March 19, 2026

Fourth Memorial Scientific and Professional Conference "Predrag Marić"
MODERN INTEGRATED DISASTER RISK MANAGEMENT

Faculty of Security Studies, University of Belgrade DOI: https://doi.org/10.5281/zenodo.19410158

Article

Continuity of State Functions and Protection of Classified Information in Disaster Conditions: Theoretical Framework and Strategies of Digital Resilience

Goran Matić[1,2*]

[1] National Security Council and Classified Information of the Government of the Republic of Serbia, Nemanjina 22-26, 11000 Belgrade, Serbia; goran.matić@nsa.gov.rs.

[2] Faculty of Business Studies and Law, *Union – Nikola Tesla* University, 11070 Belgrade; Jurija Gagarina 149a (TC Piramida), *Staro sajmište 29*; goran.matic@fpsp.edu.rs.

[3] Military Academy, University of Defense, Veljka Lukića Kurjaka 33, 11042 Belgrade, Serbia.

Correspondence: goran.matic@nsa.gov.rs

Abstract

Contemporary integrated disaster risk management requires a holistic approach that encompasses not only the physical protection of people and material assets, but also the preservation of the continuity of key state institutions and protected information systems. This paper analyzes strategies and mechanisms for ensuring the continuity of state functions and the protection of classified information under conditions of complete or partial collapse of infrastructure and information systems caused by disasters of natural, technological, or hybrid origin. Through a comparative analysis of Switzerland's system (territorial

Academic Editor:
Prof. Dr. Vladimir M. Cvetković

decentralization model), Finland's system (total defense model), and Israel's system (constant operational readiness model), key principles of successful frameworks are identified. These include: decentralization and redundancy of critical infrastructure, a unified and functional legal-institutional framework, integration of cyber security into crisis management systems, and an institutionalized culture of regular capability testing. Based on these observed experiences, concrete recommendations are formulated for improving the system in the Republic of Serbia, including the development of a National Strategy for the Continuity of State Functions, the construction of a hierarchically organized network of backup centers following the Primary–Alternate–Contingency–Emergency (PACE) model, and the establishment of a mandatory exercise program for relevant institutions. The paper contributes to the theoretical framework of national resilience by pointing to the necessity of establishing a balance between physical and digital resilience as a key prerequisite for preserving the sovereignty and functionality of the state in conditions of deep and complex crises.

Keywords

National security, classified information protection, continuity of state functions, disasters, backup centers, digital resilience.

1. Introduction

In the contemporary, globalized, and digitally interdependent world, the concept of national security has been significantly expanded beyond traditional military-political frameworks. Today, it also encompasses the resilience of state systems under conditions of complete or partial collapse caused by natural disasters, technological failures, or deliberate hybrid actions. This paper is based on the assumption that a state's ability, in times of extreme crisis, to ensure the continuity of its key functions while simultaneously protecting its most sensitive information represents the ultimate test of its sovereignty and functional maturity—particularly for candidate countries whose access to European security mechanisms is conditioned by harmonization with requirements, such as Decision 2013/488/EU (Council of the European Union, 2013)[1] and the protection of classified information and the Critical Entities Resilience Directive (European Parliament & Council of the European Union, 2022)[2].

The aim of this paper is to analyze the strategic, legal, organizational, and technical aspects of ensuring the continuity of state functions and the

protection of classified information in disaster conditions, with particular emphasis on the synergy of four interdependent dimensions: (1) a unified strategic framework, (2) an operational plan for the protection of classified information in emergency situations, (3) a hierarchical network of backup centers based on the PACE model, and (4) an institutionalized culture of regular testing through national exercises. Through a comparative analysis of the systems of Switzerland (territorial decentralization model), Finland (total defense model), and Israel (permanent operational readiness model), the paper seeks to formulate applicable and contextually adapted recommendations for improving the domestic normative and institutional framework, with an explicit link to European standards of institutional resilience.

Operationalization of Key Concepts

In this paper, the following terms are used in a precisely defined sense:

- *Continuity of Government (COG):* the ability of state institutions to maintain key functions of decision-making, command, and governance under conditions of extreme crises, including scenarios of partial or complete collapse of primary infrastructure.
- *Digital resilience:* the ability of information systems to maintain the integrity, availability, and confidentiality of data even under conditions of degradation or loss of primary technological resources.
- *Classified information in emergency conditions*: information whose disclosure would endanger national security, as stated in Article 4 of the Law on Classified Information (Republic of Serbia, 2009)[3], with particular emphasis on the minimal set of data necessary for the functioning of the state in crisis ("state minimum").
- *Unified continuity system:* an integrated framework that connects the strategic, normative, infrastructural, and procedural levels into a single functional whole, where each element enhances the effectiveness of the others, and the absence of any element compromises the overall preparedness of the state.

Research Gap and Contribution of the Paper

The existing literature primarily addresses the continuity of government functions through the lens of crisis management and the physical resilience of infrastructure (Boin & McConnell, 2007)[4], while the protection of classified information is analyzed within the frameworks of information security and cyber defense (Dunn Cavelty & Suter, 2009)[5]. However, there is a lack of a theoretical framework that integrally connects institutional continuity and the protection of the most sensitive data as synergistic components of

national resilience under conditions of total collapse. Furthermore, current research neglects the Euro-integration dimension of this issue—namely, the fact that for candidate countries, the development of continuity systems is a prerequisite for security cooperation with the EU and for access to classified information within the framework of the Common Foreign and Security Policy.

This paper fills the identified gap through a holistic model of "physical-digital resilience," which: (a) conceptually integrates the maintenance of decision-making functions and the protection of classified information as inseparable elements of state sovereignty; (b) offers a comparative analysis that simultaneously encompasses legal, technological, institutional, and procedural aspects; (c) formulates a mechanism for transposition into the domestic context through the synergy of four system dimensions; and (d) explicitly connects the domestic solution with the European framework, with a direct link to Article 87, paragraph 1, item 9 of the Serbian Law on Classified Information and its European parallel in Article 15 of the previously cited Decision 2013/488/EU.

2. Theoretical Framework: Resilience as an Existential Prerequisite of Sovereignty

The concept of national resilience today requires a theoretical rearticulation that goes beyond its traditional definition as the ability of a system to 'recover after disruption' (Hollnagel, 2011)[6]. In the context of hybrid threats and cascading crises, resilience must be understood as an existential prerequisite of sovereignty—the ability of the state to preserve its functional identity amid total or partial collapse of physical and digital infrastructure. This theoretical framework is built upon three interrelated foundations:

First, the theory of Complex Adaptive Systems (CAS) enables the conceptualization of the state not as a static bureaucratic structure, but as a dynamic system that must preserve its functional integrity even when its physical carriers disintegrate (Comfort et al., 2010)[7]. In this sense, continuity of government functions is not a matter of maintaining buildings or servers, but of safeguarding the network of decision-making, legitimacy, and control that constitutes the state as a political entity. When primary infrastructure is compromised, the state must be able to 'shift' to alternative carriers of that network—requiring predefined protocols, redundant systems, and a culture of institutional adaptation.

Second, the theory of sovereignty in the digital age requires a revision of the classical Weberian definition of the state as the monopoly on legitimate physical force (Weber, 1919)[8]. In the era of cyber and information warfare, control over key information becomes an equally important component of sovereignty as control over territory (Kello, 2017)[9]. The loss of access to classified data on critical infrastructure, military capabilities, or diplomatic communications in times of crisis does not represent merely a technical obstacle—it constitutes an existential threat to sovereignty, as it prevents the state from making informed decisions about its own survival. In this context, the protection of classified information under emergency conditions is not a subdomain of information security, but the very core of the concept of state survival.

Third, the concept of the "state minimum"—the minimal set of functions and information necessary to preserve the state as a political entity under conditions of total crisis—requires theoretical grounding in Schmitt's understanding of sovereignty as "the ability to decide on the state of exception" (Schmitt, 1922)[10]. In a state of exception caused by disaster, the state must be able to maintain three elements of the "state minimum": (a) the chain of decision-making and command; (b) access to key information on security and critical infrastructure; and (c) the ability to communicate among the holders of sovereignty.

The loss of any of these three elements leads to the disintegration of the state as a functional entity—even if its territory and population physically survive the disaster.

On the basis of this threefold theoretical foundation, a holistic model of "physical-digital resilience" has been developed, which represents the key contribution of this paper. The model assumes that physical resilience (protected locations, redundant infrastructure) and digital resilience (data protection, continuity of information flows) are not additive dimensions, but synergistically conditioned: physical infrastructure loses its meaning without access to key information, while data becomes powerless without functional institutions capable of using it for decision-making. Therefore, the development of a continuity system for state functions is possible only through the integration of four interdependent dimensions—strategic framework, operational plan, infrastructure, and testing culture—into a unified system whose integrity is greater than the sum of its parts.

Finally, for candidate countries, such as Serbia, this theoretical framework acquires an additional dimension through the theory of regulatory harmonization. The European Union has developed the concept of collective resilience as the foundation of its security architecture, where the ability of each member state to maintain functionality in crisis is a prerequisite for

the security of the entire bloc (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2016,[11]; European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2022,[12]; Council of the European Union, 2022[13]). In this sense, the development of continuity systems is not merely an internal security imperative, but also a theoretical condition for integration into the European security space—adding normative weight to the theoretical framework presented in this chapter.

3. Methodological Approach: An Integrated Methodology for Analyzing the Unified Continuity System

This paper applies an integrated methodological approach that combines four interrelated methods in accordance with the theoretical framework of "physical-digital resilience":

1. Normative-legal analysis of the domestic framework;
2. Comparative case study with theoretical sampling;
3. Doctrinal analysis of European standards;
4. Synthetic method for constructing the model of the "unified continuity system".

The comparative method is not the primary research instrument, but rather an analytical intermediary that enables the identification of universal structural principles from different national contexts, while avoiding the mechanical transplantation of solutions.

4. Comparative Analysis: Structural Principles of Continuity from the Experience of Three Models

The comparative analysis in this chapter is not aimed at identifying "the best model" that could be mechanically adopted and implemented in the domestic context, but rather at extracting the structural principles underlying functional and sustainable systems of continuity of state functions. Each of the three models analyzed — Swiss, Finnish, and Israeli — was developed within a specific geostrategic, historical, and institutional environment, shaped by different threats, resources, and political-legal traditions. Nevertheless, despite these differences, all three models demonstrate a shared capacity to preserve the so-called "state minimum" in conditions of extreme crises, that is, the continuity of key functions necessary for the survival of the state as a functional and sovereign political entity.

The analysis is structured through the prism of four interconnected dimensions of the "unified continuity system" — strategic, normative, infrastructural, and procedural — which together enable a comprehensive understanding of how states institutionalize resilience in times of crisis. The purpose of this analytical approach is not to identify specific technical solutions, but to recognize conceptual and organizational patterns that have demonstrated functional sustainability and that, with critical adaptation, can be adjusted to the Serbian context. Particular emphasis is placed on their compatibility with the normative requirements of Decision 2013/488/EU, as a key European standard in the field of classified information protection and continuity of decision-making under crisis conditions.

The selection of the three states for comparative analysis is based on theoretical sampling, in line with the concept of the "state minimum" and the need to cover three key organizational-institutional models:

Table 1. Comparative analysis of three organizational-institutional models

State	Theoretical relevance	"State minimum" model	Relevance for Serbia
Switzerland	It tests the hypothesis that territorial decentralization and physical redundancy can compensate for a less developed cybernetic infrastructure	Physical dimension: underground infrastructure as a guarantee of continuity, even in the event of the loss of digital systems	Relevant for a state with pronounced regional autonomy and the need for geographical dispersion of key functions
Finland	It tests the hypothesis that legal coherence and the total integration of civilian and military resources create resilience event in a state with an exposed geostrategic position	Institutional dimension: chain of deputies, as a legal mechanism for maintaining the decision-making chain	Relevant as a model for a state that is confronted with hybrid threats and demands a unified legal framework
Israel	It tests the hypothesis that permanent operational readiness and cyber-physical integration can compensate for the lack of strategic depth	Digital dimension: automated protocols for switching to backup systems in real time	Relevant for a state exposed to continuous hybrid threats in the digital domain

Source: Author's compilation

The analysis is conducted through four analytical dimensions that directly correspond to the four components of the "unified continuity system" from the theoretical framework:

- **Strategic dimension** — analysis of the existence and quality of a unified strategic document that defines the principles of continuity of state functions;

- **Normative dimension** — analysis of the legal foundations for the protection of classified information under emergency conditions (e.g., Article 87, paragraph 1, item 9 of the earlier mentioned Serbian Law on Classified Information and Article 15 of Decision 2013/488/EU);
- **Infrastructural dimension** — analysis of the hierarchical organization of backup centers and mechanisms for offline archiving of key data;
- **Procedural dimension** — analysis of the testing culture through regular exercises simulating communication collapse and incapacitation of leadership.

As an additional methodological instrument, doctrinal analysis of European security standards (set out in the previously cited EU Strategy for Countering Hybrid Threats, Critical Entities Resilience Directive, NIS2 Directive (European Parliament & Council of the European Union, 2022) [14], and the earlier discussed Decision 2013/488/EU) was applied with the aim of identifying regulatory requirements that will become mandatory for Serbia in the process of EU accession. This analysis enables the transformation of comparative insights into European-contextualized recommendations, avoiding a "Western-centric" approach in favor of a "European-harmonized" model.

The sources used include: a) primary legal sources (laws, strategies, decisions); b) secondary sources (academic literature in the fields of security studies, resilience theory, and crisis management); c) official presentations and reports of international organizations (EU, NATO, OSCE); d) a limited number of expert interviews with representatives of competent institutions within permitted security protocols.

Research limitations — The study is subject to four significant methodological limitations that require explicit acknowledgment**:**

1. Access to classified operational protocols and technical details of continuity systems is restricted due to the nature of national security. The analysis therefore relies exclusively on publicly available sources (national strategies, laws, official reports), which limits the depth of examination of technical and operational aspects—particularly in the case of Israel, where most protocols are classified. This limitation is partially compensated through the analysis of publicly available academic works written in cooperation with security structures and through comparative triangulation of sources.
2. The scope of analysis of the domestic system is limited by the fact that many operational plans and protocols for the protection of classified information under emergency conditions (including the implementation of Article 87, paragraph 1, item 9 of the Law on Classified Information) are classified or not publicly available. This limitation is

methodologically compensated through the analysis of the normative framework and institutional capacities, with explicit acknowledgment that operational implementation may differ from formal provisions.

3. Contextual differences between the analyzed states—including geopolitical position, territorial size, demographic structure, and historical experiences with existential threats—require critical adaptation of the identified models. The Swiss model of underground infrastructure, for example, is not directly transferable to Serbia due to differing geological and financial conditions. Instead of direct adoption, the study focuses on extracting structural principles (e.g., "redundancy by design," "chains of deputies") that can be contextually implemented.
4. The dynamic nature of European regulation in the domain of critical entities' resilience means that some standards (e.g., earlier mentioned the NIS2 Directive) are still in the process of being transposed into the national legal systems of member states. This limits the possibility of precisely assessing their operational effectiveness, but does not diminish their normative relevance for candidate countries, which must harmonize their legislation prior to accession.

Despite these limitations, the applied methodological approach enables the identification of structural gaps in the domestic system and the formulation of recommendations that are theoretically grounded, comparatively verified, and European-harmonized—representing a significant methodological contribution to research under conditions of restricted access to classified operational details.

4.1. Switzerland: Decentralization and Physical Resilience

The Swiss system of continuity of state functions is based on the principles of strict decentralization and systemic duplication of key state capacities. Federal administrative centers, archives, and server resources are housed in protected underground facilities (*Schutzbauten*), which are geographically dispersed throughout the country's territory. This spatial organization aims to minimize the risk of centralized system failure in conditions of armed conflict, natural disasters, or prolonged infrastructural disruptions.

The key structural principle of this model is *redundancy by design,* whereby every critical state function has at least one physically separate and operationally independent backup location. Continuity, therefore, does not rely on improvisation under crisis conditions but is instead embedded in the very architecture of the state.

The protection of data relevant to national security is regulated by the Federal Act on Official Secrecy (*Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung – BGÖ*), as well as by special military protocols that mandate offline archiving of the most sensitive information on physically secured media. This practice reflects an awareness of the limitations of digital security in conditions of total crisis and represents a deliberate departure from complete digital dependency (Federal Council of Switzerland, 2021)[15].

4.2. Finland: Legal Coherence and Total Defense Concept

The Finnish model of *total defense* (*kokonaispuolustus*) represents a highly integrated approach to national security that unites civil, military, economic, and social resources into a single system. This model is not limited to the institutional level but rests on a deeply rooted culture of collective defense and societal preparedness, in which security is viewed as a shared responsibility of the state, the economy, and the citizens.

The Crisis Management Act 741/2011 (Finnish Parliament, 2011) [16] obliges all ministries, local government bodies, and critical infrastructure operators to develop, update, and regularly test continuity plans. These plans are verified through national exercises, such as "Operation Total Defense," which are held annually and simulate scenarios of prolonged and multidimensional crises.

The protection of classified information in the Finnish system is based on the complementary jurisdiction of two key authorities.

- **SUPO** *(Suojelupoliisi*), as Finland's security and intelligence service, is responsible for the protection of classified information in the context of national security, counterintelligence, and conducting security clearances for individuals with access to classified data.
- **Traficom** (*Liikenne- ja viestintävirasto*) - Finnish Transport and Communications Agency, on the other hand, oversees the technical security of information and communication systems, including the protection of critical digital infrastructure and the implementation of information security standards.

A particularly significant element of the Finnish model is the precise legal regulation of the transfer of authority through the *substituutti-ketju* ("chain of deputies"), which establishes a clear and predetermined hierarchical order for assuming the powers of the President of the Republic, the Prime Minister, and ministers in the event of their incapacity. This mechanism, regulated by the Act on the Exercise of the Powers of the President of the Republic

(751/1999) (Finland, 1999) [17], and the Government Act (751/2003) (Finland, 2003)[18] ensures "continuity of decision-making and governance even under conditions of extreme crisis" (Finnish Ministry of Defense, 2022)[19].

Note on terminology: The Finnish term *substituutti-ketju* is most accurately translated as "chain of deputies" in the Serbian legal context, since it refers to a predefined sequence of individuals who assume authority according to hierarchy, rather than succession in the sense of inheritance law.

4.3. Israel: operational continuity and cyber-physical integration.

The Israeli approach to the continuity of state functions is characterized by a permanent state of operational readiness, serving as an institutional response to ongoing security, hybrid, and cyber threats. The National Emergency Management Authority (*Rashut HaHatzala HaLeumit – RAHEL*), operating within the Ministry of Defense, functions on a 24/7 basis and coordinates civilian, military, and security resources across all phases of a crisis.

The protected communications system of the state leadership, referred to in public sources by the general term "protected communications system," enables continuous, confidential, and resilient communication at all levels of government, even under conditions of intense cyberattacks and hybrid operations. This ensures the operational continuity of command and decision-making, regardless of the state of public communication networks.

Integration of cyber defense into the continuity system has been achieved through the National Cyber Directorate, which operates directly within the Prime Minister's Office and coordinates both civilian (NCSA) and military cyber capabilities. This model enables predefined protocols for the immediate transfer to backup digital infrastructures in the event of a compromise of primary systems, thereby ensuring continuity of governance and command even under conditions of partial collapse of key information systems (Government of Israel National Cyber Directorate, 2023).[20]

Note: Due to the nature of national security, details regarding the technical characteristics of protected communication systems and the locations of backup centers are not publicly available; therefore, the analysis is based solely on officially published strategic and doctrinal documents.

4.4. Synthesis: universal principles and their transferability

Although the analyzed models differ significantly in institutional structure and technical solutions, it is possible to extract from them four universal

principles that form the core of a functional system of continuity of state functions.

The first principle is ***redundancy by design,*** which means that critical functions and data must have at least one physically and logically independent backup location in order to avoid a single point of failure. The Swiss model achieves this through underground infrastructure, the Finnish model through a legally regulated mechanism of a chain of substitutes, and the Israeli model through digital duplication of systems. The first principle is *redundancy by design*, which means that critical functions and data must have at least one physically and logically independent backup location, in order to avoid a single point of failure. The Swiss model achieves this through underground infrastructure, the Finnish model through a legally regulated mechanism of a chain of substitutes, and the Israeli model through digital duplication of systems.

Another principle relates to *a unique and coherent legal framework*, which excludes fragmentation of competences and ensures clear protocols for the transfer of authority in crisis conditions. The Finnish model in this regard represents the highest standard and directly corresponds to the requirements of Article 15 of Decision 2013/488/EU.

The third principle is **cyber-physical integration**, which stems from the fact that under conditions of hybrid threats, physical and digital resilience cannot be treated as separate spheres. The Israeli model demonstrates that cyber defense must be integrated into the very architecture of continuity systems, rather than organized as a parallel or secondary domain.

The fourth principle represents **a culture of testing as an institutional norm**. Without regular, realistic, and critically oriented exercises, even the most developed plans and infrastructure lose practical value. All three models show that exercises are not treated as a formality, but as a key mechanism for identifying weaknesses and continuously adapting the system.

These principles are not tied to a specific national context and can be contextually implemented in the Republic of Serbia through the development of a unified continuity system that integrates a strategic framework, operational plans for the protection of classified information, a hierarchical network of backup centers, and a program of national exercises. The key challenge in this process is not technical feasibility, but rather the political will to overcome institutional fragmentation and to accept continuity of state functions as a permanent security priority, in line with European resilience standards that will become mandatory during the process of accession to the European Union.

Table 2. Comparative Analysis of Models for Continuity of State Functions and Protection of Classified Information

Dimensions	Switzerland	Finland	Israel
Strategic	Federal Strategy for Critical Infrastructure Protection with Emphasis on Territorial Decentralization and Resilience of State Functions	*Total defence* as a Social and Security Pact; Integration of Continuity into All Sectors of Society and the State	Permanent Operational Readiness as a Response to Continuous Hybrid and Security Threats
Normative	Federal Law on Official Secrets (BGÖ) and Special Military Protocols; Decentralized Jurisdiction at the Cantonal and Federal Levels	Crisis Management Act (741/2011); Precisely Regulated *Substituutti-ketju* (Chain of Deputies) and Clear Division of Competences between *SUPO* and *Traficom*	Continuous Operational Protocols in Emergency Situations; Integration of Cyber Defense into the Normative and Managerial Crisis Framework
Infrastructural	Underground Protected Facilities (*Schutzbauten*); *Redundancy by Design*; Offline Archiving on Physically Secured Media	Government ICT Network (*Valtioneuvoston tietoturvaverkko*), Physically and Logically Separated from the Public Internet	Protected Communications System; Automatic Switching to Backup Digital Infrastructures in Real Time
Procedural	Regular Exercises at the Local and Federal Levels; Simulations of Scenarios of Total Institutional Collapse	Annual National Exercises within the Concept of Total Defense (*Yhteiskunnallinen Turvallisuus*)	Continuous Simulations of Hybrid and Cyber Threats; Permanent Operational Readiness of the System

Source: Author's compilation

Methodological note – The table Does Not Represent a Ranking of Models, but Rather an Analytical Tool for Identifying Structural Principles of Continuity of State Functions Across Four Key Dimensions of a Unified Continuity System.

5. Analysis of the Situation in the Republic of Serbia: Existing Framework and Challenges

The Republic of Serbia has, over the past decade, established a relatively developed legal and institutional framework for emergency management, primarily through the Law on Emergency Situations (Republic of Serbia, 2009)[21] and the National Security Strategy (Republic of Serbia, 2019)[22]. However, a more detailed analysis points to pronounced fragmentation in terms of an integrated approach to the continuity of state functions under disaster conditions, as well as the absence of a clearly articulated and normatively

consolidated concept of *Continuity of Government* within the domestic legal and institutional system. This gap is particularly evident in the domain of systemic protection of classified information, where continuity of control over sensitive data is a crucial element of state sovereignty.

5.1. Framework for the Protection of Classified Information and the Role of the Office of the National Security Council and Classified Information Protection

By the already discussed Serbian Law on Classified Information, a unified system was established for the designation and protection of classified information relevant to national and public security, defense, and the internal and external affairs of the Republic of Serbia. The central institutional actor in this system is the Office of the National Security Council and Classified Information Protection (hereinafter: the Council Office), which functions as a professional service of the Government of the Republic of Serbia with the status of a legal entity, responsible for implementing and overseeing the application of the law.

Article 87, Paragraph 1, Item 9 of that law stipulates that the Council Office "*proposes to the Government of the Republic of Serbia a plan for the protection of classified information for emergency and urgent situations*." This provision serves as the legal basis for integrating the protection of classified information into the disaster and crisis management system. However, in practice, no unified, comprehensive, and operationally applicable plan has been adopted that would encompass scenarios of complete or partial collapse of infrastructural, communication, and information systems.

Article 88 of the same law regulates the handling of classified information belonging to public authorities that have ceased to exist without a legal successor, stipulating that "*the Council Office shall take over the classified information of public authorities that have ceased to exist and have no legal successor, or assign another public authority to store and use such information*." Although this provision is significant for long-term archival protection, it operates *ex post* and does not address the continuity of access to and operational use of classified information during an active crisis, when uninterrupted and authorized access to information is crucial for making strategic and operational decisions.

5.2. Law on Information Security and Protection of Critical Infrastructure

The Law on Information Security (Republic of Serbia, 2025)[23] regulates measures for protecting information and communication systems from security risks, as well as the obligations of critical infrastructure operators. Particularly significant are Articles 5–25, which prescribe the obligation to develop incident management plans and measures for enhancing the technical and organizational resilience of systems.

Nevertheless, the aforementioned law does not contain explicit provisions concerning the continuity of state functions as an integral concept, nor does it define the hierarchy of backup systems and the priorities of state authorities' functioning under a wide spectrum of disasters. The integration of information security into the emergency management system remains at the level of general principles and sectoral obligations, without precise operational protocols that would ensure synchronized action by the Office for Information Technologies and e-Government, the Security-Information Agency, and the Ministry of Interior in conditions of systemic crisis.

5.3. Law on the Foundations of the Organization of Security Services and the Crisis Management System

By the Law on the Foundations of the Organization of Security Services (Republic of Serbia, 2007)[24], the national security system is defined as "*a set of institutions, organizations, resources, and activities carried out for the realization of national security*." The National Security Council, as the highest political body, has the role of coordination and guidance, but the law does not provide for a unified mechanism for assuming functions, ensuring continuity of command and decision-making in conditions of collapse or serious dysfunction of existing governing and managerial structures.

The Law on Disaster Risk Reduction and Emergency Management (Republic of Serbia, 2018)[25] regulates crisis management primarily through the activities of a special organizational unit of the Ministry of Interior and other protection and rescue entities. The normative focus is directed toward the protection of people, property, and the environment, while the preservation of the functionality of state institutions, continuity of decision-making, and protection of information systems handling classified data as elements of state sovereignty remain outside its primary scope.

5.4. Strategic Framework and Identified Institutional Gaps

The previously noted 2019 National Security Strategy of the Republic of the Republic of Serbia recognizes societal resilience as a key element of modern security architecture and highlights the importance of hybrid threats. However, the strategic document lacks a dedicated and systematized chapter focused on the continuity of state functions *(Continuity of Government*), as well as clearly defined indicators of institutional and digital resilience under conditions of extreme crises.

The key gaps in the domestic system can be summarized as follows:

- Lack of a unified strategy for the continuity of state functions that would integrally connect the protection of classified information, cybersecurity, and emergency management;
- Pronounced fragmentation of institutional competences, whereby the Council Office (classified information protection), the Office for Information Technologies and e-Government (infrastructure), the Security-Information Agency (security and counterintelligence protection), and the Ministry of Interior (crisis management) operate within their own mandates without a unified and pre-defined operational protocol for coordination in crisis conditions.
- Absence of a hierarchically organized network of backup centers for ensuring the continuity of state authorities' operations, including physically protected locations with offline reserves of classified information.
- Insufficiently developed culture of testing and exercises, since plans for the protection of classified information and cybersecurity are rarely verified through realistic scenarios that involve communication collapse, loss of access to key databases, and incapacitation of leadership structures.

A particular relevance for the Republic of Serbia, as a candidate for membership in the European Union, lies in the fact that the concept of resilience of state institutions—including the continuity of work with classified information in crisis conditions—is explicitly integrated into the European security architecture. The previously cited EU Strategy for Countering Hybrid Threats (2016, updated 2022) and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (JOIN/2022/12) emphasize that a state's ability to maintain the functionality of key institutions under the pressure of hybrid threats represents a key indicator of societal resilience—one of the six fundamental pillars of the European security architecture.

The key legal framework for the protection of classified information at the EU level is Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information. This decision regulates not only classification and access procedures, but also obliges Member States to ensure the continuity of classified information protection under emergency conditions, including scenarios of partial collapse of information systems or incapacitation of competent authorities. Article 15 of this decision explicitly requires each Member State to establish *"security evacuation and continuity plans for classified information handling"* as part of its national system for the protection of classified information.

Additionally, the already mentioned Critical Entities Resilience Directive and the NIS2 Directive establish the obligation for operators of critical infrastructure—including public institutions managing sensitive data—to develop continuity plans. In this context, the development of a unified system for continuity of state functions in Serbia—with particular emphasis on the implementation of Article 87, paragraph 1, item 9 of the Law on the Protection of Classified Information—represents not only a domestic security priority, but also a preventive harmonization with the requirements of Council Decision 2013/488/EU. This harmonization is a prerequisite for security cooperation with the EU, access to classified information within the framework of the Common Foreign and Security Policy (CFSP), and the reduction of the regulatory gap in the final phase of accession.

Overall, the identified institutional, normative, and operational gaps point to systemic fragmentation in the domain of continuity of state functions in the Republic of Serbia. The absence of a unified strategic framework that would integrally connect the protection of classified information, cybersecurity, and crisis management makes the state vulnerable precisely in those scenarios of extreme crises where the continuity of decision-making and access to key information is most critical for the preservation of sovereignty.

6. Recommendations for Improving the System in the Republic of Serbia

Based on the conducted comparative analysis and the identified normative, institutional, and operational gaps in the domestic system, the following measures are proposed to improve the continuity of state functions in the Republic of Serbia. These recommendations are formulated as an interconnected set of measures at different levels—from strategic to operational—whose common purpose is to strengthen state resilience under conditions of extreme crises. The implementation of this framework requires prior or par-

allel regulation of cybersecurity as an integrated national-level concept, with clearly defined competences, technical standards, and operational protocols for the protection of critical information systems.

6.1. Strategic Level: National Strategy for the Continuity of State Functions

It is recommended to adopt a unified strategic document that would explicitly define the principles, objectives, and procedures for preserving the functionality of state institutions in conditions of disaster, systemic crises, and hybrid threats. This strategy would, for the first time in the domestic system, clearly articulate the concept of *Continuity of Government* as an integral part of national security.

The strategic document would integrally connect the provisions of the earlier stated Law on Classified Information (Article 87, paragraph 9), the Law on Information Security, and the Law on Disaster Risk Reduction and Emergency Management, thereby overcoming the existing sectoral fragmentation and establishing a unified framework for state action in crisis conditions. Special emphasis would be placed on preserving the continuity of decision-making, command, and control, as well as on protecting critical information and communication flows.

6.2. Normative Level: Operational Plan for the Protection of Classified Information in Emergency Situations

In accordance with Article 87, paragraph 9 of the Law on Classified Information, it is necessary to develop a unified and binding executive document—the Operational Plan for the Protection of Classified Information in Emergency and Crisis Situations. This plan would serve as a normative bridge between strategic commitments and concrete procedures for action in crisis conditions.

Such a document would include:

- A clearly defined procedure for the immediate transfer to backup systems for storing and accessing classified information;
- Protocols for offline archiving of key data in geographically dispersed and physically protected locations;
- Definition of the "state minimum" of data—a set of information essential for decision-making at the highest political and security levels under conditions of limited access to systems.

In this way, the protection of classified information, currently framed as a formal legal obligation, would be transformed into a functional instrument of state continuity.

6.3. Infrastructural Level: Hierarchical Network of Backup Centers

It is recommended to build a hierarchically organized network of backup state centers based on the PACE model *(Primary, Alternate, Contingency, Emergency).* The network would be geographically dispersed, functionally autonomous, and technically independent from the primary infrastructure, in order to avoid systemic vulnerability caused by a single point of failure.

The backup centers would be physically and technically protected in accordance with relevant national and international information security standards, equipped with integrated systems for storing, processing, and accessing classified information. Such infrastructure would provide the material foundation for the continuity of state functions under conditions of serious security and technological disruptions.

6.4. Procedural Level: Unified Operational Protocol and Exercise System

As the final but crucial element of the system, it is recommended to establish a unified operational protocol for crisis response, accompanied by a mandatory program of regular national exercises. These exercises could be conducted under the working title *"State Under Pressure"* and would focus on simulating scenarios of complete or partial communication collapse, loss of access to key databases, and incapacitation of leadership structures.

The exercise program would encompass all key institutional actors—the Council Office, the Office for IT and eGovernment, the Security Information Agency, and the Emergency Management Sector of the Ministry of Interior—in accordance with predefined coordination and synchronization protocols. In this way, a culture of testing would be developed, institutional interoperability enhanced, and the gap between formal plans and actual operational capabilities reduced.

7. Conclusion

In conditions of complex, multilayered, and cascading risks, the state's ability to preserve the functionality of its institutions and protect classified information during disasters is not a luxury, but the very foundation of state

sovereignty. This study has shown that success in this area does not primarily depend on the level of technological development or budgetary capacity, but rather on the degree of strategic planning, a clear and functional division of competences, an institutionalized culture of regular testing, and the adoption of a holistic approach that treats both the physical and digital resilience of the state.

The key contribution of this study is the conceptualization of a unified system for the continuity of state functions as a synergistic whole, whose elements—the strategic framework, the operational plan for the protection of classified information, the hierarchical network of backup centers based on the PACE model, and the program of regular exercises—function only through their interconnection. Without a strategic framework, the operational plan becomes a technical document without political legitimacy; without physical infrastructure, the plan remains theoretical; and without regular testing, neither the strategy nor the infrastructure guarantees actual readiness in times of crisis. Therefore, the development of a system for the continuity of state functions in the Republic of Serbia is possible only through the simultaneous and coordinated advancement of all four dimensions.

A special significance in this context lies in Article 87, paragraph 1, item 9 of the previously discussed Law on Classified Information, which explicitly enables the drafting of a plan for the protection of classified information in emergency and crisis situations and provides a clear legal basis for integrating the protection of classified information into the crisis management system. This provision, together with its European parallel in Article 15 of Decision 2013/488/EU, constitutes a key regulatory bridge between the domestic and European frameworks for the protection of classified information under crisis conditions.

Nevertheless, despite the existence of relevant normative prerequisites, the analysis has shown that the operational implementation of these solutions, as well as their institutional integration into a unified and functional system for the continuity of state functions, remains insufficiently developed.

The comparative analysis of the models of Switzerland, Finland, and Israel indicates that state resilience is not built through *ad hoc* reactions in moments of crisis, but through long-term institutional investments, systematic duplication of critical functions, and continuous testing of the readiness of the entire apparatus of government. In this sense, the implementation of the proposed framework in the Republic of Serbia will require strong political will, stable inter-institutional cooperation, and the acceptance of continuity of state functions as a permanent security priority—as well as a European integration imperative.

Institutional resilience, including the continuity of work with classified information, is explicitly required in the earlier mentioned EU Strategy for Countering Hybrid Threats, the Critical Entities Resilience Directive and the NIS2 Directive, and its absence represents a regulatory gap that will need to be overcome in the final phase of EU accession.

Although the costs of building and maintaining such a system are significant, the comparative experiences of the analyzed states show that investments in the continuity of state functions are investments whose true value is not measured in peacetime conditions, but is fully manifested only in moments of the deepest, systemic, and existential crisis—when that very continuity becomes the last line of defense of state sovereignty.

Funding: The author reports no funding.

Data availability statement: Due to the sensitive nature of classified information protection and national security protocols, the datasets and operational plans analyzed in this study are not publicly available. Access is restricted in accordance with the Law on Classified Information of the Republic of Serbia and Council Decision 2013/488/EU.

Conflicts of Interest: The author declares no conflict of interest.

8. References

1. Council of the European Union. (2013). *Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information*. *Official Journal of the European Union*, L 274/1.
2. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (Critical Entities Resilience Directive)*. *Official Journal of the European Union*, L 333/119.
3. Republic of Serbia. (2009). *Law on classified information [Zakon o tajnosti podataka]*. *Official Gazette of the Republic of Serbia*, No. 104/2009.
4. Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50–59.
5. Dunn Cavelty, M., & Suter, M. (2009). The art of CIB: The rhetoric and reality of critical infrastructure protection. *International Studies Review, 11*(4), 768–782.
6. Hollnagel, E. (2011). *Proactive risk management in a dynamic society*. Lund: Studentlitteratur.

7. Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). *Designing resilience: Preparing for extreme events*. Pittsburgh, PA: University of Pittsburgh Press.
8. Weber, M. (1919). *Politik als Beruf*. München: Duncker & Humblot. [Serbian translation: Weber, M. (2003). *Politika kao poziv i zanimanje*. In *Ekonomija i društvo* (pp. 145–198). Beograd: Pegaz.]
9. Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.
10. Schmitt, C. (1922). *Politische Theologie: Vier Kapitel zur Lehre von der Souveränität*. München: Duncker & Humblot. [Serbian translation: Schmitt, C. (2015). *Politička teologija* (M. Marković, Trans.). Beograd: Pejton.].
11. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2016). *Joint framework on countering hybrid threats: A European Union response (JOIN/2016/18 final)*. Brussels: European Union.
12. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2022). *Joint communication on the EU's response to hybrid threats (JOIN/2022/12 final)*. Brussels: European Union.
13. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities*. *Official Journal of the European Union*, L 333, 164–189.
14. European Parliament & Council of the European Union. (2022). *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 (NIS 2 Directive)*. *Official Journal of the European Union*, L 333, 80–152. Retrieved from http://data.europa.eu/eli/dir/2022/2555/oj
15. Swiss Federal Council. (2021). *Schutz kritischer Infrastrukturen: Strategie des Bundes*. Bern: Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport.
16. Finnish Parliament. (2011). *Crisis Management Act (741/2011)*. Helsinki: Ministry of Justice.
17. Finland. (1999). *Act on the exercise of the powers of the President of the Republic (107/1999)*. Finlex. Retrieved from https://finlex.fi
18. Finland. (2003). *Government Act (751/2003)*. Finlex. Retrieved from https://finlex.fi
19. Finnish Ministry of Defence. (2022). *National defence report 2022*. Helsinki: Ministry of Defence of the Republic of Finland.

20. Government of Israel, National Cyber Directorate. (2023). *Operational continuity in the cyber era: National guidelines*. Tel Aviv: National Cyber Directorate.
21. Republic of Serbia. (2009). *Law on emergency situations [Zakon o vanrednim situacijama]. Official Gazette of the Republic of Serbia*, No. 111/2009.
22. Republic of Serbia. (2019). *National security strategy of the Republic of Serbia [Strategija nacionalne bezbednosti Republike Srbije]. Official Gazette of the Republic of Serbia*, No. 94/2019.
23. Republic of Serbia. (2025). *Law on information security [Zakon o informacionoj bezbednosti]. Official Gazette of the Republic of Serbia*, No. 91/2025.
24. Republic of Serbia. (2007). *Law on the foundations of the organization of security services [Zakon o osnovama uređenja službi bezbednosti]. Official Gazette of the Republic of Serbia*, Nos. 114/2007, 72/2012.
25. Republic of Serbia. (2018). *Law on disaster risk reduction and emergency management [Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama]. Official Gazette of the Republic of Serbia*, No. 87/2018.

List of Symbols

BGÖ – Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung [DE]; Federal Law on the Principle of Transparency in Administration [EN];

CAS – Complex Adaptive Systems

CFSP – Common Foreign and Security Policy

COG – Continuity of Government

EU – European Union

NATO – North Atlantic Treaty Organization

NIS2 – Network and Information Security Directive

OSCE – Organization for Security and Cooperation in Europe

PACE – Primary-Alternate-Contingency-Emergency

RAHEL – Rashut HaHatzala HaLeumit [HE]; Israeli National Emergency Management Authority [EN];

SUPO – Suojelupoliisi [FI]; Finland's Security and Intelligence Service [EN];

Traficom – Liikenne- ja viestintävirasto [FI]; Finnish Transport and Communications Agency [EN]