Прегледни рад

351.74/.78(73+410+94)
doi:10.5937/zrpfns55-30333

Vladimir M. Ninković
University of Belgrade
Faculty of Security Studies
vladimirninkovic@yahoo.co.uk

CRITICAL INFRASTRUCTURE RESILIENCE – NATIONAL APPROACHES IN THE UNITED STATES OF AMERICA, THE UNITED KINGDOM AND AUSTRALIA

Abstract: *Securitization of the critical infrastructure as an important factor of national security has been among the aspects of wider changes in the security discourse since the end of the Cold War. The concept of critical infrastructure protection, initially focused on countering the terrorism threat, has been changing and expanding, from adopting the 'all-hazard approach', until the recent prevalence of the strategy of resilience in managing strategic security and operational risks. The sources of those risks are found mainly in climate-change induced natural hazards, as well as in global challenges of interconnection and interdependencies of critical infrastructure. The paper discusses the concepts of resilience and critical infrastructure, and then analyses the approaches to critical infrastructure protection and resilience in the United States, the United Kingdom and Australia. Analyzed are the official documents – strategies, laws and by-laws, reviews and guidelines produced by the governmental bodies of the mentioned countries, with the aim of clarification of the concept, as well as the country-specific variations in its operationalization.*

Keywords: *critical infrastructure, resilience, all-hazard approach, risk management, national security.*

1. INTRODUCTION

A complex security environment requires the balance between reactive and proactive activities of decision-makers. The progressive increase and unpredictable nature of modern security threats emanating from turbulent geopolitical environment, but also those that are immanent to internal system structures brought

about numerous changes in the way modern states consider national security. The concept of resilience basically contains an implicit assumption that the world surrounding us possesses system features characterized by dynamic changes and interdependencies. Nowadays security studies talk about community resilience, resilience to catastrophes and emergency situations, also organisational resilience. Challenges of managing business continuity, securing undisturbed supply chains and energy security are closely related to the concept of resilience, in the sense of a possible, and often preferred, risk management strategy.

Critical infrastructure security as an important factor of national security is just one of the aspects of wider changes in the security discourse since the end of the Cold War. In the words of Miriam Dunn Cavelty, the US military is responsible for the change of security discourse for two reasons – first because of the expansion of threats to security after the Cold War, and then also because of the change in perception of possible targets, since targets do not mean just military objects, but also some other "soft targets".[1]

The imperative of secure and resilient critical infrastructure is imposed not only as an answer to direct threats (either those caused by climate change, or political or economic situations), but also due to networking and so-called interdependence between critical infrastructures at national, international and global level. Just those complexity and infrastructure interdependences bring about more and more uncertainty, and that invokes the shift in protection trends from the approach oriented towards individual threats, through the all-hazard approach, all the way to the approach oriented towards resilience or system resistance, as a strategy for facing and managing system risks and uncertainties.

Accordingly, the first hypothesis of this paper is that, due to the complexity and uncertainty that characterize the mentioned risk sources, in the last two decades the resilience strategy has been favored over the anticipation strategy in managing strategic security and operational risks threatening critical infrastructure.

From this, the second hypothesis was evolved, that sources of strategic risks can be recognized primarily in natural hazards induced by climate change, and challenges of global networks (above all in the digital sphere) and interdependencies of critical infrastructures, rather than by isolated attacks of terrorist or criminal groups.

The hypotheses will be tested by analyzing official documents of the United States of America, the United Kingdom and Australia, and there will be chronologically tracked application and interpretation of terms of resilience and protection of critical infrastructure, as well as relations between those two concepts from the 1990s to most recent documents.

This research will, apart from theoretical deliberation of the concept of critical infrastructure resilience, try to provide an insight into the practical operationali-

[1] Myriam Dunn Cavelty, "*Critical Information Infrastructure: Vulnerabilities, Threats and Responses*", UNIDIR Disarmament Forum, 3/2007, 16.

zation of that concept envisaged in mentioned documents. We are of opinion that analysis of operationalization of the critical infrastructure resilience concept may enable its practical use in the Republic of Serbia.

In the first part of the paper, we will provide a theoretical overview of the resilience concept and its application in security studies. The other part is dedicated to defining concepts of critical infrastructure and critical infrastructure protection. The last part is reserved for analysis of the effects of resilience strategy in managing risks to critical infrastructure in official documents of the USA, the UK and Australia.

2. THE CONCEPT OF RESILIENCE

The popularity of the term "resilience" over the last ten years or so can be attributed to the implicit or explicit recognition of shortcomings of traditional approaches to protection and prevention.[2] Also, observing society and nature as systems that tend towards balance was replaced with a dynamic view that emphasizes complex, non-linear relations between units that are in a state of continual change and a system facing discontinuities and uncertainties.[3]

As Walker and Cooper noticed, the term "resilience" proliferated since the formation of the US Department of Homeland Security and the publication of its *National Strategy for Homeland Security* in 2002.[4] Many national security strategies nowadays employ the same term as something nations should strive towards, regarding terrorist attacks, natural disasters and technical-technological incidents, but also system risks such as climate and demographic changes. The popularity of this equivocal term brought about multiple attempts to define the concept of "resilience" in academic and expert literature, also in official documents:

- Capacity of a system to absorb disturbance, undergo changes, and retain the same essential functions, structure, identity and feedbacks.[5]
- Ability of systems, infrastructures, government, business and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction or loss of national significance.[6]

---

[2] Zoran Keković, Vladimir Ninković, "*Towards a Conceptualization of Resilience in Security Studies*", Српска политичка мисао, vol. 67, br. 1, 2020, 154.

[3] Ola Dahlman, "*Security and Resilience*", Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, 2/ 2011, 40.

[4] Jeremy Walker, Melinda Cooper, "*Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*", Security Dialogue, 42/2011, 143-160.

[5] Patricia H. Longstaff et al. "*Building Resilient Communities: A Preliminary Framework for Assessment*", Homeland Security Affairs*, vol.6, no.3, 2010,* 1-23.

[6] US Department of Homeland Security, What is Critical Infrastructure, https://www.dhs.gov/what-critical-infrastructure, 11. децембар 2019.

- Capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures.[7]
- The ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.[8]
- The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.[9]

Although the term "resilience" has a long history of use in psychology and anthropology,[10] we can safely assert that it was finally brought forth in 1973 in the seminal paper of ecologist Crawford Holling "Resilience and Stability of Ecological Systems".[11] In accordance with Holling's view, modern considerations of that concept recognize resilience as the key feature of complex adaptive systems,[12] among which are certainly critical infrastructures, being complex socio-economic-technical systems.

For certain authors, resilience is a risk management strategy rather than the desired state.[13] Those authors contrast this strategy to anticipation,[14] security, or protection.[15]

Anticipation is a threat-based risk management approach or strategy, so it can be characterized as risk management in the narrow sense. In this approach or strategy threats are identified, they are assigned certain probabilities of occurrence and consequences they would produce if realized, a risk registry is established, risks are prioritized, and for each identified risk mitigation measures are suggested. Anticipation strategy can be adequate for treating those risks that have reliable historical and statistical data, so they can be quantified with a certain degree of reliability. Therefore, this strategy is adequate for the critical infrastructure protec-

---

[7] *Ibid*.

[8] National Infrastructure Advisory Council, "*Critical Infrastructure Resilience: Final Report and Recommendations",* 2009.

[9] The White House, "*National Security Strategy*", 2010.

[10] For detailed description of academic application of the term "resilience" through history se.: David E. Alexander, "*Resilience and disaster risk reduction: an etymological journey*", Natural Hazards and Earth System Sciences, 13/2013, 2707-2716.

[11] Crawford S. Holling, "*Resilience and Stability of Ecological Systems*", Annual Review of Ecology and Systematics, 4/1973, 1–23.

[12] Edwine Barasa, Rahab Mbau, Lucy Gilson, "*What is Resilience and How It Can Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience*", International Journal of Health Policy Management, vol. 7, no. 6, 2018, 491-503.

[13] P.H. Longstaff et al., 2010,.

[14] Aaron Wildavsky, *Searching for Safety*, Transaction publishers, New Brunswick/Oxford 1991.

[15] Christian Fjäder, "*The nation-state, national security and resilience in the age of globalization*", Resilience, vol. 2 no.2, 2014, 114-129.

tion or security approach, since this approach was initially aimed at clearly defined threats of terrorist attacks.

On the other hand, resilience is the recommended strategy in managing those risks that are characterized by a high level of uncertainty (or very low probability), but high impact. According to mentioned authors, threats generated by complex phenomena are characterized by a low level of predictability, but potentially extremely big consequences. Namely, if we cannot predict oncoming danger, prevention and protection become extremely hard and with a low ratio of price and efficiency. Likewise, Baum argued that the concepts of risk and resilience are related, but that resilience should be favored for managing unknown, unquantifiable, systemic risks.[16] According to Wildavsky, resilience and anticipation are two strategies that when used in a balanced manner, can result in the optimal level of security.[17]

Resilience is an asset-based, not a threat-based risk management strategy. For Fjäder, the concepts of resilience and security are opposed to each other: "security is essentially preventive and proactive in nature, […] whereas resilience is a combination of proactive and reactive measures aiming at reducing the impact but not at preventing threats as such. Just the opposite, the notion of resilience suggests that preventive measures were not fully effective, so that consequentially focus is shifting to minimizing of disruption of critical functions, when an event took place despite everything".[18] Similar to Fjäder, Kaufmann stated that the concept and paradigm of security primarily relates to making proactive decisions, in accordance with which futures in which the contingency in question does not or should not materialise are planned.. Contrarily to this paradigm, policies made upon resilience postulates are based on a premise that disturbances will necessarily occur.[19] In other words, the risk is accepted as a social reality that cannot be controlled or changed, but that can be overcome through processes of strengthening, or some kind of preparedness for them.[20]

3. CRITICAL INFRASTRUCTURE

The term "critical infrastructure" was coined in the 1990s. Namely, in the US President's Commission report from 1997, infrastructure was, without the prefix "critical" defined as "a network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce

[16] Seth D. Baum, "*Risk and Resilience for Unknown, Unquantifiable, Systemic and Unlikely/Catastrophic Threats*", Environment Systems and Decisions, 35/2015, 230.

[17] A. Wildawsky, 1991, 89 and further on.

[18] C. Fjäder, 2014, 122-123.

[19] Mareile Kaufmann, "*Emergent self-organisation in emergencies: resilience rationales in interconnected societies*", Resilience, vol.1, no.1, 2013, 55.

[20] Olga Pavićević, "*Koncept otpornosti u sociologiji*", Sociologija, vol.58, br.3, 2016, 435.

and distribute a continuous flow of essential goods and services.".[21] In the same document eight infrastructures were identified as "vital", i.e., "critical". Those infrastructures are telecommunication, energy systems for production and exploitation of electric power, natural gas and oil, banking and finances, traffic and transport, water supply systems, government offices and emergency situations relief services.[22] The report concluded that the state is so dependent on these infrastructures that the US Government must consider them within the concept of national security, thus these infrastructures were classified as critical.[23] Nowadays, the US Government, on the website of the Department of Homeland Security, defines critical infrastructure as "assets, systems and networks, physical and virtual, that are of vital significance for the United States because their destruction or disablement would compromise security, economy, public health or security, or a combination thereof".[24]

In June of 2004 the European Council required from the European Commission to prepare a comprehensive strategy for protecting critical infrastructure. In a Communique that Commission sent to the Council, critical infrastructure was defined as "physical and IT information plants, networks, services and other protected assets that, in case of disablement or destruction, could have a serious negative impact on health, security or economic welfare of citizenry or efficient functioning of governments of the European Union".[25] A similar definition can be found in a proposal by the European Commission on the identification of the European Critical Infrastructure (ECI) from December of 2006.[26] The final directive from December of 2008 states that "European critical infrastructure implies a plant, system or a part thereof situated in the territory of Member Countries that is of essential importance for maintaining vital social functions, health, security, safety, economic and social welfare of people, whose incapacitating or destruction would have a significant impact on Member Country as a result of lack of maintenance of these functions".[27]

---

[21] The President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, Washington 1997, 3.

[22] *Ibid*.

[23] Elgin M. Brunner, Manuel Sutter, *International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich 2009, 37.

[24] US Department of Homeland Security, What is Critical Infrastructure, https://www.dhs.gov/what-critical-infrastructure , December 11, 2019.

[25] European Commission, *Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism* (COM/2004/0702 Final), Official Journal of the European Union 2004.

[26] European Commission. *Proposal for a DIRECTIVE OF THE Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection***,** (CNS 2006/0276*)**,** Official Journal of the European Union 2006.

[27] European Council, *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*, Official Journal of the European Union 2008, 345/75-345/82.

The Republic of Serbia defines the notion of critical infrastructure similarly. According to The Law on Critical Infrastructure, critical infrastructure represents "systems, networks and objects or parts thereof, whose disrupted functioning or ceasing of delivery of goods or services can have serious consequences to national security, health or lives of citizens, property, environment, the safety of citizens, economic stability, i.e. endanger the functioning of the Republic of Serbia".[28] The Law identifies the following sectors as critical: energy, transport, water and food supply, health, finances, telecommunication and information technologies, environment protection, functioning of state organs.[29]

The syntagm of critical infrastructure protection (CIP) was first used by US president William Clinton in 1996, after the terrorist attack on the federal building in Oklahoma City in 1995.[30] Activities and protection measures of critical infrastructure were in the beginning focused on the prevention of terrorist attacks, but later other, primarily anthropogenic threats, were added.

As per Serbian Law on Critical Infrastructure, critical infrastructure protection is defined as a "set of activities and measures aimed at ensuring the functioning of critical infrastructure in case of obstruction or destruction, i.e. protection in case of threats and prevention against consequences of obstruction or destruction".[31] This definition, as is obvious, incorporates strategies of anticipation and resilience, in order to secure business continuity of critical infrastructure after a disruptive event.

4. CRITICAL INFRASTRUCTURE RESILIENCE

In the last twenty years in academic, but also practical discourse there is a noticeable shift of the focus from the concept of protection towards the resilience of critical infrastracture. Shortcomings of classic risk management based on quantitative assessments have been increasingly considered, as well as consideration of crisis management as an area separate from risk management. Still, in the beginning, the focus shifting towards the resilience of critical infrastracture was primarily oriented toward technical-technological solutions, i.e. on the physical strengthening of potential targets. This discourse shift in security approach originated after key events: the first phase, initiated by the terrorist attack of 9/11 lasted from 2001 to 2005 and focused on terrorism and endangering of physical infrastructure as an element of asymmetrical warfare between Islamic terrorist

[28] Закон о критичној инфраструктури Републике Србије, Службени гласник РС, бр. 87/2018, чл. 4.

[29] *Ibid*., чл. 5.

[30] William J. Clinton, *Executive Order 13010 – Critical Infrastructure Protection*, July 15, 1996.

[31] Закон о критичној инфраструктури Републике Србије, Службени гласник РС, бр. 87/2018, чл. 2.

groups and the "West". In phase two, after hurricane Katrina, from 2006 to 2011, all-hazard approach was recommended, considering the fact that endangerment of critical infrastructure does not necessarily stem from anthropogenic threats only, but also natural hazards. The series of cyber attacks on critical infrastructure systems[32] stipulated that, apart from physical objects, digital networks should also be included among systems of outstanding value for the welfare of nations and economies. Those digital networks may be jeopardized not only by physical threats and natural hazards, but by "cyber threats" as well. Consequently, national centres for the prevention of security risks in information-communication systems, Computer Emergency Response Teams (CERTs), and other institutions for cyber security assumed an important role in critical infrastructure protection. After the Fukushima disaster in 2011, deliberations focused more on phenomena of interdependence, cascade effects, and concurrent crises. Interdependence of critical infrastructures is explained by the impact of damage or disruption of one critical infrastructure (sector) on other infrastructures.[33] Also, the continuity of the functioning of critical infrastructures becomes at least as important concept as the protection itself.

These theoretical deliberations have made an impact on decision-makers and legislators. Hereinforward we will analyze solutions in the application of these theoretical concepts in official documents of the United States of America, the United Kingdom and Australia.

4.1. The United States of America

As already explained, the syntagms "critical infrastructure" and "critical infrastructure protection" were first mentioned in the US presidents' directives. The Homeland Security Act of 2002 stipulated the formation of the Department of Homeland Security (DHS).[34] Within competence of the Department will, further on, be all activities related to critical infrastructure protection at a national level.[35] The Law on Agency for Cyber and Infrastructure Security established the agency of the same name (Cyber and Infrastructure Security Agency – CISA) within the DHS, to serve as the coordination body for all identified critical infrastructure sectors.

Still, in the United States, there is no separate strategic or regulatory document that specifically addresses the resilience of critical infrastructure, although the "approach directed to all threats" has been applied for fifteen years already.

[32] This is primarily related to attacks on Estonia's e-administration in 2007, and so-called "Stuxnet" attack on Iranian nuclear program.

[33] Zoran Keković, Vladimir Ninković, *Zaštita kritične infrastrukture – sistemski pristup*, Beograd, Centar za analizu rizika i upravljanje krizama 2021, 34-35.

[34] Homeland Security Act of 2002. Washington D.C.: U.S. Congress. Name of the institution in Serbian translations is Министарство отаџбинске безбедности.

[35] Z. Keković, V. Ninković, 2020b, 56.

Namely, the Critical Infrastructure Task force of Homeland Security Advisory Council initiated in 2006 a debate on the excessive focusing of state policies on critical infrastructure protection from terrorist attacks, while neglecting other threats. The Taskforce emphasized that the US Government policies favored investments into security measures such as video surveillance, security personnel, etc., but did not encourage efforts to enable protected assets to maintain functions at a certain level, or to recover the full function after an attack.[36] Such efforts, according to the Taskforce, could include increased redundancy (e.g. multiple backup power sources) or the designing of more robust systems.[37] The first recommendation of the Taskforce was to promote the concept of critical infrastructure resilience as a primary strategic goal to be considered in planning national policies.[38]

Soon afterwards, the term "resilience" entered official US documents. The National Strategy for Homeland Security from 2007 linked the "structural resilience" of critical infrastructure with "operational resilience" of emergency services, government institutions and private companies in a crisis. This strategy highlighted that none of the threats these systems might face is entirely predictable, so it gives precedence to the resilience concept over the older concept of prevention.[39] According to the Strategy, resilience can, inter alia, be achieved through the dispersion of key functions onto multiple service providers, a flexible supply chain and linked systems.[40]

In the National Infrastructure Advisory Council's (NIAC) 2009 report, critical infrastructure resilience is defined as an "ability for reduction of the magnitude, impact or duration of a disruption".[41] According to that report, resilient critical infrastructure posesses the following characteristics:

- Robustness – ability to maintain critical functions and to absorb impacts resulting from a crisis or disruption.
- Resourcefulness – ability to prepare, respond and manage crisis or disruption through establishing and maintaining adaptive capacities for redirection of resources and assets.
- Quick recovery – ability for fast and efficient returning to normal operational mode.[42]

---

[36] Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*, January 2006.

[37] John Moteff, *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, CRS Report for Congress, August 23, 2012.

[38] Homeland Security Advisory Council, 2006, iii.

[39] Department of Homeland Security, *The National Strategy For Homeland Security*, October 2007.

[40] *Ibid*., p. 28.

[41] National Infrastructure Advisory Council (NIAC), *Critical Infrastructure Resilience*, Washington DC 2009, 2.

[42] *Ibid*., p. 24.

Presidential Directive 21 – "Security and resilience of critical infrastructure" from 2013, highlights the need for the existence of safe, operative and resilient critical infrastructure, in order to maintain continuity of essential state functions.[43] Unlike documents enacted directly after the attack on Twin Towers that were overwhelmingly motivated by terrorist attack threats, in this directive noticeable is an all-hazard approach, as well as the phenomena of interdependency and "cascade effect". This directive emphasizes the criticality of energy and communication systems, due to their impact on all other critical infrastructure sectors.[44]

4.2. The United Kingdom

Gradual abandoning of exclusive orientation on terrorism threat and focus shifting towards all-hazard approach and resilience occurred also in other countries that were included in the "War on Terror". Sir Michael Pitt's review of the United Kingdom (UK) government response to catastrophic floods that hit the UK in 2007 exposed for the first time shortcomings of critical infrastructure protection policies vis-a-vis natural hazards. Pitt concluded that "the government shoud establish a systematic, coordinated, cross-sector campaign to reduce the disruptions caused by natural events to critical infrastructure and essential services".[45]

"The Strategic framework with the statement on policy"[46] that adduces Pitt's report published in 2010 provides more specific guidelines for operationalization

[43] Presidential Directive has legal power of Executive Order, and is different just in its form. Compare: Randolf D. Moss, "*Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order – Memorandum Opinion for the Counsel to the President*" Opinions of the Office of Legal Counsel in Volume 24, 2000, 29-30. On function and legal power of executive orders by US president see: Harold Relyea, *Presidential Directives: Background and Overview,* CRS Report for Congress – Order Code 98-611 GOV, 2008. and Danilo Stevandić, "*Izvršne uredbe Predsednika Sjedinjenih Američkih Država*", Pravni zapisi, vol.3, br, 1, 2012, 198-216.

[44] The Department of Homeland Security has competence over eight critical infrastructure sectors (chemical industry; objects with a commercial purpose; communications; manufacturing of critical goods; dams; emergency services; information technologies; nuclear reactors, materials and waste). The Department of Homeland Security has co-competence also over objects that are US Government property (together with General Services Administration) and transport systems (with the Department of Transport). The sector of arms industry is under competence of the Department of Defence, the energy sector – Department of Energy, finances – Department of Treasury, health and public health – Department of Health and Human Services, water and sewage management – Environment Protection Agency, while the sector of agriculture and food production is under co-competence of the Department of Agriculture and the Department of Health and Human Services. Presidential Policy Directive/PPD-21, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. January 25, 2020.

[45] Michael Pitt, *Learning Lessons from the 2007 Floods. An Independent Review by Sir Michael Pitt, Interim Report (The Pitt Review),* U.K. Government, London 2007, 99.

[46] *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, Cabinet Office, March 2010.

of the resilience concept, with a focus on natural disasters, primarily floods. According to the Strategic framework, the main goal is "to identify and assess risks from natural hazards, and thereafter to develop a range of options to avoid, transfer, accept, reduce or share those risks. Options could vary from the provision of physical protection through the relocation of assets, or the provision of alternative supplies, or improved arrangements for emergency response".[47] Further on, the Strategic Framework emphasizes that it is "important to get the balance right between investment in the critical infrastructure itself and investment in emergency response and recovery capabilities and plans. A programme to improve resilience within the UK"s critical infrastructure will need to encompass prevention, protection, response and recovery important to achieve right balance between investing into critical infrastructure and investing into response to emergency events, capacities and recovery plans. In an increasingly networked society, it will also need to take account of dependencies and interdependencies within and between sectors".[48]

At the same time, the Strategy on the national security of the UK from 2010 accepted resilience as a risk management strategy suitable for tackling unpredictable risks.[49] The Strategy emphasized the importance of the resilience of networks of major British companies to cyber attacks and severe disruptions of telecommunication systems.[50] Finally, one of the listed "tasks of the national security" is to "provide resilience for the UK by being prepared for all kinds of emergencies, able to recover from shocks and to maintain essential services".[51]

Strategic Defence and Security Review from the same year listed conditions that should be met to achieve the abovementioned task, among them security and resilience of the infrastructure most critical to keeping the country running (including nuclear facilities) against attack, damage or destruction; crisis management capabilities able to anticipate and respond to a variety of major domestic emergencies and maintain the business of government; resilient supply and distribution systems for essential services; effective, well organized local response to emergencies in the UK, building on the capabilities of local responders, businesses and communities.[52] The review also envisaged establishment of a new Infrastructure Security and Resilience Advisory Council, which would significantly enhance cooperation between public and private sectors and improve their resilience to all kinds of hazards and threats, particularly with regard to cyber-attacks.[53]

[47] *Ibid*., 5.

[48] *Ibid*., 7.

[49] *National Security Strategy – A Strong Britain in an Age of Uncertainty*, HM Government, 2010, 25.

[50] *Ibid*., 29.

[51] *Ibid*., 33.

[52] *Strategic Defence and Security Review – Securing Britain in an Age of Uncertainty*, HM Government, 2010, 14.

[53] *Ibid*., 49.

The following defence and security strategic documents with no exception include critical infrastructure resilience among pillars of national security. Section G, "Crisis Response and Resilience" of the National Security and Defence Review from 2015, begins with the following sentence: "The UK's resilience depends on all of us – the emergency services, local and central government, businesses, communities and individual members of the public".[54] In the same chapter, it is argued that the large parts of critical infrastructures are in the private sector, which therefore requires joint efforts of the Government and infrastructure owners and operators to mitigate risks from malicious attacks and natural hazards, as well as from cyber threats.[55] Finally, it was highlighted that essential services must be able to carry on running in the event of a widespread power cut, and that new measures should be introduced to ensure enhanced resilience towards that risk.[56] The frequency of the term "resilience" also increased, so in comparison to 11 mentions in the 2010 National Security Strategy, in the 2015 *National Security Strategy and Strategic Defence and Security Review* the term was used 53 times.

Annual reviews that monitor the application of the national security and defence strategy concretize these requests. Therefore, in the 2019 review (Third Annual Review), section 2.100 emphasizes the efforts made by the Government to form an adequate and change existing regulatory framework to achieve the resilience of National critical infrastructure to future threats, and keep the evolving risk landscape under continual review to identify impacts to the security and resilience of critical infrastructure.[57] It was confirmed that multisector regulatory solutions were introduced, with examples including the network and information systems regulations and the amendment to the Enterprise Act from 2002. Also, the Third Annual Review mentions that a White Paper published in 2018 provided substantive proposals how national security implications of foreign investment may be scrutinized.[58]

In the Third Annual Report on the Cyber Security of the UK's National Infrastructure for the period 2017-2019, critical infrastructure protection against cyber threats is considered to be a 'wicked' problem, and thus the recommended approach is resilience, not security.[59] Resilience, according to the Report, requires strengthening of regulatory framework, improvement of 'culture' of owners and

[54] *National Security Strategy and Strategic Defence and Security Review*, HM Government, 2015, 43.

[55] *Ibid*., 44

[56] *Ibid*., 44.

[57] *National Security Strategy and Strategic Defence and Security Review 2015. Third Annual Report*, 24.

[58] *Ibid*.

[59] *Cyber Security of the UK's Critical National Infrastructure. Third Report of Session 2017-2019*, Joint Committee on the National Security Strategy. House of Lords, House of Commons, 2018, 8.

operators of CI, which means improving day-to-day cyber 'hygiene' (policy of minimum access, passwords, etc.) and risk assessment in the supply chain.[60]

Finally, the recently published Resilience Study Scoping Report by the UK National Infrastructure Commission is a good indicator of a tendency towards the all-hazard approach. At the very beginning of the document, it is stated that "the UK's current and future infrastructure must be resilient to the growing challenges of climate change, population growth and an increasing reliance on, and integration of, digital technologies. This is on top of day-to-day challenges around changes in the economy, from natural hazards and from security threats. (...) It is difficult to find examples of holistic and cross sector approaches to resilience, and there is not yet an overall understanding of the resilience and vulnerabilities of the UK's economic infrastructure".[61]

Especially important is Commision view that in next period its efforts should be directed to following issues:

1. What are the systemic issues that make infrastructure vulnerable to current shocks and future changes and how could they be addressed?
2. What does the public expect of infrastructure services and how should their views be considered in decisions about resilience?
3. What changes to governance and decision making could improve current levels of resilience and ensure future challenges are addressed?[62]

4.3. Australia

Australia, due to its specific geographical position and geopolitical role in the world, early on discarded the dominant narrative that terrorism is a "threat above all threats" to critical infrastructure and national security. Theoreticians, decision-makers and legislators, all realized that on huge Australian wastelands the climatic phenomena, as well as its dependence on external resources, are extremely disruptive factors. Towards the end of the first decade of this century, the resilience strategy started to take over supremacy over the protection/security approach. As the introduction to Critical Infrastructure Resilience Strategy stated: "The review on critical infrastructure of 2009 found that, while it is possible to plan protection measures for some incidents that may affect critical infrastructure, given the broad range of potential threats and hazards, including natural disasters, pandemics, negligence, accidents, criminal activity, or computer network attack, it is not possible to foresee, mitigate or prevent all of these events. In particular, protective security measures alone cannot mitigate supply chain disruption, nor ensure the rapid restoration of services. Owners and operators of critical infra-

[60] *Ibid*., 31-32.
[61] *Resilience Study Scoping Report,* National Infrastructure Commission, September 2019, 4.
[62] *Ibid*.

structure often have limited capacity to continue operations indefinitely if the essential goods and services they require are interrupted. Therefore, a resilience approach is more suitable for activities in response to all hazards".[63]

Official Australian terminology makes a clear difference between concepts of security/ protection, and critical infrastructure resilience, as well as the institutional competencies over them.

The Australian Security of Critical Infrastructure Act of 2018 seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.[64] The Act applies to some two hundred organizational systems across sectors of electric energy, gas infrastructure, water management and seaports. Critical infrastructure security falls under the competence of the Department of Home Affairs of Australia, which also keeps the registry of critical infrastructure and can require detailed information from critical infrastructure owners and operators.[65] The Act empowers the Department to impose certain risk mitigation measures on owners and operators of critical infrastructure, if they were not previously implemented, or were implemented in an inadequate manner.[66]

The systematic network for improving the resilience of critical infrastructure was formed already in 2003 in a form of the Trusted Information Sharing Network – TISN. This platform is used for information exchange between government institutions and the private sector through coordination of responses to security challenges and potential disruptions of continual operation, in order to improve critical infrastructure resilience.[67] The sectors incorporated in the Network are: banking and finance, communications, energy, health, agriculture, food production and distribution, transport and water management. Also, within the network, specialist forums and the expert group for resilience are established. The Network activities include the development of a common activity framework, guidelines and plans, and organizing exercises and workshops directed towards specific threats to these sectors.

The first Critical Infrastructure Resilience Strategy was enacted in 2010.[68] The strategy envisaged a wide spectrum of activities aimed at improving CI resilience: from capacity building, promoting resilience concept and widening the corpus of practical knowledge, all the way to establishing Critical Infrastructure

---

[63] *Critical Infrastructure Resilience Strategy – Policy Statement*, 2015, 2.

[64] *The Security of Critical Infrastructure Act*, 2018, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018, 14. april 2021.

[65] *Ibid*., 3.

[66] *Ibid*.

[67] Trusted Information Sharing Network, https://www.tisn.gov.au/Pages/default.aspx., 16. april 2021.

[68] *Critical Infrastructure Resilience Strategy*, 2010.

Program for Modeling and Analysis that models and simulates the behavior of critical infrastructure system and 'cascade effects' of disruption in one sector to other sectors.[69]

The new strategy, published in 2015, was divided into the policy statement and practical part. On a national level, the term "critical infrastructure protection" was used to describe activities or measures for mitigating risk from the specific terrorist threat, whilst the term "critical infrastructure resilience" includes government all-hazard approach, including the terrorism threat.[70] The goal of the Strategy was defined as the continual functioning of critical infrastructure in the face of all hazards.[71]

The Strategy envisages two approaches for accomplishing the mentioned goal. The first one is a management of predictable risks using the approach based on risk assessment and management. The other one is the management of unpredictable risks, i.e. uncertainties, which can be accomplished through an organisational resilience approach.[72] "Organisations must build an inherent capacity to respond to unforeseen or unexpected risks and events. In the face of adversity, organisations with a strong resilience culture and capability will maintain operational continuity for longer, and return to normal business more quickly. (...)An organisation with a strong resilience culture is more likely to share information with others, learn from crises, have flexible approaches to problem-solving and have collaborative relationships with government and the industry sectors. An organisational resilience approach does not preclude the use of traditional risk management practices. Highly resilient organisations are able to adapt and utilise risk-based methods and tools more flexibly and across a range of circumstances. In addition to planning for reasonably foreseeable risks, resilient organisations prepare for uncertainty and ensure their arrangements are adaptable and scalable to disruptions of all kinds".[73]

Also, the two most populous states of the Australian Commonwealth, New South Wales and Victoria, developed their own strategies and harmonized them with the national one.[74] The state of Victoria also developed guidelines for the Minister of police and emergency services for the operationalization of the strategy,[75] as well as annual reports on critical infrastructures resilience. The annual reports identify key risks that eight identified critical infrastructure sectors are facing, and initiatives undertaken to improve their resilience.[76]

---

[69] *Ibid*.

[70] *Critical Infrastructure Resilience Strategy – Policy Statement*, 2015,2.

[71] *Ibid*., 3.

[72] *Ibid*., 7-8.

[73] *Ibid*., 8.

[74] *NSW Critical Infrastructure Resilience Strategy – Partner, Prepare, Provide*, State of New South Wales, 2018. *Critical Infrastructure Resilience Strategy*, State of Victoria, 2015.

[75] *Ministerial Guidelines for Critical Infrastructure Resilience*, State of Victoria, 2016.

[76] *Victoria's Critical Infrastructure All Sectors Resilience Report 2020*, State of Victoria, 2021.

5. CONCLUSION

In the last two decades, the focus of critical infrastructures protection shifted from the threat of international terrorism to natural disasters, cyber threats, risks originating due to interdependence of critical infrastructures, systemic risks such as climate changes and migrations, and finally to the acceptance that not all risks can be predicted. This change of paradigm occurred due to efforts of academic community and practitioners of risk management that denoted that the highest risks to critical infrastructure, and therefore to the well-being of societies, do not come from statistically predictable events. Also, developed countries are increasingly aware that their well-being depends on undeveloped countries; therefore, the control of systemic risks, inherent to the modern supply chains' structure, will necessarily be set up as an unavoidable topic of critical infrastructure resilience.

Briefly, the meaning of critical infrastructure resilience amounts to the following:

- Critical infrastructure, especially its business and operational continuity, is of key importance for the social and economic prosperity of the state.
- Resilient critical infrastructure has a key role in accomplishing wider principles of communal and disaster resilience.
- Public and private sector have a common responsibility for critical infrastructure resilience, which requires establishment of a strong partnership and sufficient trust for an efficient exchange of sensitive information.

National approaches reviewed in this text come from highly developed countries, those that in the last decades put resilience as a risk management strategy of choice on the worldwide agenda. Common to all these approaches is that they see the global phenomena such as climate change, infrastructure networks and interdependencies, foreign ownership over critical infrastructure systems and geopolitical dynamics as sources of strategic risks to which resilience strategy may provide answers. Notwithstanding, it is possible to notice differences between the national approaches in the level of operationalization of the concept of resilience in official documents – laws, regulation acts, strategies, reports and studies.

From regulation acts, strategies and reports of relevant US institutions, it is not possible to get a clear picture of what is concretely understood as critical infrastructure resilience. Except for isolated mentioning of resilience as a desired state of the infrastructure, or preferred strategy for managing "all-hazards", there is no strategical, regulatory or methodical USA document that would operationalize the meaning of that notion, suggest initiatives, activities and measures in order to improve resilience, neither legal sanction against owners and operators that fail to execute those initiatives, activities and measures.

The UK publicly available documents emphasize the need for closer linking of the public and private sector in strengthening alertness, planning and response to unwanted events, and consider the phenomena of multirisks, organizational and

security culture, while a special place was given to deliberating responses to new risks in digital domains and those induced by climate changes.

Finally, for almost two decades Australia has had an institutionalized approach to critical infrastructure resilience, with separate strategic and methodical documents, both on national level and the level of its states. From the Australian documents reviewed in this paper, particularly from guidelines for application of the National Resilience Strategy, we can understand the specific measures, initiatives and activities taken vis-a-vis management of complex risks such as the foreign ownership over critical infrastructure, COVID-19 pandemics and forest fires in the state of Victoria.

Critical infrastructure is the term that has recently entered the legislation of the Republic of Serbia. Regardless, in the Serbian Law on Critical Infrastructure, as in the regulatory acts of the EU and its member states, the concept of resilience has still not taken enough hold. Therefore, we are of opinion that it may be beneficial to observe the good practice of the countries analyzed in this paper. That, of course, does not mean we should neglect protecting our most important systems from anthropogenic security threats like terrorism, espionage, sabotage, or crime. Still, the protection approach alone is inadequate for those risks that most often severely disrupt the delivery of critical products and services of those systems. Namely, in 2014 the energy system of Serbia was severely affected by the so-called "May Floods". At the time of writing this paper, health and education sectors, among many others, have been severely hit by COVID-19 pandemic. Also, it is well documented that geopolitical events, such as an increased enmity between Russia and Ukraine, can bring about the disruption of energy supply chains. Finally, digitalization and impact of information-communication technologies on all sectors have incurred emerging risks that can be managed in a systemic manner only.

Certainly, further research is needed that would help governments and organizations to understand how exactly they could become resilient. Without it, resilience may remain just one of numerous vague and trendy academic concepts. We hope that the overview of national approaches and good practices in the countries included in this paper can, at least, help the discussion on institutional solutions and operationalization of critical infrastructure resilience in the Republic of Serbia.

REFERENCES

Alexander, David E., "*Resilience and disaster risk reduction: an etymological journey*", Natural Hazards and Earth System Sciences, 13/2013, 2707-2716.

Australian Government, *Critical Infrastructure Resilience Strategy*, Australian Government, Canberra 2010.

Australian Government, *Critical Infrastructure Resilience Strategy – Policy Statement*, Australian Government, Canberra 2015.

Barasa, Edwine, Rahab Mbau, Lucy Gilson, "*What is Resilience and How It Can Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience*", International Journal of Health Policy Management, vol.7, no.6, 2018, 491-503.

Baum, Seth, "*Risk and Resilience for Unknown, Unquantifiable, Systemic and Unlikely/Catastrophic Threats*", Environment Systems and Decisions, 35/2015, 229-236.

Brunner, Elgin, Manuel Sutter, *International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich 2009.

Clinton, William J., *Executive Order 13010–Critical Infrastructure Protection*. July 15, 1996.

Critical Infrastructure Resilience Strategy, State of Victoria, 2015.

Cyber Security of the UK's Critical National Infrastructure. Third Report of Session 2017-2019. Joint Committee on the National Security Strategy. House of Lords, House of Commons 2018.

Dahlman, Ola, "*Security and Resilience*", Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, 2/ 2011, 39-51.

Department of Homeland Security, *The National Strategy For Homeland Security*, October 2007.

Department of Homeland Security, "*What is Critical Infrastructure*", https://www.dhs.gov/what-critical-infrastructure , 11. децембар 2020.

Dunn Cavelty, Miriam, "*Critical Information Infrastructure: Vulnerabilities, Threats and Responses*", UNIDIR Disarmament Forum, 3/2007, 15–22.

European Commission, *Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism* (COM/2004/0702 Final), Official Journal of the European Union 2004.

European Commission, *Proposal for a DIRECTIVE OF THE Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection,* (CNS 2006/0276*), Official Journal of the European Union 2006.

European Commision*, 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*, Official Journal of the European Union 2008, 345/75-345/82.

Fjäder, Christian, "*The nation-state, national security and resilience in the age of globalizatio*n", *Resilience*, vol.2, no.2, 2014, 114-129.

Haimes, Yakov. Y., Kenneth Crowther, Barry M. Horowitz, "*Homeland security preparedness: Balancing protection with resilience in emergent systems*", Systems Engineering, vol.11, no. 4, 2008, 287-308.

Holling, Crawford S., "*Resilience and Stability of Ecological Systems*", Annual Review of Ecology and Systematics, 4/1973, 1–23.

Homeland Security Act. U.S. Congress, Washington D.C, 2002.

Homeland Security Advisory Council (2006). *Report of the Critical Infrastructure Task Force*, January 2006.

Kaufmann, Mariele, "*Emergent self-organisation in emergencies: resilience rationales in interconnected societies",* Resilience, vol.1, no.1, 2013, 53-68.

Keković, Zoran, Vladimir Ninković, "*Towards a Conceptualization of Resilience in Security Studies*", Српска политичка мисао, vol. 67, br. 1, 2020[a], 153-175.
Keković, Zoran, Vladimir Ninković, *Zaštita kritične infrastructure – sistemski pristup*, Centar za analizu rizika i upravljanje krizama, Beograd, 2020b.
Longstaff, Patricia. et al., "*Building Resilient Communities: A Preliminary Framework for Assessment*", Homeland Security Affairs, vol.VI, no.3, 2010, 1-23.
Ministerial Guidelines for Critical Infrastructure Resilience, State of Victoria, 2016.
Moss, Randolf D., "*Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order – Memorandum Opinion for the Counsel to the President*", Opinions of the Office of Legal Counsel, Volume 24, 2000, 29-30.
Moteff, John, *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, CRS Report for Congress, August 23 2012.
National Infrastructure Advisory Council (NIAC), *Critical Infrastructure Resilience*, Washington DC 2009.
National Security Strategy – A Strong Britain in an Age of Uncertainty, HM Government, United Kingdom 2010.
National Security Strategy and Strategic Defence and Security Review 2015 – A Secure and Prosperous United Kingdom, HM Government, United Kingdom 2015.
National Security Strategy and Strategic Defence and Security Review 2015 – Third Annual Report. HM Government 2018.
National Strategy for Homeland Security, Department of Homeland Security, Washington DC, October 2007.
NSW Critical Infrastructure Resilience Strategy – Partner, Prepare, Provide, State of New South Wales, 2018.
Obama, Barak, *Presidential Policy Directive/PPD-21*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
Pavićević, Olga, "*Koncept otpornosti u sociologiji*", Sociologija, vol.58, br.3, 2016, 432-449.
Pitt, Michael, *Learning Lessons from the 2007 Floods. An Independent Review by Sir Michael Pitt, Interim Report (The Pitt Review),* U.K. Government, London 2007.
Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience. (2013). Washington: The White House.
Relyea, Harold. "*Presidential Directives: Background and Overview*", CRS Report for Congress – Order Code 98-611 GOV, 2008.
Resilience Study Scoping Report, National Infrastructure Commission, UK September 2019.
Stevandić, Danilo, "*Izvršne uredbe Predsednika Sjedinjenih Američkih Država*", Pravni zapisi, vol.3, br.1, 2012, 198-216.
Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, Cabinet Office, March 2010.
The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures*, Washington DC 1997.
The Security of Critical Infrastructure Act, Australian Government, Canberra 2018.
Victoria's Critical Infrastructure All Sectors Resilience Report 2020, State of Victoria, Melbourne 2021.

Walker, Jeremy, Melinda Cooper, "*Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*", Security Dialogue, 42/2011, 143-160.
Wildavsky, Aaron, *Searching for Safety*, Transaction publishers, New Brunswick/ Oxford 1991.
Закон о критичној инфраструктури. Службени гласник РС, бр. 87/2018.

Владимир М. Нинковић
Универзитет у Београду
Факултет безбедности
vladimirninkovic@yahoo.co.uk

Отпорност критичне инфраструктуре – национални приступи у Сједињеним Америчким Државама, Уједињеном Краљевству и Аустралији

Сажетак: *Секуритизација критичне инфраструктуре као значајног фактора националне безбедности само је један од аспеката ширих промена у безбедносном дискурсу од краја Хладног рата. Концепт заштите критичне инфраструктуре, првобитно усмерен на претњу тероризма, мењао је и ширио фокус, од усвајања "приступа заснованог на свим претњама", па до усмерења на примену стратегије отпорности критичне инфраструктуре у управљању стратешким безбедносним и оперативним ризицима. Извори стратешких ризика препознају се, пре свега, у природним хазардима индукованим климатским променама, те глобалним изазовима умрежавања (пре свега у дигиталној сфери) и међузависности критичних инфраструктура. У раду се анализирају национални приступи примени стратегије отпорности у управљању ризицима по критичну инфраструктуру у Сједињеним Америчким Државама, Уједињеном Краљевству и Аустралији. Рад анализира званична документа– стратегије, регулаторна акта, као и институционалне извештаје и студије о њиховој примени, у циљу расветљавања појма отпорности критичне инфраструктуре, као и разлике у његовој операционализацији у поменутим државама.*

Кључне речи: *критична инфраструктура, отпорност, приступ заснован на свим ризицима, управљање ризицима, национална безбедност.*

Датум пријема рада: 14.01.2021.
Датум достављања коначне верзије рада: 14.02.2022.
Датум прихватања рада: 23.02.2022.