that or those essential services.

CRITICAL INFRASTRUCTURE: An asset, a facility, equipment, a network, or system, or a part of an asset, a facility, equipment, a network, or system, which is necessary for the provision of an essential service.

ESSENTIAL SERVICE: A service which is essential for the maintenance of critical societal and/or economic activities, the provision of which depends on network and information systems; An incident would have significant disruptive effects on the provision of that service.

INCIDENT: An event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, having an effect on national systems that safeguard the rule of law.

RESILIENCE: The ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from an incident.

RISK: The potential for loss or disruption caused by an incident, taking into account the magnitude of such loss or disruption and the likelihood of such an incident occurring.

RISK ASSESSMENT: The process of determining the nature and extent of a risk by identifying and analyzing potential threats, vulnerabilities, and hazards which could lead to an incident, and by evaluating the potential loss or disruption of the provision of an essential service caused by such an incident.

Definitions from the DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive):

CYBERSECURITY: The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

INCIDENT HANDLING: Any actions or procedures aiming to prevent, detect, analyze, contain, respond to, and recover from an incident.

LARGE-SCALE CYBERSECURITY INCIDENT: An incident which causes a level of disruption that exceeds a Member State's capacity to respond to it, or which has a significant impact on at least two Member States.

NEAR MISS: An event that could have compromised the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or of the services offered by, or accessible via, network and information systems, but did not materialize.

NETWORK AND INFORMATION SYSTEMS: Any device or group of interconnected or related devices, one or more of which, pursuant to a program, conduct automatic processing of digital data; or digital data stored, processed, retrieved, or transmitted for the purposes of their operation, use, protection, and maintenance.

SECURITY OF NETWORK AND INFORMATION SYSTEMS: The ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or of the services offered by, or accessible via, those network and information systems.

SIGNIFICANT CYBER THREAT: A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity, or the users of the entity's services, by causing considerable material or non-material damage.

ACRONYMS

CISR	Critical Infrastructure Security and Resilience
CIP	Critical Infrastructure Protection
CISR-WG	Critical Infrastructure Security and Resilience Working Group
NCI	National Critical Infrastructure
ECI	European Critical Infrastructure
OSP	Operator Security Plan
CE	Critical Entity
NSC	National Security Council of Georgia
CNCPIC	the National Center for Coordinating Critical Infrastructure Protection in Romania
EPCIP	European Programme for Critical Infrastructure Protection
HPP	Hydropower Plant
EU	European Union
US	The United States of America
NATO	The North Atlantic Treaty Organization

INTRODUCTION

/01

1. INTRODUCTION

A recent report jointly published by the European Commission and the European Centre of Excellence for Countering Hybrid Threats1 provides an up-to-date picture of the threat landscape facing countries, governments, authorities, and critical infrastructures today. The report shows that such threats have evolved far beyond the cyber/physical dimensions of national and international critical infrastructures, and now include much more sophisticated threats, like hybrid ones, which rely on a combination of conventional and unconventional methods targeting the security and continuity of vital assets and essential services.

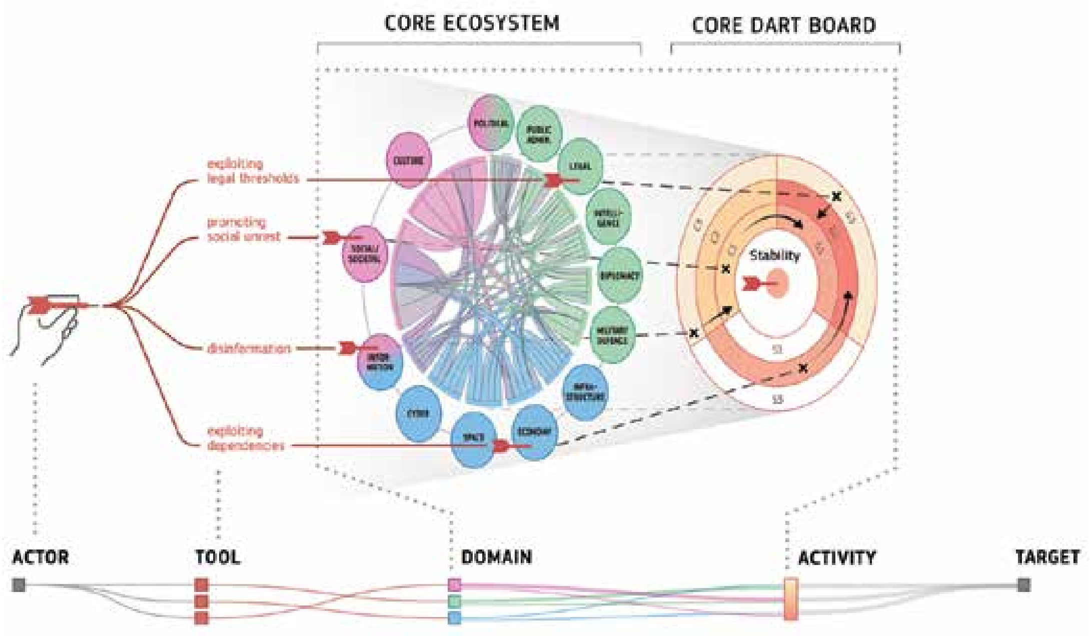


Fig. 1 "Presenting the impacts of hybrid threats"[2]

Exploits target all pillars of modern society to introduce uncertainty, instability, unrest, economic damage, and loss of competitiveness.

In the current global landscape, the protection, resilience, and cybersecurity of critical infrastructures are all of the utmost importance. Critical infrastructures such as energy, transportation, communication, and healthcare systems form the backbone of modern societies, and any disruption thereto or destruction thereof can have severe consequences for the economy, public health, and national security. Therefore, it is imperative that countries adopt up-to-date frameworks to ensure the resilience and cybersecurity of critical infrastructures to mitigate known risks, prepare for new ones that may arise, and preserve the continuity of services perceived as vital and taken for granted by citizens.

In this policy paper, we explore the significance of having in place modern frameworks for the protection, resilience, and cybersecurity of critical infrastructures, especially given the

[1] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., "Hybrid threats: a comprehensive resilience ecosystem", Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.

[2] "Hybrid threats: a comprehensive resilience ecosystem", p. 11.

current threat landscape and societal challenges. Hybrid threats, the COVID-19 pandemic, and the wars in Ukraine and Israel/Gaza are all considered in the analysis.

In today's heavily digitalized era, critical infrastructures are more vulnerable to cyber threats than ever before. Advances in technology have made it easier for cyber threat actors to exploit vulnerabilities in critical infrastructure systems and disrupt them. Therefore, it is essential for countries to establish and maintain frameworks that comprehensively cover all aspects of critical infrastructure security and resilience (CISR), including risk assessment, threat analysis, incident response, and recovery. Moreover, establishing national frameworks is crucial to ensure resilience in the face of natural disasters, terrorist attacks, and/or pandemics. The COVID-19 pandemic demonstrated the importance of having such resilient critical infrastructure systems in place to withstand unexpected shocks and disruptions. Healthcare systems, for example, had to deal with unprecedented challenges including shortages of medical equipment and personnel, and cyberattacks targeting healthcare facilities. Initially classified as low-frequency with high-impact disruptions, pandemics are now treated with the highest priority. Since the COVID-19 pandemic has forced every organization on the globe to completely review, reassess, and redesign their security procedures, business continuity plans, and human resources policies.

As alluded to at the beginning of this chapter, hybrid threats represent a significant concern for countries when it comes to critical infrastructure protection, resilience, and cybersecurity. Hybrid threats refer to a combination of conventional and non-conventional threats, including cyberattacks, disinformation campaigns, and terrorist attacks.[3] These threats can be difficult to detect and respond to because they involve multiple actors, and they can have varying degrees of impact on critical infrastructure systems. Hybrid threats have been on the rise in recent years, targeting critical infrastructure systems in several instances. For example, in Russia's war on Ukraine, critical infrastructure systems such as power plants and water treatment facilities have been targeted by cyberattacks, causing disruptions and damage. Pertinently, the war has highlighted the vulnerabilities of critical infrastructure systems to cyberattacks and other forms of hybrid threats.

Since the commencement of the Israel-Hamas war in early October 2023, over 60 cyber activist groups have initiated attacks against state entities in both Israel and the Palestinian Territories, with a particular focus on critical national infrastructures, encompassing governments as well as the communication and energy sectors.[4] These orchestrated cyber activities have highlighted an evolving dimension in this particular conflict, where the security and resilience of critical infrastructure emerges as a central concern for the sustained functioning of essential services and national security as a whole.

Meanwhile, in the wake of Georgia recently being granted EU candidate status, the country must accelerate the implementation of reforms to meet the EU's security policy standards. In that regard, safeguarding and enhancing the resilience of critical infrastructure stands as a top priority on the EU's security agenda. Relatedly, implementation of the Directive on the Resilience of Critical Entities, effective as of 16 January 16 2023, is devoted to bolstering this area.

In this context, it is of paramount importance for Georgia to prioritize the reform of CISR domain and acknowledge its responsibility to establish a national framework.

Successfully accomplishing reform in this domain demands internal and external efforts. The internal steps pertain to the need to establish a plan of action and to execute it with the maximum involvement of all necessary stakeholders, while the external efforts entail absorbing international best practices to improve internal efforts and interacting with international entities and experts that can provide Georgia with authoritative advice and recommendations.

[3] On the matter of hybrid threats and the approach of the European Union, see: (1) Joint Framework on countering hybrid threats (2016) – available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018; (2) Hybrid Threats: A Comprehensive Resilience Ecosystem (2023) – available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC129019; (3) A comprehensive portal on the EU's joint actions and measures to counter hybrid threats is available at https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en#:~:text=Hybrid%20threats%20refer%20to%20when,the%20threshold%20of%20formal%20warfare.

[4] https://www.controlrisks.com/our-thinking/insights/israel-hamas-conflict-to-heighten-cyber-espionage-and-disruptive-cyber-threats?utm_referrer=https://www.google.com

The process of tailoring a national approach to CISR requires blending the national identity and ways of tackling internal issues with international approaches already implemented and validated elsewhere, to guarantee the greatest possible efficiency and impact. At the same time, the involvement of internal actors and stakeholders is pivotal since the implementation of such reform depends on the willingness of policymakers, regulators, agencies, private operators, and supply chains to willingly work toward a common goal, namely the enhancement of the security and resilience of vital assets and critical infrastructures.

Securing the involvement of internal actors is the most demanding part of any reform and policy lifecycle. In this phase, some such actors may be reluctant to engage in discussions with external entities and public bodies. There are several possible reasons for such difficulties, such as their lack of interest in and understanding of the given domain and/or issue, a lack of trust in external entities, and a fear of reputational damage.

Indeed, obstacles of this nature have been found in this research, which initially aimed at complementing desktop findings with in-field interviews. Specifically, the project team reached out to 10 potential critical entities, some of which are categorized as critical information systems under Georgian legislation. However, the targeted stakeholders were either unavailable or uninterested in engaging in information exchanges and interviews aimed at capturing the state of play, accomplishments, and challenges. While various underlying causes could potentially explain this absence of engagement, a lack of awareness among these entities was certainly evident. When it comes to CISR in Georgia, it is imperative to acknowledge the significant shortage of substantial research and primary as well as secondary sources on this subject. Despite the growing importance of safeguarding critical infrastructure in the face of various threats, there remains a noticeable void in the scholarly literature and documented expertise concerning the specific context of Georgia.

In conclusion, the current threat landscape and Georgia’s EU and NATO aspirations would strongly suggest that putting in the efforts necessary to establish a comprehensive national framework to guarantee the resilience of national critical infrastructures and essential services should be of the utmost importance.

Georgia, like any other country, prioritizes national security but takes a rather incomplete and fragmented approach whereby the efforts of all involved stakeholders lack coordination and harmonization, and are not focused on a common goal[5].

This policy paper endeavors to stimulate dialogue among the public, expert community, academia, and media in Georgia on the criticality of CISR for national security, emphasizing the significance of raising awareness and accumulating knowledge to assist the Georgian government and stakeholders to implement reforms effectively. In addition, this policy paper serves as an instrument through which to attract the attention of the international donor community, aiming to bring vital expertise and resources to Georgia to support local actors in the reform process.

Moreover, it shows potential ways in which Georgia could update and reinforce its approach to national critical infrastructure protection, resilience, and cybersecurity. Accordingly, the policy paper looks at the governance models, strategies, and policies already in place. In particular, approaches like those of the US and the EU, which have undergone many policy lifecycles in the last 50 years, are also considered.

After having provided an overview of the most important CISR milestones in recent history, the policy paper aims to set out a tailor-made approach for Georgia. To do so, Georgia’s relevant legislation, policy, and governance model are deeply examined in order to inform recommendations that will allow for the establishment and maintenance of a suitably comprehensive and inclusive national framework.

As Georgia does not yet have such a comprehensive framework, means initial efforts and goals must first be prioritized, since embarking on a fully-fledged approach could not be achieved in a short space of time. With that in mind, the policy paper will primarily propose that steps be taken to establish solid foundations and kick-start mechanisms, after which Georgia will be better placed to pursue wider and more ambitious initiatives in this area.

[5] Shalva Dzebisashvili, “One Step Forward – One Step Back: The Dilemma of State Resilience in the Absence of Coordinated Policy”, Policy Paper No. 19, Georgian Institute of Politics, February 2021.

Research

THE CONCEPT OF CISR AND ITS INCREASING IMPORTANCE IN NATIONAL SECURITY POLICY

/02

2. THE CONCEPT OF CISR AND ITS INCREASING IMPORTANCE IN NATIONAL SECURITY POLICY

The concept of CIP dates back to the Cold War era, when the U.S. government started to develop plans to ensure the continuity of government operations in the event of a nuclear attack. These plans included the protection of critical infrastructure systems such as communication and transportation systems.[6]

More recently, CIP has gained prominence on various nations' security agendas after the infamous 9/11 terrorist attacks in 2001 in the US, and subsequent attacks on Madrid and London in 2004 and 2005 respectively. In response, the U.S. government established the Department of Homeland Security (DHS), for which one of the priorities is to coordinate the protection of critical infrastructure systems, according to the framework laid out in its National Infrastructure Protection Plan (NIPP) in 2006.[7]

The EU has similarly recognized the importance of critical infrastructure protection by adopting the European Programme for Critical Infrastructure Protection (EPCIP), which provided a framework for the protection of critical infrastructure systems in the EU.

In this regard, both the US and the EU have reached several milestones and inspired many nations to establish, maintain, or update their own framework CIP. Generally, in the past two decades, Western critical infrastructure policies have shifted from mere protection to prioritizing security and resilience. This change reflects the challenge of safeguarding against an increasing array of risks. Within CISR frameworks, while security and resilience both encompass some form of protection, they are distinct: **Security** involves using cyber or physical defense mechanisms to prevent or mitigate the impacts of wide range of threats; **Resilience** pertains to critical infrastructure's capacity to withstand, recover, or adapt to evolving circumstances.[8]

Analyzing the paths taken by other nations toward establishing their CIP framework can help to pinpoint the several key elements that other nations ought to consider while devising their own frameworks. It is important here to highlight that although having many examples to follow is important, the given nation or entity needs to build its own framework tailored to specific needs. No two security frameworks are the same as they are determined by various context-specific factors including the governance model, the legislative framework, culture, economy, geography, history, security posture, and threat exposure.

The following various directives, decisions, and documents, are worth considering in the establishment of a national CISR framework:

[6] While there is less consensus on which sectors qualify as critical infrastructure, countries with an established national CIP or CISR policies determine their critical infrastructure sectors based on their unique national context. Globally, transportation, water, energy, and communications are universally acknowledged as lifeline sectors.

[7] For some literature on critical infrastructure protection and resilience, see: (1) "European Critical Infrastructure Protection", Lazari A, Springer Inc., ISBN 978-3-319-07496-2 (2014); (2) "The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation", Lazari A, Mikac R, CRC Press, 2022, ISBN 9780367517182; (3) "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency NATO COE-DAT Handbook 1", multiple authors, US Army War College Press, 2022.

[8] See "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)" Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner - USAWC Press - US Army War College – 15/11/2022.

- **THE US:**
  - Presidential Decision Directive 63: Critical Infrastructure Protection - Issued by President Clinton in 1998[9].
  - Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection - Issued by President G.W. Bush in 2003[10].
  - Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors - Issued by President G.W. Bush in 2004[11].
  - Presidential Policy Directive 21: Critical Infrastructure Security and Resilience - Issued by President Obama in 2013[12].
  - Presidential Policy Directive 41: United States Cyber Incident Coordination - Issued by President Obama in 2016[13].
  - Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure - Issued by President Trump in 2017[14].
  - Executive Order 13870: America's Cybersecurity Workforce - Issued by President Trump in 2019[15].
  - Executive Order 14028: Improving the Nation's Cybersecurity - Issued by President Biden in 2021[16].

- **THE EU:**
  - EU Plan of Action on Combating Terrorism[17].
  - Critical Infrastructure Protection in the fight against terrorism[18].
  - Green Paper on a European Programme for Critical Infrastructure Protection[19].
  - Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008)[20].
  - Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure[21].
  - Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (2016)[22].

[9] See https://irp.fas.org/offdocs/pdd/pdd-63.htm

[10] See https://irp.fas.org/offdocs/nspd/hspd-7.html

[11] See https://www.dhs.gov/homeland-security-presidential-directive-12

[12] See https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

[13] See https://irp.fas.org/offdocs/ppd/ppd-41.html

[14] See https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[15] See https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

[16] See https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[17] Council of the European Union, EU Plan of Action on Combating Terrorism—Update (Brussels: Council of the European Union, 2004), 2, https://data.consilium.europa.eu/doc/document/ST-14330-2004-REV-1/en/pdf.

[18] Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52004DC0702

[19] See https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en

[20] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

[21] See https://energy.ec.europa.eu/publications/new-approach-epcip-swd-2013-318_en

[22] See https://eur-lex.europa.eu/eli/dir/2016/1148/oj

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[23].
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)[24].
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC[25].

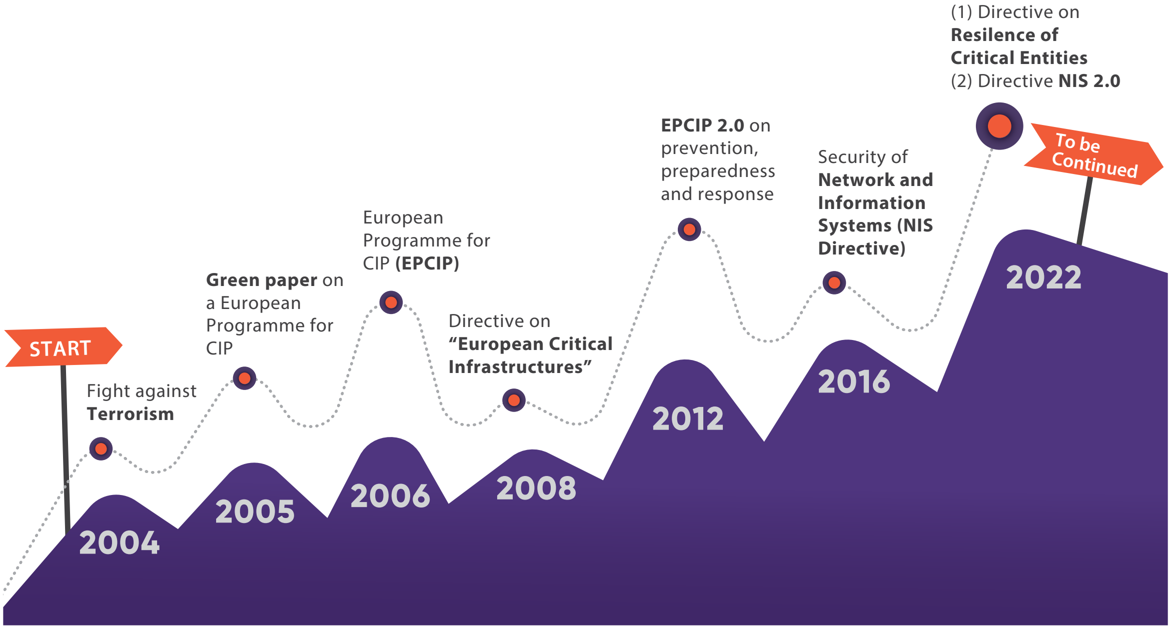

START
Fight against Terrorism
2004
Green paper on a European Programme for CIP
2005
European Programme for CIP (EPCIP)
2006
Directive on "European Critical Infrastructures"
2008
EPCIP 2.0 on prevention, preparedness and response
2012
Security of Network and Information Systems (NIS Directive)
2016
(1) Directive on Resilence of Critical Entities
(2) Directive NIS 2.0
2022
To be Continued

Fig. 2 "Milestones in EU CISR policy development (2004-2020)"[26]

Knowledge and information in the field of CISR can be overwhelming for countries or entities designing their future frameworks, as many horizontal and vertical practices, procedures, and approaches are available. Here, vast materials and insights should be collected and analyzed to establish the initial mechanisms paving the way for policy improvements in the future.

[23] See https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

[24] See https://eur-lex.europa.eu/eli/dir/2022/2555

[25] See https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[26] See "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)" Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner - USAWC Press - US Army War College – 15/11/2022.

(2.1) KEY COMPONENTS OF A CRITICAL INFRASTRUCTURE POLICY

A critical infrastructure policy usually contains several components essential to ensuring the security and resilience of critical infrastructure systems.

For countries that working to establish reform in the field of CISR, it is of pivotal importance to choose the approaches that allow future initiatives to grow.

Since CISR is characterized by complexity, the first policy lifecycle should allow both public and private parties to get acquainted with the new framework and develop internal/external mechanisms for compliance, coordination, and information sharing. Being overly ambitious at this stage could entail the introduction of an excessive number of elements to deal with, thus potentially putting stakeholders off and jeopardizing the successful implementation of the chosen initiatives. Even where a country does not have a formalized approach to CISR, there will inevitably be entities and people in that country engaged in the security and continuity of critical infrastructures. It is fundamental at this stage to move from non-informal and ad-hoc approaches toward structured, transparent, efficient, and effective ones. In addition, the importance of raising awareness is paramount. Meanwhile, correct and impactful implementation of a reform in this domain must incorporate a plan to include the public and private sectors by explaining to both the consequences of a lack of action and the importance of resilient businesses with regard to national security. Public discussion of security matters, with the involvement of citizens, is among the fundamental steps taken by advanced countries in the course of devising suitable frameworks.

Other CISR experiences have demonstrated that once mechanisms, protocols, and procedures are established and executed, the whole domain of CISR is intrinsically affected. For instance, all members of a supply chain have to comply with rules and duties mainly imposed to protect national critical infrastructures. This is an example of the so-called "contamination" that occurs once such a new framework is established. Other areas affected include educational instituríons and research centers.

With all of this in mind, it is advisable that an initial CISR framework should be based on a combination of the following three pillars:

- **A national strategy and action plan on CISR (first pillar);**
- **A law on CISR (second pillar);**
- **A set of administrative instructions to implement the mechanisms introduced by the law on CISR (third pillar).**

The first pillar, which entails the devising of a national strategy and action plan, comprises the following elements:

- Strategic objectives and priorities for the purposes of enhancing the overall protection of critical infrastructures, taking into account cross-sectoral dependencies and interdependencies;
- A governance framework through which to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical infrastructures, and other parties involved in the implementation of the strategy;
- A description of the measures necessary to enhance the overall protection of critical infrastructures, including a risk-driven and all-hazards approach;
- A description of the process by which critical infrastructures are identified and officially designated;
- A description of measures to be taken to enhance cooperation between the private and public sectors;
- A list of the main authorities and relevant stakeholders involved in the implementation of the strategy;
- A mechanism for coordination between the competent CISR authorities and the competent authorities on ICT and cybersecurity.

- The second pillar, namely establishing a law on CISR, is crucial to the reform, and could incorporate the following elements that are common to the US and the EU, and particularly EU Directives 114/08/EC and 2022/2557 on European critical infrastructures and on the resilience of critical entities respectively.

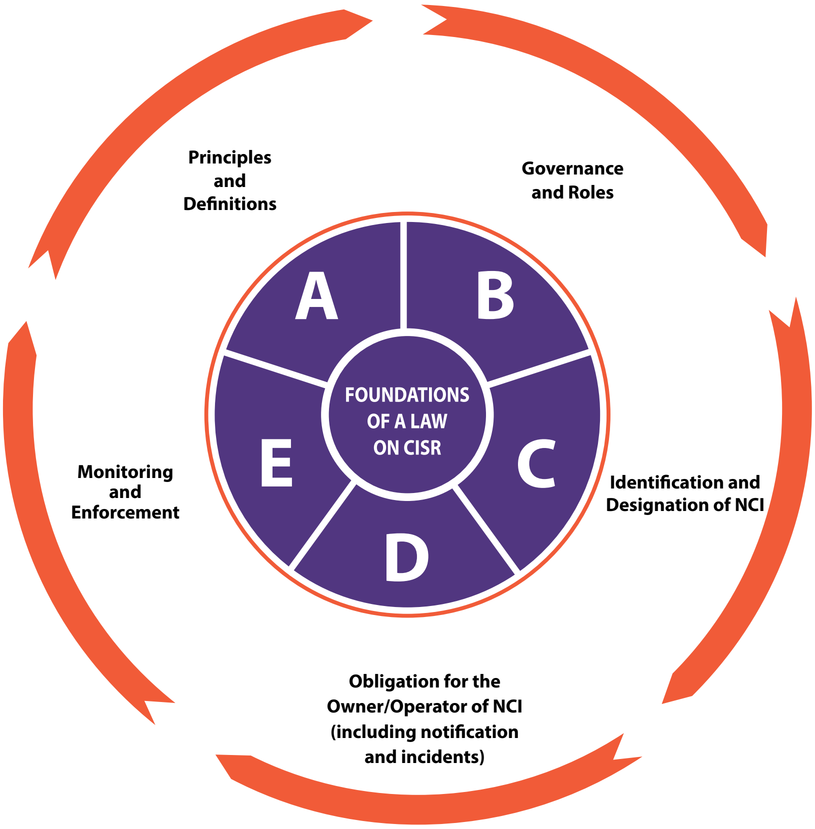

Principles and Definitions
Governance and Roles
A
B
FOUNDATIONS OF A LAW ON CISR
E
C
D
Monitoring and Enforcement
Identification and Designation of NCI
Obligation for the Owner/Operator of NCI (including notification and incidents)

Fig. 3 "Foundations of a Law on CISR"

Initially, CISR reform should focus mainly on establishing the initial mechanisms fundamental to providing a stable framework conducive to subsequent enhancements and ensuring the sustainability of the overall initiative.

For countries embarking on CISR reform for the first time, the following directives should be referred to:

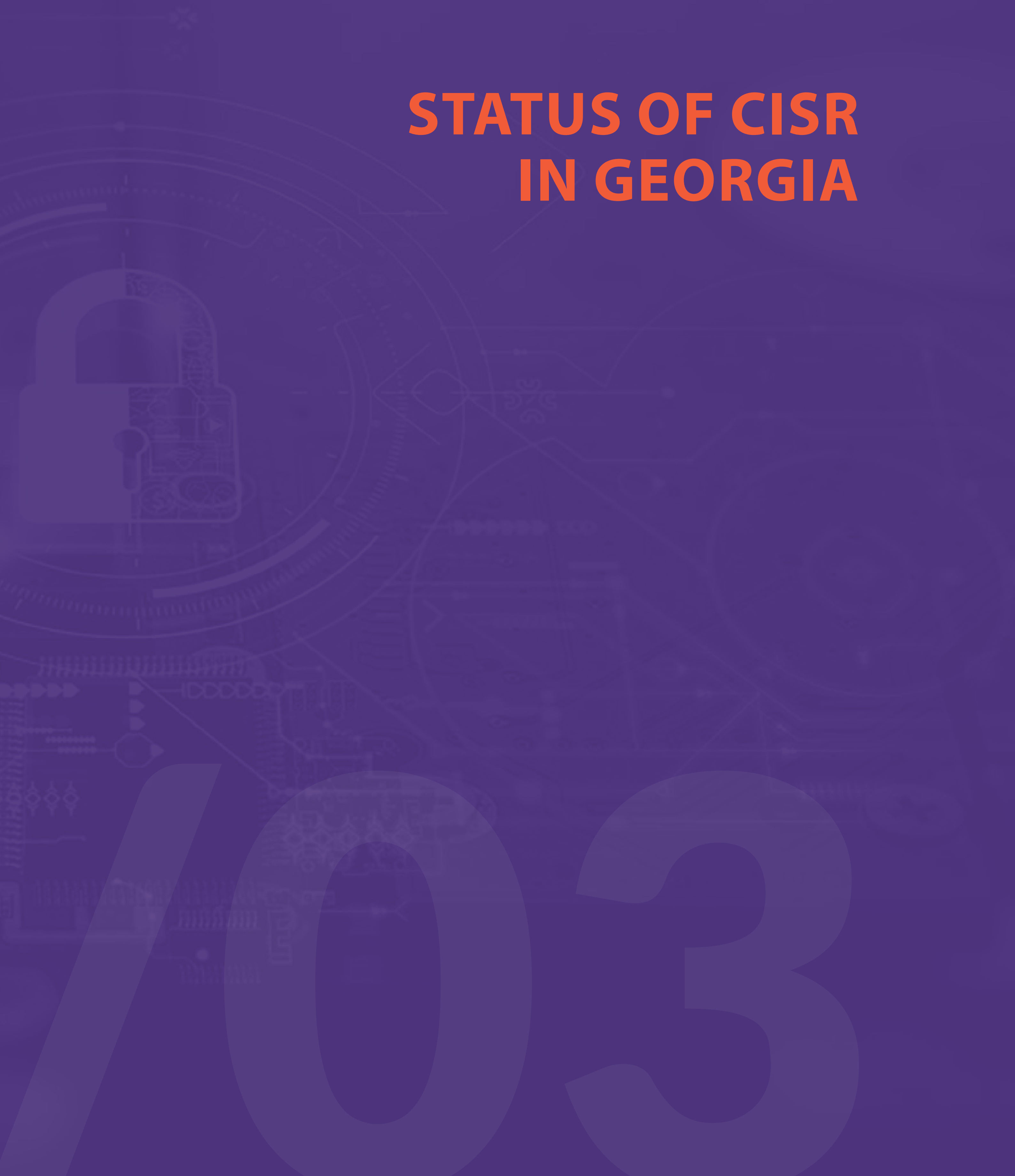
- **Directive 114/08/EC (as the main reference for drafting legislation and describing the initial coordination and cooperation mechanisms);**
- **Directive 2022/2557 (as the main reference for drafting articles related to the obligations of operators/owners of critical infrastructures, including the mandatory notification of incidents of significant relevance).**

Directive 114/08/EC is much more streamlined, having been designed to create the conditions for EU Member States to establish their national frameworks. Meanwhile, Directive 2022/2557 is much more verbose in the areas of risk assessment, security measures, and incident notification mechanisms to be implemented by operators/owners.

Embracing such a blended approach would allow the given country to establish a sound and effective national framework and work on only the most pertinent elements at the beginning of a CIP policy lifecycle.

Among the priorities here, procedures for the identification and designation of national critical infrastructures are the highest priority, since neither public nor private stakeholders could engage in protection-related activities without these being formalized.

STATUS OF CISR IN GEORGIA



/03

3. STATUS OF CISR IN GEORGIA

Having in place a robust CISR policy is of the utmost importance with regard to safeguarding national security and keeping essential services running. This is especially true for countries like Georgia, constantly at risk of renewed military and hybrid aggression from Russia.[27] Since the war in 2008, the Kremlin has established military bases and stationed troops in Georgia's occupied regions including near the Georgian East-West Highway and critical infrastructure such as pipelines that transit oil and natural gas from the Caspian Basin to the West.[28]

More recently, Russia's war on Ukraine has not only increased Georgia's resilience risks due to the unpredictable and fragile security environment in the wider region, but it has also compromised European security order, prompting many nations to reassess their security strategies in response to emerged geopolitical tensions. In particular, Black Sea states are challenged by the threat of Russian malign activity, as well as energy dependence, political fragility, and economic underperformance.[29]

The geopolitical landscape of the South Caucasus has also undergone a significant upheaval in the wake of the most recent war in Nagorno-Karabakh that erupted in September 2020, increasing Russia's military presence in the region and leading to a qualitative shift in regional power.[30]

With extensive experience of Russian military aggression and malign activity in Georgia spanning decades and an immensely unstable geopolitical situation in the region, achieving effective governance of CISR remains a present challenge.

However, Georgia lacks a comprehensive legal framework for identifying, designating, regulating, and protecting such infrastructures. There is no formal list of critical infrastructures in the country, nor is there a clear distribution of responsibilities for their protection. Without proper guidance on what constitutes critical infrastructures, it is challenging to prioritize resources and allocate funds to their protection. This ambiguity also makes it challenging to identify potential threats to critical infrastructure and develop appropriate response measures.

In general, the lack of a definitive list of critical infrastructures and a clear regulatory framework to ensure their security and resilience is a significant gap in Georgia's national security policy. To address this shortcoming, the Georgian government needs to develop new legislation, regulations, and standards to protect its critical infrastructures against potential threats and ensure their resilience in the face of emerging challenges.

In this regard, the Georgian government has been placing a greater emphasis on cybersecurity in recent years,[31] with efforts being made to exploit the country's well-established ICT sector and digital ecosystem, as well as country's strategic priority to establish the country as a digital hub in the region (Europe-Asia digital corridor)[32] against the backdrop of the

[27] See https://mfa.gov.ge/en/national-security-concept

[28] See https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools

[29] See https://www.atlanticcouncil.org/in-depth-research-reports/report/a-security-strategy-for-the-black-sea/#h-iii-regional-challenges-and-threats

[30] https://www.cmi.no/publications/8911-changing-geopolitics-of-the-south-caucasus-after-the-second-karabakh-war

[31] See https://matsne.gov.ge/en/document/view/1679424?publication=3 https://nsc.gov.ge/en/NEWS/georgia-national-cybersecuri.html

[32] see https://pmcg-i.com/publication/georgia-digital-ecosystem-country-assessment-deca/

ongoing risk of cyberattacks from Russia. Recognizing the potential impact of such attacks on national security and the economy, the Georgian government has taken measures to strengthen its cybersecurity dimension, enhance its resilience to cyber threats, and protect its critical assets and operations.

The Law of Georgia on Information Security, which establishes standards for information security, has been in force since 2012. The Law defines the term "critical information system" as an information system whose uninterrupted operation is essential to national defense and/or economic security, as well as to the normal functioning of the state and/or society.

The Law of Georgia on Information Security defines the rights and responsibilities of public and private sectors in the field of information security maintenance, and identifies mechanisms for the exercising of state control of the implementation of information security policy.

On January 1, 2022, significant legislative changes reshaped the legal landscape within the cyber security domain. Among these changes was the expansion of the Law's scope, extending its reach to encompass a broader spectrum of subjects. This expansion necessitated the categorization of relevant critical information system subjects, facilitating more efficient regulation and oversight. Accordingly, coordinating and supervisory agencies were changed.

Specifically, the amendments divide the critical information system subjects into the following three categories:

1st Category

Institution	Supervisory Body
Public entities and state-owned enterprises	LEPL Operational-Technical Agency

2nd Category

Institution	Supervisory Body
Internet Service Providers	LEPL Operational-Technical Agency

3rd Category

Institution	Supervisory Body
Insurance, Transportation and Energy companies;	LEPL Digital Governance Agency
Commercial Banks	LEPL Digital Governance Agency; and National Bank of Georgia

Fig. 4 "Categories of critical information systems according to the Law of Georgia on Information Security"

Furthermore, the legislative amendments include the establishment of administrative sanctions for non-compliance with the Law's requirements. These sanctions are designed to enhance regulatory effectiveness and ensure adherence to legal obligations. Previously, the lack of this type of legal responsibility negatively affected the enforcement of cybersecurity legislation not only within private sector, but in public sector as well.

It should be emphasized that in 2012-2021, Georgia experienced certain problems in the enforcement of the Law on Information Security. In particular, developing a comprehensive regulatory framework for information security and defining critical information infrastructure posed a significant challenge during the Law's implementation.[33]

It's worth noting that the Georgian CSOs have heavily criticized the amendments, arguing that they provide the LEPL Technical-Operative Agency under the State Security Service, Georgia's chief domestic intelligence body, with unrestricted access to the information of

[33] See https://idfi.ge/public/upload/GG/CyberN333.pdf

public agencies and telecommunications companies.[34] Furthermore, while one of the primary objectives of the amendments was to introduce a new system of categorization for critical information infrastructure subjects, they lack transparency regarding the fundamental principles and criteria used for such classification.

Nevertheless, in light of the previous shortcomings and contradictions in the Law, the amendments represent a significant advance toward aligning with EU standards and establishing a more robust framework governing cybersecurity.[35]

Despite considerable efforts being devoted to maintaining cybersecurity, there exists a significant void in the regulatory principles and legislative framework with regard to national critical infrastructure security and resilience. This encompasses all aspects of security and resilience, indicating that current endeavors in cybersecurity may be falling short of addressing the broader challenges and risks facing critical infrastructure systems, including physical security, supply chain security, and personnel security. This inadequacy impedes Georgia's ability to address the multifaceted risks faced by critical infrastructure systems effectively.

Although the critical infrastructure domain in Georgia is not yet properly regulated, the Georgian legislation does contain several related terms, including "property of special importance" and " Subjects with High Risk for State Security ".

Law on State Property	Definitively lists state properties not to be subject to privatization
List of Subjects of High Risk to State Security	The State Security Service of Georgia (SSSG) is responsible for securing entities of high importance to national security. Although the SSSG is authorized to establish safety regimes and control the protection of such entities, this does not constitute a modern model for managing critical infrastructure
List of Property of Special Importance in the Civil Aviation Sector	Approved by the Order of the Minister of Economic Development of Georgia in 2010

Fig. 5 "Pertinent laws in Georgia in the area of CIP"

Despite the growing importance of CISR today, Georgia still lacks a comprehensive approach thereto. Instead, the country takes a fragmented approach, focusing on sector-specific measures and regulations, which do not fully address the complex and interconnected nature of critical infrastructure.

CISR is essential not only for national security but also for fostering economic development and stability. Given Georgia's relatively small economy, it heavily depends on foreign investment. As such, attracting and supporting foreign investors represents a central goal of economic policy. However, at the same time, it is imperative that robust formal mechanisms are in place to shield the nation from investments or investors that could pose risks to national security. Thus, investment screening is an integral part of CISR reform. On one hand, this safeguards the nation's vital interests, while on the other it fosters secure and transparent climate for foreign investment. Of note, Georgia's "Promotion and Guarantees of Investment Activity" framework is broad, outdated, and fails to tackle the contemporary challenges and realities of the investment landscape.

[34] See https://idfi.ge/en/the_parliament_of_the_10_convocation_adopted_the_problematic_draft_law_on_information_security_

[35] See https://twitter.com/MarkClaytonFCDO/status/1403286833644150784

The case of the acquisition of Caucasus Online, a leading internet service provider (ISP) in Georgia and a major owner and operator of submarine fiber optic cables that connect Georgia to the worldwide web, led to extraordinary amendments being made to the Law on Electronic Communications in September 2020.[36]

The Caucasus Online case serves as a vivid example of the threats posed by not having a dedicated legislative framework pertaining to critical infrastructure, including investment policy. Such a scenario, over time, has the potential to threaten the interests of the state while simultaneously impeding the growth of private enterprises and deterring foreign investors.[37]

Without a holistic approach to CISR, Georgia is at risk of experiencing major disruptions that could have serious consequences for the country's economy, public safety, and overall stability. Moreover, these disruptions could also have regional and even global implications, given Georgia's strategic location at the crossroads of Europe and Asia.

In October 2018, the Government of Georgia established an interagency commission tasked with developing a legislative framework for CIP. The responsibility for providing organizational and technical support to this commission was assigned to the Ministry of Internal Affairs.[38] Later, in 2020, this function was transferred to the Office of the National Security Council.[39] The interagency commission, in its endeavors to establish a legislative framework for CIP, succeeded in developing a draft law. The Government of Georgia has since put its plans to establish a CIP framework on hold. Thus, the commission's progress has been hampered, and the project is at a standstill, with no notable advancements made beyond the initial draft law.

(3.1) KEY PLAYERS IN CISR REFORM IN GEORGIA: POLICY AND GOVERNANCE LEVELS

(3.1.1) NATIONAL SECURITY COUNCIL

The National Security Council is a consultative body directly subordinated to the Prime Minister of Georgia, making the highest-level decisions on national security issues. The Council is the main coordinating institution in the field of national security policy planning. It is headed by the Prime-Minister of Georgia. Information-analytical and organizational support to the National Security Council is provided by the National Security Council's Office.

(3.1.2) THE DEFENCE AND SECURITY COMMITTEE OF THE PARLIAMENT OF GEORGIA

The Defence and Security Committee of the Parliament of Georgia is responsible for overseeing matters related to national defense, security, and law enforcement. The Committee was established in 1995 and operates under the supervision of the Georgian Parliament.

The Committee's main responsibilities include drafting and reviewing legislation related to defense, security, and law enforcement, as well as monitoring the activities of relevant government agencies and providing oversight on their budgets and operations. The Committee also plays a role in shaping national defense and security policy, and in assessing the country's preparedness to respond to internal and external threats.

[36] See https://idfi.ge/en/analysis_of_the_venice_commission_report

[37] See https://forbes.ge/a-law-for-one-the-case-of-caucasus-online/

[38] See https://www.gov.ge/files/495_68573_326517_2033.pdf

[39] See https://nsc.gov.ge/en/NEWS/first-session-of-the-inter-age.html

(3.2) RELEVANT EVENTS IN GEORGIA WITH IMPACTS ON CRITICAL INFRASTRUCTURES AND ESSENTIAL SERVICES

The following sections present a short review of some events to have significantly influenced both the security landscape and economic development of Georgia in its recent history.

These sections are intended to raise awareness and inspire collective action, aiming to prevent or alleviate similar occurrences through critical infrastructure reform and the active engagement of relevant stakeholders.

(3.2.1) GEORGIA'S ENERGY CRISIS IN 2006

Russia imposed an energy blockade against Georgia in 2006[40], starting in January 2006 and lasting several weeks. The primary aim of the blockade was to put pressure on Georgia, which Russia perceived to be moving closer to the West.

Until 2006, Russia was the primary supplier of natural gas to Georgia. The gas was transported via a pipeline passing through Russian territory and then through Georgia. In the winter of 2006, two gas pipelines and a high-voltage power line were blown up on Russian territory very close to Georgian border. This disrupted all connected thermal power stations, and the hydropower plants (HPPs) could not withstand the additional burden. As a result, Georgia as a whole was left without power for days. Russia cited the need for repairs to the pipeline.

Russia's restriction of the gas supply caused an energy crisis in Georgia. Many households were left without heat, and some businesses were forced to close. The price of gas also tripled in the months following the crisis, as Georgia was forced to seek alternative sources and diversify its energy supply.

The energy crisis had a significant impact on the Georgian economy, and the Georgian government at the time accused Russia of using its control over gas supplies as a political tool to put pressure on Georgia. In response, the Russian government denied any wrongdoing, and suggested that the blasts might be attributed to extremists intent on exacerbating tensions between Russia and Georgia.[41]

In the aftermath of the crisis, Georgia sought to reduce its energy dependence on Russia, exploring alternative sources of gas and developing new energy infrastructure.[42] Russian use of its gas supplies as a means of economic warfare against Europe—designed to undermine

NATO unity and support for Ukraine—is another example of why adversaries, nation-states, and terrorists alike target critical infrastructure.[43]

(3.2.2) THE IMPACT OF CYBER WARFARE ON NCI DURING THE 2008 RUSSO-GEORGIAN WAR

The 2008 Russo-Georgian War marked the first instance of cyberattacks being used alongside traditional military operations, setting a precedent for future conflicts.[44]

[40] See https://www.rferl.org/a/1064976.html

[41] See https://www.theguardian.com/world/2006/jan/23/russia.georgia

[42] See https://eurasianet.org/gas-crisis-over-georgia-vows-to-diversify-energy-supplies

[43] See "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)" Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner - USAWC Press - US Army War College – 15/11/2022.

[44] See https://gfsis.org.ge/cbgl/blog/view/970

In addition to the conventional attacks launched by Russian land, naval, and air forces during the 2008 war, a massive DDoS attack was launched against Georgia's communication grids, paralyzing the banking sector, transport companies, telecommunications providers, and government websites. The objective here was to facilitate Russia's execution of military objectives, establish an information vacuum, attain information superiority, and promote the Russian narrative about the conflict[45] according to which the intervention of Russian military forces was necessary to "stop the bloodshed and the ethnic cleansing of the Ossetian population."

At the time, the Georgian government responded to the cyberattacks by seeking assistance from partner countries and organizations. The US and Estonia provided technical expertise and assistance to help Georgia secure its information systems and recover from the attacks. Nevertheless, the cyberattacks had a significant impact on Georgia's infrastructure and information systems, causing widespread disruption and damage.

(3.2.3) CYBERATTACKS ON GEORGIA'S DIGITAL ECOSYSTEM AND INFORMATION OPERATIONS AGAINST HEALTHCARE SECTOR

In October 2019, Georgia endured a number of significant cyberattacks. These incidents disrupted the operations of thousands Georgian government and privately-run websites, and interrupted the broadcasts of at least two major television stations, thus directly impacting the Georgian population.[46]

The cyberattacks targeted Georgia's national security, and intended to harm Georgian citizens and government structures by disrupting and paralyzing the functionality of various organizations, thereby fueling anxiety among the general public.[47] The corresponding investigation conducted by the Georgian authorities, together with information gathered through cooperation with partners, concluded that these cyberattacks had been planned and carried out by the Main Division of the General Staff of the Armed Forces of the Russian Federation, known as "Sandworm," which has been linked to several high-profile attacks on government agencies and critical infrastructures in various countries.[48]

In September 2020, another large-scale cyberattack targeted the ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia. The attack resulted in the theft of sensitive personal information belonging to thousands of patients, including medical records and personal identification data.[49]

The main objective of the cyberattack was to unlawfully obtain and utilize documents belonging to the central office of the Ministry and its subordinate units, including the National Center for Disease Control and Public Health and the Richard Lugar Research Center, as well as important information on the management of the COVID-19 pandemic. Some documents obtained via the cyberattack were uploaded on a foreign website and thus publicly available. In addition, with the aim of intimidating society and fostering confusion and distrust, falsified documents were also uploaded on the same website.[50] The attack had severe consequences for the Georgian healthcare system, with medical professionals unable to access patient records and critical services disrupted.

Based on the evidence obtained during the subsequent investigation, the Ministry of Internal Affairs attributed the cyberattack to foreign special services. Although it did not specify

[45] See https://idfi.ge/en/how_russian_disinformation_tactics_were_utilised_in_the_context_of_the_2008_5_day_war

[46] See https://osce.usmission.gov/u-s-condemnation-of-russian-cyber-attack-on georgia/#:~:text=On%20October%2028%2C%202019%2C%20as,against%20the%20country%20of%20Georgia.

[47] See https://georgiaembassyusa.org/2020/03/02/georgia-is-targeted-by-russia-in-a-disruptive-cyber-attack/

[48] See https://edition.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html

[49] See https://police.ge/en/saqartvelos-shinagan-saqmeta-saministros-gantskhadeba/13926

[50] See https://idfi.ge/en/strategy_of_russian_cyber_operations

the country from which the cyberattack was carried out, the processes and disinformation campaign that preceded the accident indicate the high probability of this being Russia.[51] In Russian hybrid warfare tactics, information is weaponized to influence operations, aiming to weaken the targeted societies through inciting social unrest, polarization, and undermining trust in government institutions and democracy, where cyber means are the primary instruments.[52] In particular, there have been disinformation campaigns led by Russian state-controlled media and security forces targeting the Richard G. Lugar Center for Public Health Research,[53] which is the highest-level institution in Georgia's laboratory network and the referral laboratory of the public health system.[54] The Center is part of a joint project between the Georgian and American governments.

Here, the campaigns have sought to undermine the credibility of the laboratory by spreading false narratives about its activities and disseminating conspiracy theories. These narratives often accuse the Center of engaging in covert activities, such as the creation and spread of biological weapons or conducting unethical experiments. However, these claims lack credible evidence and are widely regarded as part of a disinformation campaign.[55]

(3.2.4) RUSSIA'S COERCIVE ECONOMIC TACTICS: THE NAMAKHVANI HPP CASE

Russia's use of hybrid strategies has grown markedly in recent years. Information operations, alongside economic and political influences, constitute key components of Russia's hybrid warfare toolkit, employed to advance Russian national interests.[56]

Field experts have highlighted the Namakhvani HPP case as an example of Russia contributing to impeding a crucial energy infrastructure project in Georgia through propaganda and coercive economic tactics.[57]

Crucially, the Namakhvani project exposed numerous systemic shortcomings in Georgia's state policy on hydro resource management, as well as legal failings and unsubstantiated, nebulous concessions, triggering significant opposition from local communities, environmental activists, and international organizations alike. These groups of stakeholders subsequently raised concerns regarding the project's potential environmental and social repercussions. In particular, environmental groups conducted thorough analysis, pointing out that environmental considerations had been neglected throughout the planning and execution of the project, as well as highlighting violations of constitutional and property rights of the affected communities and citizens. Furthermore, revelations of infringements of rights pertaining to access to environmental information, participation in decision-making processes, and a safe living environment sparked widespread protests across Georgia. Compounding these issues, the Georgian government's shortcomings in its strategic communication with the local population escalated tensions further.[58]

When there are flaws in good governance, which could stem from either incompetence, unprofessionalism or deliberate actions, potentially serving as enablers of hybrid warfare (a subject meriting detailed examination in separate research). In this particular case, pro-Russian political activists and proxies managed to effectively leverage these governance short-

[51] See https://idfi.ge/en/strategy_of_russian_cyber_operations

[52] See https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

[53] See https://gfsis.org.ge/files/library/opinion-papers/144-expert-opinion-eng.pdf

[54] See https://ncdc.ge/#/pages/content/2fd8140d-956a-45a0-bc6c-63f9fdd63346

[55] See https://www.pmcresearch.org/policypapers_file/f6ac5dfb34c12e31c.pdf

[56] See https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

[57] See https://mdfgeorgia.ge/uploads//Russian_and_Chinese_influences_in_Georgia-2021_update.pdf

[58] See https://greenalt.org/en/statement-on-the-construction-of-namakhvani-hpp-cascade/

comings to their advantage. Malevolent actors capitalized on this scenario to cultivate public distrust toward the national government, instill fear about foreign acquisition of Georgian land, and stoke anti-Turkish sentiments (as the investor, ENKA Renewables LLC, was a Turkish industrial conglomerate).

After long and complex negotiations between opponents of the project and the Georgian government mediated by the Energy Community Secretariat, the contract between ENKA Renewables LLC and the Georgian government to build and operate the Namakhvani HPP in western Georgia (a project worth USD 800 million) was terminated.[59]

The cancellation of the Namakhvani HPP project not only directly affects Georgia's energy independence and security, but also carries significant economic consequences. It tarnishes Georgia's reputation as a reliable partner and undermines the nation's investment climate, deterring much-needed foreign direct investment (FDI), essential for the country's ongoing economic advancement.

3.2.5 CONCLUSIONS

The events highlighted in this chapter and elaborated on throughout the report emphasize the imperative of formulating an overarching CISR policy. Such a policy, once established, will play an indispensable role in safeguarding essential services and guaranteeing that any new projects affecting critical infrastructure sectors undergo thorough analysis and adhere to transparent procedures throughout their planning and implementation phases. Indeed, a robust national framework for CISR can serve as the cornerstone of effective governance in the rapidly developing domain of national security.

In Georgia today, the absence of a holistic approach to CISR is compounded by significant deficiencies across multiple fronts. Primarily, there persists a notable lack of foundational understanding regarding critical infrastructure among public servants, industry stakeholders, media outlets, and the general public. Furthermore, measures aimed at combating disinformation and enhancing public awareness concerning information warfare are insufficient,[60] while information sharing and collaboration among public and private entities are ineffective. These inadequacies further weaken Georgia's resilience against emerging threats. Addressing these interconnected challenges demands a holistic effort to develop policy frameworks, improve educational outreach, and foster greater cooperation among all of Georgia's CISR stakeholders.

[59] See https://civil.ge/archives/481355

[60] https://www.transparency.ge/en/post/spreading-disinformation-georgia-state-approach-and-countermeasures

LESSONS LEARNED FROM OTHER COUNTRIES

/04

4. LESSONS LEARNED FROM OTHER COUNTRIES

In the ever-evolving landscape of security and technology, CISR has become a paramount concern for countries worldwide. As nations embark on reforming their CISR strategies, it is imperative to learn from the experiences of other countries, with a focus on the following aspects:

1. Global interconnectedness[61];
2. Diverse threat landscapes[62];
3. Resources optimization and allocation[63];
4. Existing regulatory frameworks[64];
5. Public-private partnership models[65];
6. Crisis management and resilience approaches[66].

A collaborative approach to CISR is essential for countries initiating reforms in this domain. By drawing on the experiences of other nations, policymakers can improve their strategies, foster cooperation, and safeguard the backbone of modern societies. As threats to critical infrastructure continue to evolve, the ability to adapt and learn from others becomes an indispensable aspect of national security.

To provide a high-level comparison with countries that have efficiently and effectively reformed their national CISR frameworks, the cases of Croatia and Romania are described in the following chapters.

(4.1) THE CASE OF CROATIA

In 2013, Croatia joined the EU and, in compliance with Council Directive 2008/114/EC, enacted the Critical Infrastructure Act to regulate the identification and protection of European critical infrastructure. Before this, Croatia had recognized the importance of critical infrastructure in strategic documents such as the National Strategy for the Prevention and Countering of Terrorism (2008) and the Protection and Rescue Plan (2010).

[61] Critical infrastructure is often interconnected across borders. By examining the experiences of other nations, policymakers can gain insights into potential vulnerabilities, collaborative solutions, and shared best practices that transcend geographical boundaries.

[62] Countries face a multitude of threats, ranging from cyberattacks to natural disasters and terrorism. Analyzing how other nations have tackled diverse threats allows for a more comprehensive understanding of potential risks and effective mitigation strategies.

[63] Implementing and maintaining a robust CIP framework requires substantial resources. Learning from the successes and failures of other countries enables policymakers to optimize resource allocation.

[64] Examining the regulatory frameworks of countries to have enjoyed successful CISR implementation provides a blueprint for designing effective legislation.

[65] CISR often involves collaboration between government entities and private stakeholders. Studying how other countries have fostered successful public-private partnerships can offer an understanding of the dynamics of co-operation and information-sharing.

[66] Understanding how other nations have responded to and recovered from significant disruptions to critical infrastructure helps in developing effective response plans.

Before 2013, CIP in the country was addressed through various legal solutions, including the Police Act and intelligence system regulations. Notably, the Ministry of Defense coordinated the protection of objects important for defense. In addition, the Private Protection Law empowered private security companies to contribute to CIP.

Despite some attention already being paid to critical infrastructure up until this point, Croatia lacked a comprehensive legal framework. The Critical Infrastructure Act of 2013[67] initiated a reconceptualization process to align with EU guidelines. The Act defines national critical infrastructure and outlines the responsibilities of the Croatian government, administrative bodies, and owners/managers.

Under this Act, two significant subordinate documents were introduced: the Decision on Designation of Sectors[68]; The Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure.[69] These documents identify 11 critical sectors, depicted as follows:

ENERGY	COMMUNICATION AND ICT	WATER MANAGEMENT	TRANSPORT	HEALTH	FINANCE
• Production, including reservoirs and dams; • Transmission; • Storage; • Transportation fuels; • Energy distribution Systems	• Electronic communication; • Data transmission; • Information systems providing audio and audiovisual media services	• Control and protective water structures; • Municipal water structures	• Road transport; • Railway transport; • Air transport; • Sea and inland waterways	• Healthcare; • Manufacturing; • Marketing and supervision of medicinal products	• Banking; • Stock Exchange; • Investment; • Insurance; • Payment Systems

PUBLIC SECTOR	NATIONAL CULTURAL HERITAGE	SCIENCE AND EDUCATION	FOOD	PRODUCTION, STORAGE, AND TRANSPORT OF DANGEROUS GOODS
• Ensuring public order; • Police and rescue services; • Emergency medical services	• National monuments and valuables	• Science; • Education	• Production and food supply; • Food safety system; • Stockpiles	• Chemical, biological, radiological and nuclear materials

Fig. 6 "Sectors and subsectors of Croatia's national critical infrastructure"

[67] Critical infrastructure act, 2013, in Official Gazette, No 56/2013 (Croat.), http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama.

[68] Decision on Designation the Sectors, in Official Gazette, No 108/2013 (Croat.), http://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html

[69] Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure,in Official Gazette, No 47/2016 (Croat.), http://www.poslovni-savjetnik.com/propisi/pravilnik-o-metodologiji-za-izradu-analize-rizika-poslovanja-kriticnih-infrastruktura-vazeci

The Rules provide guidelines for risk analysis, in line with international standards like ISO 31000:2009.

While the normative structure has proved challenging, Croatia is continually improving its CIP framework. Its implementation of Council Directive 2008/114/EC involved identifying critical infrastructure in 11 sectors, a task requiring careful consideration.

Croatia, in its alignment with Council Directive 2008/114/EC, has established a normative framework for CIP. This has included organizing training for security coordinators and engaging with neighboring countries on the identification of European critical infrastructures.

With regard to the identification of critical infrastructures, the adoption of the Decision on cross-sectoral criteria in 2016 eased the process. The significance of the CIP system at the national level has been emphasized through the implementation of the EPCIP and EU cybersecurity policy packages.

In 2017, two key national security documents, National Security Strategy[70] and the Homeland Security Act, prioritized critical infrastructure. Meanwhile, implementing the EU cybersecurity policy package led to the adoption of the National Cyber Security Strategy in 2015, with the subsequent transposition of the NIS Directive through the 2018 Act on the Cyber Security of Operators of Essential Services and Digital Services Providers.

The strategic direction taken here aligns with EU guidelines, facilitating cooperation between state bodies. Pertinently, the Critical Infrastructure and Cultural Heritage Department was established within the Civil Protection Directorate of the Ministry of Interior in 2019. This enhances coordination and fosters cooperation with ministries in charge of the identified sectors.

At the same time, the process of revising the Critical Infrastructure Act is underway, with a focus on involving relevant stakeholders to shape an optimal and more efficient system. Public-private partnerships have also been identified as a crucial component of the national approach.

The private sector, often owning and managing critical infrastructures, bears responsibility for efficient protection and resilience. This requires collaboration with public institutions, emphasizing that safeguarding critical infrastructure is a joint task of both public and private sectors. Of note, challenges arise in developing common procedures, defining roles and responsibilities through legislation, exchanging sensitive data, building trust, and sharing knowledge and experiences.

While Croatia has a normative model for public-private partnership, the existing Public-Private Partnership Act, focuses on construction and maintenance, and requires modification to meet the diverse needs of critical infrastructure. Accordingly, amendments to the Critical Infrastructure Act should incorporate the concept of public-private partnership.

The exchange of stakeholders' opinions and knowledge occurs through national and international conferences organized by various institutions in Croatia, fostering greater collaboration and awareness.

Challenges have arisen with state-owned companies that prioritize political and economic goals over business continuity, while profit-focused private companies may neglect CISR. Therefore, raising awareness about the consequences of critical infrastructure disruption is essential to ensure a unified approach to CISR.

[70] See https://www.morh.hr/wp-content/uploads/2018/04/strategy_18012018.pdf

(4.2) THE CASE OF ROMANIA

The evolution of Romania's critical infrastructure domain serves as a compelling example of how a whole-of-government approach and consistent policy formulation can lead to the successful achievement of challenging reform objectives. The Romanian approach, characterized by its incorporation of a comprehensive set of legal and structural reforms, not only underscores the Romanian government's commitment but also highlights its capacity to foster the establishment and sustained growth of a robust CISR system, poised to effectively address ever-evolving challenges while fortifying the resilience of the critical infrastructure domain.

In 2008, following the enactment of Council Directive 2008/114/EC, which delineated procedures for the identification and designation of critical infrastructures within the EU, along with an assessment of the need to enhance their protection, the Romanian government embarked on a proactive journey. Subsequently, in 2010, Romania formally transposed Directive 2008/114/EC into its national legislation through the enactment of Government Emergency Ordinance No. 98/2010,[71] specifically addressing the identification, designation, and safeguarding of critical infrastructures, commonly referred to as "GEO 98/2010." The Ordinance defines national critical infrastructure (hereinafter referred to as "NCI") as an element, a system, or a component located on the national territory, which is essential for maintaining the vital functions of society, health, safety, security, social, or economic well-being of persons, and the disturbance or destruction of which would have a significant impact at the national level in terms of maintaining those functions and safeguarding the national interest. According to the Ordinance, if the disruption or destruction of NCI would have a significant impact on at least two EU Member States, those types of critical infrastructure should be identified as European critical infrastructure (ECI). "GEO 98/2010" also defines sectors and subsectors of Romanian national critical infrastructure as follows:

ENERGY	ICT	WATER, LAND, AND THE ENVIRONMENT	TRANSPORT	HEALTH	NATIONAL SECURITY
• Electricity; • Oil and petroleum derivatives; • Natural gases and derivatives; • Mineral resources	• Electronic comms systems and services; • Data processing and storage systems, cybersecurity infrastructures; • Radio/TV broadcasting infrastructures • Postal services at the national level	• Supply of drinking water; • Sewage; • Quality and quantitative control of water; • Environmental protection; • Protection of forestry and hunting	• Road transport; • Railway transport; • Air transport; • Water transport	• Medical and hospital care; • Medicines; • serums, vaccines and pharmaceuticals; • Bio-laboratories and bio-agents • Emergency medical and sanitary transport services	• Defense of the country public order, national security; • Borders, migration, asylum; • National security industry, production, storage facilities and capacities; • Emergency situations and Justice and penitentiary
ADMINISTRATION	**FOOD AND AGRICULTURE**	**INDUSTRY**	**SPACE AND RESEARCH**	**FINANCE/ BANKING**	**NATIONAL CULTURAL HERITAGE**
• Public administration	• Food production and supply; • Food safety and security	• Production, processing, storage and use of chemical and Nuclear radioactive materials; • Pipes carrying hazardous chemical Products	• Space and Research	• Taxes and fees; • Insurance; • Banks • Stock exchanges, Cash and payment Systems	• Public Cultural institutes

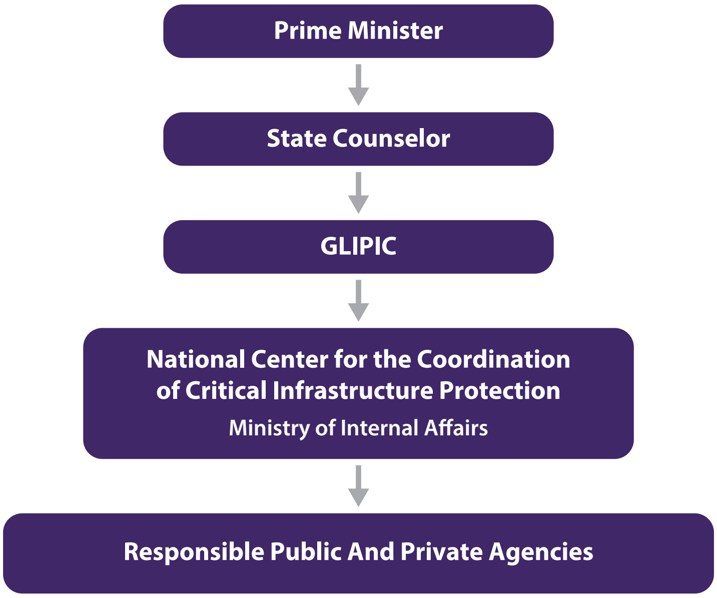
Fig. 7 "Sectors and subsectors of Romanian national critical infrastructure"

[71] See https://cncpic.mai.gov.ro/sites/default/files/2020-01/OUG%20no.98%20engleza.pdf

"GEO 98/2010" establishes a governance framework for NCI as well. According to its 4th article, coordination, at the national level, of activities regarding the identification, designation, and protection of NCI and ECI are carried out by the Prime Minister, through the designated state counselor. Alongside legal and structural reforms to ensure the effective implementation of the new legislation, the Romanian government adopted a centralized and comprehensive whole-of-government approach, recognizing the paramount importance of enacting reform. On 3 November 2010, the Government's Decision No. 1,110 established the inter-institutional working group[72] for CIP, known as "GLIPIC."[73] GLIPIC's primary mission is to facilitate coherent and unified coordination of activities in CIP. It is tasked with devising a well-informed and adaptable development strategy for the field, conducting cross-sectoral assessments of vulnerabilities, risks, and threats to critical infrastructures, and providing the Romanian government with updates on ongoing activities and recommended measures to enhance operations in this domain.

The Ordinance also establishes the National Center for Coordinating Critical Infrastructure Protection[74] (CNCPIC). The Center is a structural unit of the Ministry of Internal Affairs, has operational authority and is tasked with orchestrating and executing essential activities required for the enactment of legislation pertaining to CIP.

The CNCPIC supports the responsible authorities[75] and critical infrastructure owners/operators/administrators[76] by providing them with access to information on best practices and methods, and by facilitating participation in coordinated actions by the European Commission in the field of training and the exchange of information on new developments in CIP, and organizing public-private partnerships.


Prime Minister

State Counselor

GLIPIC

National Center for the Coordination of Critical Infrastructure Protection
Ministry of Internal Affairs

Responsible Public And Private Agencies

Fig. 8 "CISR governance model in Romania"

[72] See https://cncpic.mai.gov.ro/en/node/31531

[73] See https://cncpic.mai.gov.ro/en/node/31531

[74] See https://cncpic.mai.gov.ro/en/node/31531

[75] A public institution designated under the conditions of the Government Emergency Ordinance No. 98/2010, which, according to the legal competences and powers, is responsible for organizing and carrying out activities in the fields corresponding to critical infrastructure sectors and subsectors.

[76] Owners/operators/managers of NCI/ECI are those entities in charge of investment in an item, system, or component thereof, designated as NCI/ECI, according to the Government Emergency Ordinance No. 98/2010, and/or in charge of the current operation/management thereof.

The Romanian legislation also defines the responsible public authorities for each NCI Sector as follows:

SECTOR	RESPONSIBLE PUBLIC AUTHORITIES
Energy	The Ministry of Economy and the Ministry of Energy

ICT	The Ministry of Communications and Information Society;
	The Special Telecommunications Service;
	The Foreign Intelligence Service;
	The Service Romanian Intelligence

Water, Land and the Environment	The Ministry of Regional Development and Public Administration;
	The Ministry of Health;
	The Ministry of Waters and Forests;
	The Ministry of the Environment;
	The Ministry of Agriculture and Rural Development

Food and Agriculture	The Ministry of Agriculture and Rural Development; The National Sanitary Veterinary and Food Safety Authority
Health	The Ministry of Health; The Ministry of National Defense

National Security	The Ministry of National Defense;
	The Ministry of Internal Affairs;
	The Ministry of Economy;
	The Ministry of Justice;
	The Special Telecommunications Service;
	The Foreign Intelligence Service;
	The Romanian Intelligence Service

Administration	The Ministry of Regional Development and Public Administration
Transport	The Ministry of Transport
Industry	The Ministry of Economy

Space and Research	The Ministry of Research and Innovation;
	The Ministry of National Education;
	The Romanian Space Agency

Finance/Banking	The Ministry of Public Finance; The National Bank of Romania
National Cultural Heritage	The Ministry of Culture and National Identity

Fig. 9 "Responsible public authorities for each national critical infrastructure sector"

The sector-specific criteria and critical thresholds for identifying NCI are established by orders of the responsible public authorities. "GEO 98/2010" obliges each responsible public authority, as well as each owner/operator/administrator of NCI/ECI who has more than one NCI/ECI responsibility, to set up a specialized structure in the NCI/ECI field, playing the role of a contact point for critical infrastructure security issues between the owners/operators/administrators of NCI/ECI and the responsible public authorities. On the other hand, responsible public authorities and the owners/operators/administrators of NCI/ECI with responsibility for a single NCI/ECI, are only required to appoint a liaison officer. These provisions ensure coherent and consistent coordination, promoting effective communication and security measures under the framework established by GEO 98/2010.

(4.3) CONCLUSIONS

Growing threats, including natural disasters, terrorism, and hybrid and cyber threats, underscore the increasing need to protect national critical infrastructures. Over the last 20 years, most national critical infrastructure policies and strategies in the West have evolved from focusing solely on the protection of critical infrastructure to making it more secure and resilient.[77] The key to successful security and resilience lies in establishing an effective balance between normative solutions, implementing bodies, and field experts. This requires a primary focus on prevention, preparedness, and cooperation at all levels.

Most states already prioritize the protection of infrastructure crucial to national interests, even if this not explicitly labelled as critical infrastructure. Embracing the critical infrastructure concept, from the EU perspective, should entail harmonization with existing national efforts, with an emphasis placed on understanding, political support, and implementation synergy. While critical infrastructure is perceived primarily from a national security standpoint, the broader perspective involves international communities and cross-border cooperation to create a more resilient global network.

As new security challenges emerge, continuous upgrading and improvement of CIP systems is essential, regardless of the individual country's stage of development. Establishing and maintaining an efficient system demands significant energy, knowledge, continuous investment, and a heightened emphasis on the human factor. Managing this system requires national strategic documents, sector-specific action plans, and coordinated activities across all actors.

Despite the challenges involved, all countries should aspire to establish a comprehensive and well-coordinated CISR system. Strengthening the critical infrastructure system requires ongoing cooperation with other countries, various institutions, and the private sector to leverage knowledge and best practices. In an era marked by climate change and cyber threats, anticipating every potential shock or stressor is of course impossible. Thus, it becomes paramount for stakeholders in critical infrastructure to ready themselves as much as possible for foreseeable threats, while maintaining agility to counter the unforeseen. By doing so, they will ensure the continuous provision of vital services on which society relies.

[77] See "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)" Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner - USAWC Press - US Army War College – 15/11/2022.

Research

A PROPOSAL FOR A CISR ROADMAP FOR GEORGIA

/05

5. A PROPOSAL FOR A CISR ROADMAP FOR GEORGIA

The previous chapters have provided indicators and benchmarks to be taken into consideration when establishing or reforming a national CISR framework. The cases of Croatia and Romania, along with considerations regarding a so-called "blended" approach respectively based the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and Directive 2022/2557 on the resilience of critical entities, provide enough food for thought to streamline a high-level approach that should enlighten policymakers to establish a reform suitable to the specific needs of Georgia.

Given the fact that such a reform will pose challenges for both the public and private sectors that will have to embrace and execute certain duties, it is advisable to implement an approach that minimizes bureaucracy and maximizes impacts. The overriding objective, in fact, should be to put conditions in place to allow CISR to mature. Such an objective can only be achieved if governance is sound, and if the duties of owners/operators are clearly established.

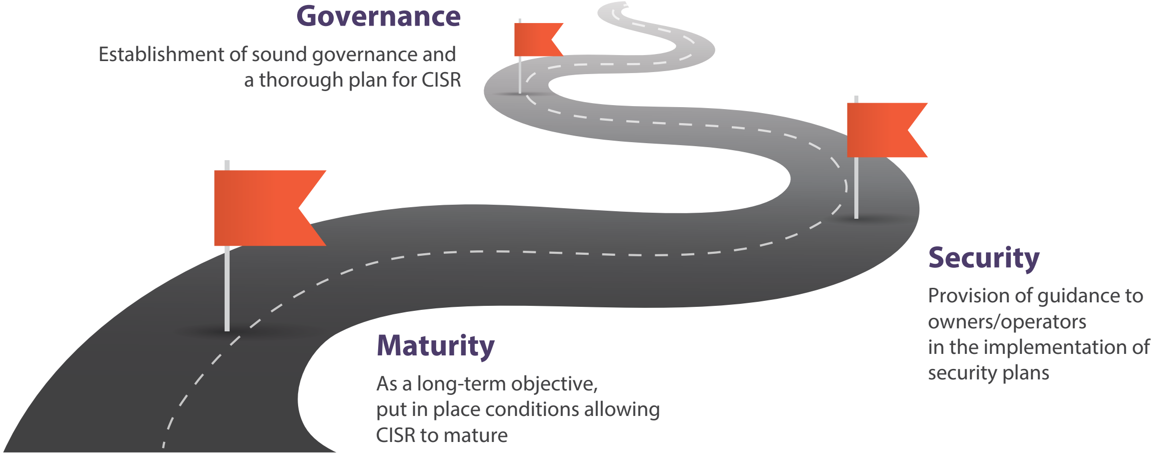

Governance
Establishment of sound governance and a thorough plan for CISR
Security
Provision of guidance to owners/operators in the implementation of security plans
Maturity
As a long-term objective, put in place conditions allowing CISR to mature

Fig. 10 "Initial pillars of the CISR reform in Georgia"

(5.1) POLICY LIFECYCLE

A policy lifecycle encompasses the stages of development, implementation, evaluation, and revision, ultimately forming a continuous and iterative process through which to address and adapt to changing needs and circumstances.

In the context of CISR, the policy lifecycle should be structured around the following phases:

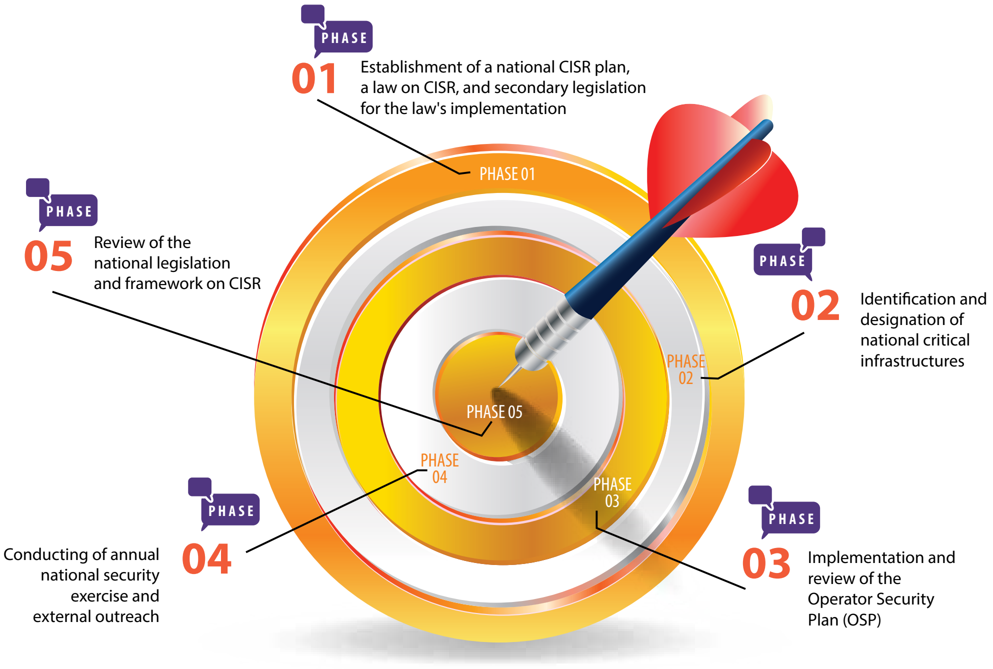

PHASE
01
Establishment of a national CISR plan, a law on CISR, and secondary legislation for the law's implementation
PHASE
02
Identification and designation of national critical infrastructures
PHASE
03
Implementation and review of the Operator Security Plan (OSP)
PHASE
04
Conducting of annual national security exercise and external outreach
PHASE
05
Review of the national legislation and framework on CISR
PHASE 01
PHASE 02
PHASE 03
PHASE 04
PHASE 05

Fig. 11 "Policy lifecycle of CISR"

A TENTATIVE CHECKLIST OF THE PHASES SHOULD ENCOMPASS THE FOLLOWING ACTIVITIES:

PHASE 1:

- Establishing an interagency working group on CISR, and its technical-scientific advisory board;
- Contacting the expert community, academia, and donor organizations to receive their guidance throughout the execution of the reform;
- Drafting and promulgating a law on CISR;
- Developing and publishing a national strategy and its implementation action plan for CISR;
- Improving the awareness of both public and private stakeholders through various activities (e.g., workshops, conferences, publications, and guidance);
- Recruiting civil servants to support the execution of the activities set out in the action plan;
- Preparing secondary legislation to determine the following:

  - Criteria for identification and designation of national critical infrastructure;
  - Cooperation mechanisms between governmental and public administration stakeholders;
  - A notification mechanism for incidents of significant relevance;
  - Requirements for the Operator Security Plan (OSP);
  - Requirements of the security liaison officer;
  - Functions of a national agency for CISR (optional)[78].

PHASE 2:

- Organizing a pilot-project on the preparation of the OSP with selected owners/operators;
- Preparing guidance for owners/operators on how to draft the OSP;

[78] This option is to be activated only in the event of the "CISR agency scenario" described in chapter 5.2.2

- Issuing letters of designation to the operators of critical infrastructures:
- Creating a national registry of security liaison officers;
- Developing an "early warning" mechanism for owners/operators about upcoming threats which require a prompt response

PHASE 3:

- Establishing a procedure for the evaluation of the OSP (secondary legislation);
- Review and amend the evaluated OSP.

PHASE 4:

- Organizing an annual national security exercise including CISR-specific scenarios;
- Arranging a forum for regional cooperation on CISR-related trans-boundary externalities;
- Learning lessons from the annual national security exercise and forum, and issuing recommendations to the relevant authorities and private sector on how to comply with the law on CISR.

PHASE 5:

- Assessing the maturity and impact of the CISR law;
- Listing lessons learned and completing gap analysis;
- Drafting a proposal to amend the national plan for and law on CISR.

(5.2) GOVERNANCE OF CISR

One of the crucial elements of CISR reform is governance. Pertinently, without well-established roles and responsibilities it is impossible to identify and designate national critical infrastructures, and to then ensure their compliance with legal requirements and familiarity with coordination and cooperation mechanisms.

Potentially diminishing the impact of the reform is the temptation to establish too many new bodies, with the consequence of introducing too many mechanisms. Such problems are typical of an overly bureaucratic approach.

Below, two scenarios are depicted, inspired by the approaches implemented by the two Member States considered for this study (Croatia and Romania), and also constituting the two most common approaches embraced worldwide. The two scenarios have been designed in a way to potentially fit the context of Georgia and have been named the "NSC scenario" and the "CISR center scenario" respectively.

(5.2.1) THE NSC SCENARIO

This scenario, as shown in the figure below, heavily relies on the status quo, by suggesting only the establishment of an interagency working group on critical infrastructures.

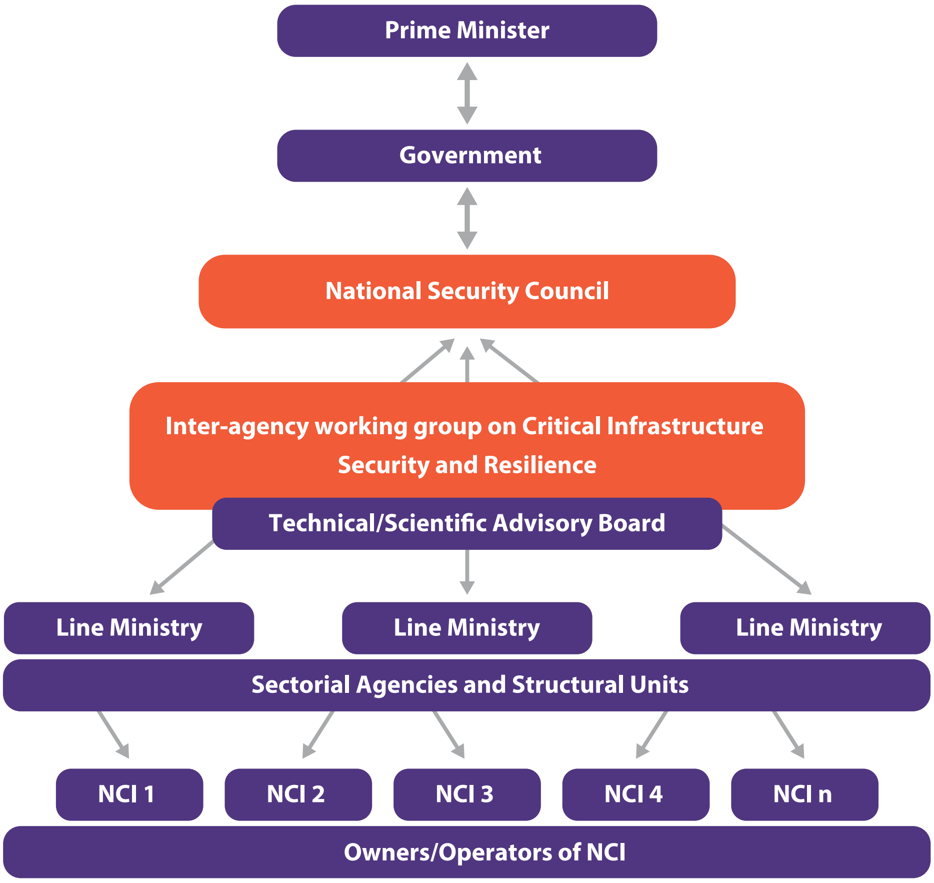

Prime Minister
Government
National Security Council
Inter-agency working group on Critical Infrastructure Security and Resilience
Technical/Scientific Advisory Board
Line Ministry
Line Ministry
Line Ministry
Sectorial Agencies and Structural Units
NCI 1
NCI 2
NCI 3
NCI 4
NCI n
Owners/Operators of NCI

Fig. 12 "Governance of CISR – the NSC scenario"

The establishment of a working group entails neither the creation of an actual body or entity, nor the provision of a budget. The main value added by the working group would be to provide an opportunity for the main stakeholders to meet, when deemed necessary, to discuss matters requiring multiple points of view, consultation, and joint work on existing or upcoming initiatives. With the aim of fostering an inclusive approach, the concept outlined above includes a technical-scientific board that could also be invited to join the working group whenever the views of its membership (comprising representatives of academia, research centers, and training centers, experts, and owners/operators of critical infrastructures) need to be considered.

In the overall policy lifecycle, as described in chapter 5.1, the interagency working group should act as a support group, which is engaged before and after the promulgation of the law on CISR.

The concept of a CISR-WG dates back to 1996 when one such group was established by the Clinton administration in the US[79]. On this matter, Mr. Stevan Mitchell,[80] during an interview,

[79] The working group is seen as the U.S. government's first attempt to involve the infrastructure owners/ operators in policymaking on CIP.

[80] Stevan D. Mitchell (Department of Justice, Attorney, Criminal Division's Computer Crime Unit) participated as Commissioner in the CIWG.

stated the following: *"I would venture to say that probably 90 to 99 percent of the preliminary thinking and the preliminary work that we had done as government representatives was quickly tossed out the window in favor of a much more trying, much more challenging, but ultimately much more productive and universally acceptable way of addressing the problem process-wise."* This historical testimony provides a strong argument for the establishment of CISR-WG before the promulgation of the law on CISR.

Following the concept outlined above, the working group may have the following features:

- Membership comprising the NSC, the Defence and Security Committee of the Parliament of Georgia, and the relevant ministries in charge of any sector defined by the law on CISR;
- An advisory board, invitations to which can be proposed by any member of the working group and is then subject to the approval of the NSC;
- The working group cannot take binding decisions, but can only provide recommendations.

(5.2.2) THE CISR CENTER SCENARIO

In this scenario, following the comparative models provided in this study, and particularly the approach of Romania, the establishment of a national center for critical infrastructure protection (CNCPIC) is put forward. Such a center could be assigned as the institution responsible for proposing and implementing CISR measures.

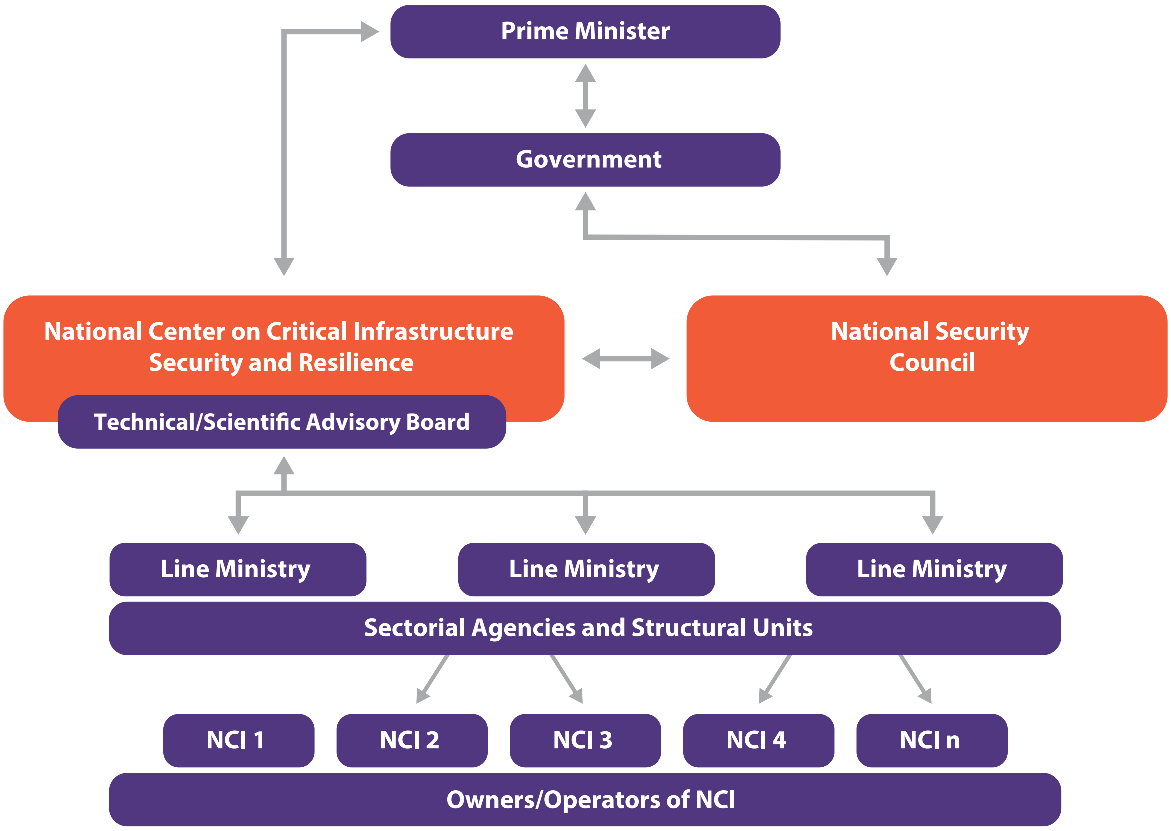

Prime Minister
Government
National Center on Critical Infrastructure Security and Resilience
Technical/Scientific Advisory Board
National Security Council
Line Ministry
Line Ministry
Line Ministry
Sectorial Agencies and Structural Units
NCI 1
NCI 2
NCI 3
NCI 4
NCI n
Owners/Operators of NCI

Fig. 13 "Governance of CISR – the CISR agency scenario"

In this case, the interagency working group would be established and kept running until a law on CISR enters into force, to provide recommendations and support regarding its preparation. Thereafter, all functions, including the possibility of scheduling a meeting with the technical/advisory board, would be absorbed by the national CISR center, once formally established.

The competencies and duties of such a center could include:

- Designing and leading the process of identification and designation of national critical infrastructure;
- Issuing guidance to owners/operators on how to prepare, maintain, and improve their OSP;
- Establishing a procedure for the notification of incidents of significant relevance and running a platform where owners/operators to provide notifications of such incidents;
- Monitoring, inspecting, and coordinating CISR activities, as well as taking measures in cases of non-implementation, pursuant to the law on CISR;
- Conducting joint tests and exercises with owners/operators of critical infrastructures, drawing conclusions, and drafting final reports and recommendations;
- Administering an incident registry;
- Creating an electronic platform for real-time information exchange and "early warnings";
- Acting as a single point of contact with CISR authorities of foreign countries and international organizations, and fostering cooperation in the domain of CIP;
- Reviewing the OSPs submitted by the owners/operators of critical infrastructures, approving/rejecting them, and issuing binding recommendations for their improvement.

In this scenario, the NSC could have a strategic and advisory role entailing the following:

- Providing strategic advice on internal/external threats;
- Giving intelligence on CISR-related threats;
- Monitoring new technological trends and developments in the context of CISR and issuing suggestions accordingly;
- Holding discussions to ensure that CISR reaches and stays on the government agenda;
- Putting forward potential measures to improve implementation of the national CISR strategy and action plan.

(5.3) EXAMPLE OF A NATIONAL CISR PLAN

Since the embryonic elements to be potentially considered in the development of a national strategy on CISR were outlined in chapter 2. Here, a **blueprint** is presented of what a national CISR plan could look. The proposed template was designed with examples from other countries in mind, and should be considered in the discussions and consultations with relevant stakeholders on the best way forward for Georgia in this regard. Accordingly, the template below can be tailored to the specific needs and security context of Georgia.

INTRODUCTION AND SCOPE

The national plan is intended to lay out a roadmap for the establishment of thorough national governance of CISR and to prepare for upcoming developments in this field.

The objective of a country's CISR policy is to *"preserve and protect national critical infrastructure, protect citizens, prevent incidents and minimize potential damage to critical infrastructure, general wealth, economic and social losses, ensure government stability, and enhance resiliency."*

As a first step towards the achievement of such an objective, the Georgian government approved the Law on Critical Infrastructure Security and Resilience (hereinafter "the Law"), which is inspired by the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and Directive 2022/2557 on the resilience of critical entities. The roadmap should thus position the Georgian government to implement the key features of its national CISR framework, by relying on the successful experiences of EU Member States and international best practices.

The following milestones are foreseen in the roadmap:

- Clear definition of competent bodies (e.g. coordination and sectorial authorities);
- Identification and recruitment of civil servants with security-related capabilities, expertise, and interests;
- Establishment of a relevant institutional mechanism for the implementation of the Law within the structure of the NSC (depending on the scenario – see chapters 5.2.1 and 5.2.2);
- Creation of a relevant institutional mechanism for the implementation of the Law within the structure of a national CISR center (depending on the scenario – see chapters 5.2.1 and 5.2.2);
- Identification and designation of national critical infrastructures;
- Publication of sectorial guidelines for the implementation of the OSPs;
- Creation of a registry of security liaison officers to be referred to in cases of crisis and for "early warnings";
- Evaluation, testing, and auditing of the OSPs;
- Establishment of an "early warning" mechanism and an information-sharing platform;
- Execution of national CISR exercises;
- Cooperation with neighboring and allied countries on regional CISR.

If a national CISR plan is produced, the following effects are predicted:

- The consolidation of national risk assessment in CISR;
- The validation and integration of existing procedures for cybersecurity, terrorism, and disaster risk response within the national CISR, with the consequent avoidance of duplication and reliance on existing tools and measures;
- The inclusion of universities and centers of excellence in the lifecycle of the national CISR, in order to foster the education and training of experts in critical infrastructure, exchanges with other countries, and the execution of international research projects;
- Greater demand for security experts in both public and private sectors.

The plan could comprise five objectives (listed and described below). Above all, the long-term goal would be to put in place the conditions that would allow national CISR to mature.

OBJECTIVE 1: Establishment of a national CISR plan, a law on CISR, and secondary legislation for the law's implementation.

The activities pursuant to the first objective would be:

- Recruitment of civil servants to support the execution of the plan;
- Establishment of an interagency working group on CISR to act discuss matters pivotal to the successful planning and execution of the plan. Specifically, representatives of the Defence and Security Committee of the Parliament of Georgia and the relevant ministries in charge of any sectors defined by the law on CISR must be approved by the NSC. The purpose of the working group is to foster discussion and strategic planning in the areas of prevention, protection, crisis, and recovery of national critical infrastructures, in accordance with the law;
- Creation of a technical-scientific advisory board under the interagency working group on CISR;
- Establishment of a national CISR center (depending on the scenario);
- Preparation and approval of secondary legislation to determine the following:

1. **Cooperation mechanisms between governmental and public administration stakeholders;**
2. **A notification mechanism for incidents of significant relevance;**

3. **Requirements of the OSP;**
4. **Requirements of the security liaison officers;**
5. **Criteria for identification and designation of national critical infrastructures.**

OBJECTIVE 2: "Identification and designation of national critical infrastructures"

The activities related to the second objective may include the following:

- Creation of a list of national critical infrastructures, based on the abovementioned criteria for identification and designation, to devise an initial database of the most vital infrastructures operating in the sectors identified by the law on CISR;
- Organization of a pilot project on the preparation of the OSPs with selected operators of critical infrastructures;
- Preparation of guidance for owners/operators on how to draft the OSPs;
- Issuing letters of designation to the owners/operators of critical infrastructures

The notification is issued through the secure delivery of an official letter, outlining:

1. **Information regarding the law on CISR and its scope;**
2. **Information regarding identification and designation procedures;**
3. **Information regarding expected efforts of the owners/operators;**
4. **Their obligation to draft/amend the OSP;**
5. **Their obligation regarding the appointment of a security coordinator/liaison officer;**
6. **Their obligation to notify the designated center of relevant incidents;**
7. **A roadmap for the implementation of the OSP;**

- Creation of a national registry of security liaison officers;
- Development of an "early warning" mechanism to alert owners/operators and to raise their awareness about upcoming threats which require a prompt response;
- Notification of the OSP's guidelines issued to the owners/operators of national critical infrastructures, following their official designation.

OBJECTIVE 3: "The implementation and review of the OSPs"

The activities under this objective could include the following:

- For owners/operators, based on the OSP's guidelines:

1. **Execution of a self-evaluation;**
2. **Preparation of a remediation plan to address residual risks (to be issued to the competent public authority for evaluation);**
3. **Implementation of high-priority countermeasures to mitigate residual risks;**
4. **Implementation of low-priority countermeasures;**
5. **Yearly repetition of activities 1 to 4, to improve the national response to CISR-related challenges.**

- Establishment of procedures for the evaluation of the OSP including penetration tests and audits (secondary legislation);
- Review and amendment of the evaluated OSP.

OBJECTIVE 4: "Annual national security exercise and external outreach"

The activities steered toward achievement of the fourth objective could include:

- Execution of an exercise with the inclusion of CISR-specific scenarios (e.g. CBRNE, physical threats, natural event);

- Organization of a forum for regional cooperation on CISR-related transboundary externalities;
- Preparation of reports on lessons learned from the annual national security exercise and the forum, and the issuing of recommendations to the relevant authorities and private sector on how to improve their compliance with the law on CISR.

OBJECTIVE 5: "Review of the national legislation and framework on CISR"

For the fifth objective, the following activities may be set out:

- Maturity and impact assessment of the law on CISR, including the elimination of duplications;
- Lessons learned and gap analysis for new objectives;
- Drafting of a proposal to amend the national plan for and the law on CISR

CONCLUSIONS

/06

6. CONCLUSIONS

The overall aim of this study, apart from raising awareness about aspects fundamental to CISR reform, is to describe and explain the various elements that could enable the successful adoption of a tailor-made approach for Georgia. Accordingly, the decision-making process and its phases and mechanisms would inform the selected scenarios and the issued recommendations.

The comparisons, analysis, and recommendations have been provided to assist the competent authorities of Georgia to evaluate the time and resources that may be necessary to accomplish the goals of the reform. Crucially, knowledge of these elements could help to fine-tune the approach taken and make it more sustainable.

Once such a sustainable, transparent, efficient, and effective national approach is established and maintained in the initial policy lifecycle, further options, initiatives, and goals could be added to the national framework to prepare Georgia for more complex and complicated challenges. These may potentially include the following:

- Establishment of an accredited training center for CISR and development of certified CISR courses;
- Creation of an information-sharing platform for national critical infrastructure stakeholders and entities;
- Informing the National Threat Assessment Document;
- Convergence and incorporation of the principles of the Law on Information Security;
- Planning and executing a national stress test;
- Fostering the establishment of a public-private partnership for CISR in Georgia;
- Establishment of an initiative countering hybrid threats with impacts on critical infrastructures.

As proposed in the initial chapters of this study, a pivotal aspect integral to the success of the proposed reform lies in acquiring the support of donor organizations and the EU. Such support is essential in facilitating the engagement of subject-matter specialists and policymakers, enabling them to offer counsel and assistance in developing a national strategy. Moreover, it paves the way for the integration of proven international best practices, thereby enriching the Georgian approach with insights gleaned from successes elsewhere. Furthermore, it fosters the establishment of channels for cooperation and coordination with pertinent stakeholders and communities, ensuring a harmonized and inclusive implementation framework. Finally, every CISR-related initiative should make "*any interruption or manipulation of critical Infrastructures brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare*"[81] of Georgia.

[81] This is taken from President Clinton as formulated in the PDD-63 of 1998 because of its comprehensive definition which is still very much valid and applicable today.

M
P C
G
Research

P M C G

Research