Fall 2021

The Role of Public and Private Sectors: How to Promote National Cybersecurity Strategies and Critical Infrastructure Protection in Southeastern Europe

Larry Cruz
SIT Study Abroad

The Role of Public and Private Sectors: How to Promote National Cybersecurity Strategies and Critical Infrastructure Protection in Southeastern Europe

By: Larry Cruz

Fall 2021: December 9, 2021

SIT Switzerland: International Relations and Multilateral Diplomacy
Dr. Gyula Csurgai, Dr. Elisabeth Meur, and Dr. Heikki Mattila

Bates College
Politics Major, Russian Minor

Abstract

This paper seeks to address the important role of public and private interests in protecting critical infrastructure in Southeastern Europe, providing examples from Serbia. While the public sector does have a role in protecting critical infrastructure needs, it is the private sector which holds major oversight of the critical infrastructures of the region, therefore having an important role in maintaining their functionality and protection. The literature in this field argues for more collaboration and information sharing between the public and private sectors of the region, though the task is not as simple as it appears given the varying aspirations of each country and their approaches to critical infrastructure protection and designation. The main argument of this paper calls for tailored approaches to public and private sector cooperation in each country with some oversight from a regional agency meant for general guidance. The tailored approach provides for a more effective solution as it considers the needs of each individual country, looks at the existing situation in each country, and provides for more effective collaboration between public and private sectors. For this paper, field experts also provided an overview of the current cybersecurity situation in the region, the roles of public and private sectors, and what can be done moving forward. This information serves to explain the main argument and why the tailored approach is needed to improve the state of cyber critical infrastructure in the region in light of current and emerging threats, which are also discussed.

Acknowledgements

I would like to extend my thanks to the experts I interviewed for this project and who offered their help, providing great insight, contributions, and guidance. This includes Dr. Dejan Dincic, Digital Transformation and Online Learning Specialist at DiploFoundation; Dr. Vladimir Radunovic, Director of Cybersecurity and E-diplomacy at DiploFoundation; Dr. Franziska Klopfer, Project Coordinator at DCAF; Marija Pavlovic, Junior Researcher at the Belgrade Center for Security Policy; Anne-Marie Buzatu, Vice President & Chief Operations Officer at the ICT4Peace Foundation; Dr. Roxana Radu, Research Associate at the CyberPeace Institute; and Mona Zimmerman, Deloitte Cybersecurity Expert. I would also like to thank the SIT academic staff Dr. Gyula Csurgai, Dr. Elisabeth Meur, and Dr. Heikki Mattila for providing advice and points of reference for this project.

Table of Contents

I. Introduction

Today's society is highly interconnected thanks to evolving technologies and infrastructures, consisting of physical structures, servers, and networks transmitting information from one point to another. This is all important given that in today's world, the high level of integration means that the functionality of network systems and its components is paramount. Without adequate means of security, protection, and adaptation, these physical and virtual structures are left vulnerable to various forms of attacks, ranging from attacks on physical structures to cyberattacks meant to cause disruption of the structure(s). This issue requires more attention when it comes to the critical infrastructure (CI) of a country, physical or virtual, which is also vulnerable to such forms of attacks that individuals, state, non-state actors, or state-sponsored actors can conduct. The effects of attacks vary by region, by sector(s) affected, and types of motivation behind the attack, but in general, attacks on CI have disruptive effects, and in an increasingly interconnected world, this is becoming a major challenge for states, corporations, and other entities affected.

The region of focus is Southeastern Europe, a strategic location for the United States, China, Russia, and Turkey. Here, these states are involved to varying extents seeking to promote their respective interests, such as Turkey collaborating with local partners in Bosnia Herzegovina or China negotiating with Serbia and Montenegro to expand its Belt and Road Initiative infrastructure projects. For countries such as the United States, China's developments are of major concern, particularly when it comes to the promotion of human rights and democracy. Likewise, Russian regional involvement has also been a challenge, in terms of political and/or economic involvement. In recent years, there have also been several cyberattacks in North Macedonia and election infrastructure attacks in the region. It is important to note these issues

given that the CI in these countries is still in development stages. More importantly, there is a lack of adequate safeguards against cyber-attacks or attacks on physical networks by state, non-state actors, or state-sponsored actors. With several external actors involved in the region, it is easy for vulnerabilities to be exploited.

The overarching question of this project is the following: How can public and private sectors in Southeastern European countries effectively cooperate to ensure the protection of physical and cyber CI? It is understood that this form of collaboration will bring benefits to cybersecurity (CS) and CI protection, but how exactly these partnerships are developed in the region is equally as important to consider. The focuses of this paper are to understand the state of CS in Southeastern Europe, including cyber and physical CI, the role of public and private sectors and CI, and cooperation between both sectors, which is a common theme addressed in interviews with experts and the literature.

I argue that a tailored approach to public and private sector cooperation in Southeastern European countries, with a degree of oversight, is a more effective solution to improving the state of cyber and physical CI. A degree of oversight means guidance from a regional organization, however, the bulk of the work for CS and CI is done within a state's context. For example, in Albania, it would be the AKCESK agency. The literature does not discuss such approaches for the region in-depth, however, other fields of study, such as the peacekeeping and conflict intervention field, have proposed contextual approaches which are applicable to the CI situation in Southeastern Europe. This paper serves to build on the existing literature that proposes further cooperation between public and private sectors while arguing that each country in Southeastern Europe will need a different strategy for effective solutions to improve the security and protection of the current physical and cyber CI.

The structure of this paper is as follows. The literature review will look at CS readiness and the current discussions about public and private sector cooperation, followed by an explanation of the research methodology. The terminology section looks at terms used in this paper and definitions. The section "State of Cybersecurity in Southeastern Europe" provides a broader overview of current security and protection measures of physical and cyber CI. The section "Public and Private Interest Cooperation in Southeastern Europe" elaborates on existing findings regarding cooperation between both sectors, arguing for a case-by-case approach in Southeastern Europe. For "Current and Emerging Threats," the discussion focuses on assessing threats in Southeastern Europe. The final section provides conclusions.

II. Literature Review

Reports from organizations, such as DiploFoundation and DCAF, point out that CS and CI protection in Southeastern Europe is not sufficient to protect from attacks that target CI. However, there has been progress in recent years "in formally establishing the legal and operational frameworks in most of the countries of the Western Balkans" (Minovic et al., 2016, p. 22). A report by Popovska (2016) points out that different countries are at different development stages of CS and CI measures. For instance, whereas Albania has "a national body that deals with cyber security (formerly the National Security Computer Agency (ALCIRT) and now the National Authority for Electronic Certification and Cyber Security (AKCESK)), Bosnia lacks such a body dealing with these issues" (p. 27-28). Kosovo* is also in its early stages of CI protection as it recently passed laws, directives, and measures focusing on CI, though more initiatives are underway (Bund and Esteve-González, 2020, p. 36-38). Serbian institutions are in a "Formative to Established" stage, including its national CS strategy, incident response (national CERT), and CI protection (Herman and Avila, 2019, p. 23-33). It is clear that some countries

have more developed CS and CI strategies, in part due to the lack of funding for CS and CI projects, underinvestment in CI, the lack of newer infrastructure, and the national governments having varying priorities.

In terms of public and private sector collaboration, it is agreed that it will benefit those involved in it. For instance, at national and regional levels, these partnerships allow for "mutual efforts in achieving the optimal level of security on the production, transport and distribution of energy through the [CI] network" (Bardzieva, 2017, p. 78). Others explain that "Cybersecurity involves public-private partnership as highlighted by policy initiatives and public statements on the value of public-private partnerships" (Kruglov et al., 2019, p. 624). In the case of Serbia, the rising "annual gross income of private security companies . . . from €10 million in 2001 to approximately €26 million in 2003 and to €140 million in 2010 (according to official data from the NBS Solvency Centre)" highlights the important role the private sector(s) have in protecting CI (Davidovic et al., 2012, p. 61). The amount of resources the private sector has in comparison to public sectors showcases the importance of public/private partnerships at national and regional levels in order to effectively address CS and CI shortcomings. These discussions are central to the paper, which include how to improve CS in the region and how to make PPP effective.

III. Research Methodology

The research methodology of this paper is as follows. Key information comes from academic journals of different parts of the world and reports from organizations that focus on CS, CI, or both. For instance, some sources are from Southeastern European academic journals, institutes, and researchers who are involved in the region. These perspectives are important as these provide important insight into the region's developments on CI. I have also looked at reports from organizations based in Geneva, Switzerland, such as DiploFoundation, which has

released reports on Southeastern Europe CI and regional CS in recent years. I also use academic sources from organizations and institutes in the European Union (EU) and the United Kingdom, including the UK based Oxford Martin School: Global Cyber Security Capacity Centre. Gathering these sources serves to complement and support the research findings and information from experts I interviewed.

Part of the research methodology also included interviews from experts in the field or related fields. These experts are from Geneva based organizations, such as DCAF, DiploFoundation, and the CyberPeace Institute, who provided important context about the general state of CS in Southeastern Europe, insight as to how public and private interests can cooperate, and potential problems to address before such initiatives take place. These experts also suggested additional resources for reference that have been useful for the main points and arguments of the paper. Note that a majority of the data used for this paper is qualitative, and any quantitative references come from sources cited for this project.

In all, the research methodology for this project is focused on obtaining qualitative data as the project looks at the broader implications of CS and CI measures versus the quantitative data specifics of CS. It is these broader implications, outcomes, and avenues of cooperation that are the primary focus. By having sources from different organizations from different locations, it provides for varying perspectives and opinions, all which are important to consider given the emerging challenges that come with securing CI in a world where the digital and physical are becoming increasingly interconnected.

IV. Terminology

One of the key terms of this paper is cybersecurity (CS), which encompasses various aspects of protection, security, and adaptability in the digital world. Azmi and Kautsarina (2019)

explain that “cyber” can be added to “space” and “security” to modify the term’s meaning (e.g. “cyber space” and “cyber security”) and it can also be used “combined with its corresponding domain,” such as cyberspace and cybersecurity (p. 22). In this paper, it will be used as the latter given the interconnectedness of both terms in the context of CI. Additionally, Azmi and Kautsarina (2019) note that the term “cybersecurity” is interchangeably used with “information security” where the former focuses on organization and the latter refers to “collaboration to address issues on security domains in cyberspace” (p. 23). For the purposes of this paper, CS will focus on the latter points of Azmi and Kautsarina’s (2019) and in the context of CI protection, though some aspects of “information security” are discussed where relevant. More about this definition and what CI is is explored below.

Critical infrastructure (CI) is another important term. Its definitions can vary depending on the region one considers as definitions have different considerations of what CI is in European, Asian, African, and Asia-Pacific countries (Gallais and Filiol, 2017, p. 65). Definitions also tend to be divided “into two parts. First there is the list of its components; and, second, there are the consequences of its disruption, damage, or destruction” (Gallais and Filiol, 2017, p. 71). It is important to note that these definitions do not always include the “human factor,” “intelligence perspective,” and “the critical infrastructure environment” (Gallais and Filiol, 2017, p. 72). Definitions of CI can also be vague or non-specific. Such definitions are “open-ended and . . . aimed to contain any infrastructure [where] its malfunction or loss negatively affects the nation [providing] a general idea of what governments understand as critical to their nations” (Harašta, 2018, p. 3). In other words, governments in Southeastern Europe can have different definitions for CI depending on what they perceive as “critical.” For the purposes of this paper, CI refers to the essential physical and virtual structures in which their

security, protection, and functioning are imperative to a state and its society, where disruption, natural or human-caused, will inhibit daily functioning. This definition does not focus on a particular sector as CI can vary from place to place, as pointed out in explanations above.

In this paper, Southeastern Europe refers to the countries of Albania, Bosnia-Herzegovina (or Bosnia), Croatia, Kosovo*, Montenegro, North Macedonia, and Serbia. While some reports use "Western Balkans," this term does not encompass the full region, hence the use of "Southeastern Europe." This paper will mainly include information from Serbia given its role as the dominant economy of the region, though information and developments from neighboring countries will be included where relevant for comparison and insight into different security strategies.

V. State of Cybersecurity in Southeastern Europe

The state of CS in Southeastern Europe is still in developing stages. Some countries have laws targeting cyber crime and data protection, while others lack a concrete national agency dealing with these issues. This section will provide a more detailed insight into the CS laws, national and regional entities, and measures that are present or lacking in the region, using reports from various organizations as a reference point, interviews with experts, and examples from countries in the region. The country examples are Albania, Bosnia Herzegovina, Croatia, and Serbia. I selected these countries given that Albania is in the process of EU membership, Bosnia is not in the EU, Croatia is an integrated EU member, and Serbia is a regional economic power. These countries also have varying progress on cybersecurity and CI protection, which will serve to make comparisons among these countries and the region.

Abania's CS readiness and CI protection includes several laws and a designated national agency, AKCESK (formerly ALCIRT). These laws include "Law No. 9918, dated 19.05.2008,

"On Electronic Communications in the Republic of Albania", as amended; Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended; Law No. 2/2017 "On Cybersecurity" (2017)" (DCAF, 2021, p. 4). These laws are meant to create a "safer, more reliable and more sustainable cyberspace for citizens, business and government in support of economic and social development" (DCAF, 2021, p. 5). This work dates to 2008 when Albania began its "National Cross-cutting Strategy on Information Security (2008-2013) strategy [prioritizing CS and] the creation of ALCIRT as the national institution for response to cyber-incidents" (Minovic et al., 2016, p. 15). As a NATO member, Albania has also signed the Memorandum of Understanding (MoU) (Minovic et al., 2016, p. 16). Furthermore, the country has adopted a new CS strategy for 2020-2025 addressing CI protection in the financial, health, energy, and transport sectors (Decision No. 1084., 2020, p. 1484-1488). These action steps highlight the emerging challenges of CS in the 21st century and the need to address them as soon as possible. Albania's case demonstrates the ever increasing priority these issues will need and how Albanian authorities are targeting these issues.

Bosnia-Herzegovina's institutions handling CS and CI include the "Ministry of Communications and Transport of Bosnia and Herzegovina; Ministry of Security in Bosnia and Herzegovina; Federal Ministry of Transport and Communications at Federal level; and Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska" (DCAF, 2021, p. 9). There are laws dealing with different aspects of CS, such as the "Law on Communications (2006); Law on Electronic Signature (2006); Law on Electronic Business Transactions (2007)", though overall, there is a lack of a comprehensive approach and cooperation (DCAF, 2021, p. 9). This means that there is little information sharing between the agencies and the laws are not adequately enforced. At the entity level, there is the "Department

for Information Security within the Agency for Information Society of the Republika Srpska" unit focusing on "computer security incidents and to supervise implementation of standards and measures of information security" with little information about the other entities (Minovic et al., 2016, p. 17). The Bosnian CS and CI protection framework is in its early stages, and there is a notable lack of cooperation between the national organizations and regional entities that is hindering crucial progress on this front, putting Bosnian CS and CI in a vulnerable position.

As a EU member, Croatia has adopted the EU framework on CS as part of its membership, making its laws and regulations "compatible with the EU regulation" (Minovic et al., 2016, p. 17). The country has its "government CERT called ZSIS-CERT, situated in the Information Systems Security Bureau (ISBB) [which oversees] technical areas of information security of [Croatian] state bodies" (Minovic et al., 2016, p. 17). These measures show a high level of priority on addressing CS issues, which, in collaboration with the EU, gives Croatia an advantage. There is also a National Cyber Security Strategy, adopted in 2015, which aims for "a balanced and coordinated response of various institutions representing all the sectors of society to the security threats in modern-day cyberspace" (Minovic et al., 2016, p. 18). Overall, there is a high level of CS readiness in the country, which, if maintained, places Croatia in a strong position on CS and CI protection measures. Croatia being a part of the EU also gives it a way to receive additional assistance or advice on CS and CI measures.

Serbia is the regional economic power in the region, and its role is important when it comes to CS and CI measures. It has taken steps to address CS and CI concerns, such as establishing "legal and institutional framework . . . based on the Law on Information Security [of] 2016" (Minovic et al., 2016, p. 21). Serbia also has a "National CERT hosted by the Regulatory Agency for Electronic Communications and Postal Services (RATEL)" (DCAF,

2021, p. 29). The goals of these measures include "enhanced operations of [important ICT systems]; information security; increased capacities . . . against high-tech crime; [based on] cooperation between the public and private sector, NGOs, the academic community and other actors" (DCAF, 2021, p. 30). Signaling public and private sector partnerships (PPP) as part of its goals is an important step towards general CS and CI measures as it can facilitate the sharing of information, databases, and cooperation where necessary. Serbia also has a "formative to established" CI protection capacity given its "[2018] Law on Critical Infrastructures, which [identifies several] national critical sectors" (Herman and Avila, 2019, p. 30). Note that Serbia is also in talks to obtain EU membership, meaning that these action steps outlined above are essential to fulfill. For instance, in 2019, it amended "the Law on Information Security" to include provisions of EU laws, essential to maintaining uniformity with the standards outlined by the EU (Herman and Avila, 2019, p. 30). In all, Serbia is taking the steps to update and improve CS and CI measures necessary for the well-being of the country's CS and CI. EU membership would also introduce Serbia to additional resources similar to other member countries.

CS and CI in Southeastern Europe is in need of greater prioritization. Dr. Vladimir Radunovic, Director of cybersecurity and e-diplomacy projects at DiploFoundation, explained that there is an awareness that CS and CI issues are becoming important in the region, but at a practical level, these are not developed (Radunovic, 2021). There is also no clear understanding of what is CI, CS, and telecommunications in part because there are no uniform definitions (Radunovic, 2021). Dr. Franziska Klopfer, Principle Programme Manager in the Europe and Central Asia Division of DCAF, adds that countries have different categorizations of what is CI, some have laws but are undefined, and it is important to consider what are CI components in each country (Klopfer, 2021). Junior Researcher Marija Pavlovic also adds that Southeastern

European countries have a case-by-case development, with some still lacking measures and others working on implementing measures (Pavlovic, 2021). CS and CI in Southeastern Europe points to a lack of clarity in some countries, firm goals in others, some PPPs, and national/regional agencies in countries present but not operating to their full potential. This is where the role of PPP becomes key in improving the state of CS and CI in the region in conjunction with national governments and relevant actors.

VI. Public and Private Sector Cooperation in Southeastern Europe

PPP can help improve the state of CS and CI in the region. How this will look like in each country varies, which is why I argue for a case-by-case approach in the region. The next section will provide an overview of PPP, its aspects, how exactly it benefits the actors involved, and will elaborate on the argument presented, using Serbia as an example of how its PPP will be, how these should be developed, and how the Serbian government can assist these efforts.

Public and private interest cooperation (also public private partnerships (PPP)) is generally seen as beneficial. In this context, PPP involves public and private sectors collaborating on a given project/topic (or several)in order to improve CS and CI. Roxana Radu, research associate at the Geneva-based CyberPeace Institute, explained that in general, everyone has a responsibility and collective action in these sectors; the public sector has an interest to protect, and the government has a role of responding to these needs with the help of the private sector (Radu, 2021). In addition, there must be a cyber resilience framework in a given country by the government, though in some cases, governments impose more control of the process, must meet a set government criteria, and in other cases, delegate this work to the private sector companies (Radu, 2021). This is important given that the public sector “is the owner of some part of the critical infrastructure systems or communication systems which is usually managed

by private operators" (Limba, 2017, p. 561). Note that different private sectors may be better prepared than others as is the case in Serbia; the energy, finance, and health sectors are more prepared (Radunovic, 2021). PPP in Southeastern Europe will become increasingly important given the degree of interdependence of CI and the different sectors, which can also happen across borders.

My argument calls for tailored PPP approaches that consider a country's context in order to better meet its needs. Here, the "country's context" refers to: the public and private sectors of a country, what is designated as CI (to help better understand how PPP are shaped), existing PPP, the role of a country's government, followed by an analysis of these points. When these factors are considered, it allows for more meaningful and concrete PPP that benefit CS and CI measures, thus benefiting the broader population and state of CS. I then propose the creation of an organization focused on CS and CI needs, composed of Southeastern European countries, overseeing these efforts with member states then implementing CS and CI measures as relevant to their situation(s).

The following paragraphs will look at the public/private sectors in Serbia and national government roles. In Serbia, the public sectors are headed by the Ministry of Public Communication, the Office for IT and E-Government, and the national CERT; the private sectors are headed by companies such as Microsoft, IBM, and McAfee (Radunovic, 2021; Pavlovic, 2021). Some of the general sectors in Serbia include energy, finance, government, health, telecommunications, with private companies having a major role in these sectors (Radunovic, 2021). Note that there is also not enough information about all the companies in the private sector and information sharing with the public sector (Klopfer, 2021). These sectors are mainly private-led, and they hold much responsibility for CS and CI measures, which makes their role

essential in promoting CI protection and reinforcing CS. Given the different sectors of the country, PPP in Serbia must focus on existing partnerships and build on these in order to develop new partnerships, such as ensuring information security with Microsoft's data servers and controlled data access.

There are some variations as to how CI is approached and designated. In EU countries, "it is obligatory to determine the supranational CI (on the European level). From the national level upwards, the system stays similar – in most cases it is the national, regional, or local level" [however] "there is a significant difference in the terminology used in individual countries [for CI]" (Novotny et al., 2016, p. 167). While there are key CI sectors in Serbia, not everything is defined. The country is still working to set concrete definitions of CI given that there is no single authority that delegates what is CI (Radunovic, 2021). This puts Serbia in a vulnerable position where the lack of clarity of what is CI becomes an issue in the face of threats. Several countries in the region face similar issues, though Serbia is better positioned to handle them given the existence of institutions that can take on these roles. In North Macedonia, its strategy involves the creation of an agency dealing with computer incidents (MKD-CIRT) and the need to clearly define CI "taking into account the various actors' specific roles in the cyber domain – from individuals to organizations and states" to attract private economic actors (Tasevski, 2015, p. 3-4). These situations in Southeastern Europe further call for country-by-country approaches where each country can assess its needs and implement strategies accordingly: partnerships in North Macedonia are likely to differ from those in Serbia.

Serbia has developed important PPP in the past years. One partnership involves Microsoft, in which the company partnered with the National Ministry to create a data center in Serbia on the Microsoft platform, considered one of the largest PPP in the region (Pavlovic,

2021). The partnership involves cooperation on several key fronts, such as e-government, IT office, information storing, and AI development (Pavlovic, 2021). This has been an important partnership for the country as it involves the vast resources of the private sector being used to create such initiatives. Another important partnership for Serbia and the region is the "Petnica Group," involving the "OSCE Mission to Serbia, DiploFoundation and [DCAF partnering with] the Petnica Science Centre and organized a coordination meeting of key public and private stakeholders in the field of cyber security," therefore making it a broader regional partnership (Rizmal, 2018, p. 41). The group also places an emphasis on policy making in Serbia, "[acting] as a bridge between the technical community and policy decision makers [and] fostering a platform for reaching proposals for joint solutions" (Rizmal, 2018, p. 42). Despite these partnerships, there is still room for improvement. There must be more ways to involve the public and private sector outside of these initiatives for trust building, cooperation, and each private actor should have a system/action plan (Klopfer, 2021). For the case of Microsoft and IBM, it would be having contingency plans in case of emergency and ways they can notify their public sector partners, the national ministry, and the general public about CS and CI developments.

The national government's involvement in PPP is also key in fostering collaborations and maintaining current partnerships. In the region, governments can set up formal working groups, become more open to policy shaping, open dialogue to stakeholders, and improve current PPP to increase trust (Radunovic, 2021). Governments must also be willing to participate in taking these action steps, relocate resources for the project, implement laws, and stray away from the notion that CS is only a national security problem (Pavlovic, 2021). For Serbia, continuing further investments into PPP, whether it is the public or private sector, is also key to the country's overall advancements on CS and CI. One case study notes that private companies make their investment

decisions based on cost-benefits, cost-savings (or avoidance), and for CS measures, these investments are made to avoid security breaches, creating a situation where companies underinvest in CS (Gordon et al., 2014, p. 80-81). It then puts the private actors involved and their supply chains in a vulnerable position where an issue at one point can cascade to another and in some cases, greatly affect the private actor itself. How this happens depends on the number of PPP in a country and the relationship between the public and private sector. In cases where the relationship between these sectors is poor or there is low communication and information sharing, more CS and CI vulnerabilities are likely.

Anne-Marie Buzatu, Vice President & Chief Operations Officer at the ICT4Peace Foundation, adds that one way for governments to encourage private actors to implement action plans, as pointed out by Klopfer (2021), is to have standards and requirements in contracts and improve regulatory efforts (Buzatu, 2021). This task is easier with domestic companies, and in the Serbian context, Microsoft and IBM are external private companies, making external actors comply with local Serbian laws and regulations a challenge. Given that the public sector holds much control over the key CI sectors and CS, the national government relies on the private sector and works with it towards a cyber-resilience framework (Radu, 2021). These measures are becoming more important in an increasingly interconnected world where the failure of one link spells trouble for another or for an entire sector, and Serbia is no exception, and its partnerships with organizations outside the country and national organizations for PPP highlight this.

The points above highlight the need for context-based approaches. Each country's public and private sectors differ, are defined differently, each country has different forms of PPP with different companies, and each government will have different strategies to address CS and CI. As pointed out in Novotny et al. (2016), there are no unitary strategies, even in the EU, much less

outside of it (p. 167). Croatian approaches to CS and CI along with the development of these institutions is different from that of France, Romania, and/or Germany. Novotny's et al. (2016) case-by-case approach considers the following information when assessing strategies for a country: what is the criticality of each sector, the impact of its disruption on society, impact of its disruption on other sectors or sub-sectors, and risk assessment (p. 167-168). For this to happen, there must be a regional organization overseeing these efforts at a national level, similar to the Regional Cooperation Council group, though focused on CS and CI. Henry (2010) proposed an international organization "composed of [IT] security representatives from each signatory state, and to task the organization with coordinating and collaborating joint security measures with states and industries" (p. 17). A similar approach can be taken in Southeastern Europe where there are representatives from the region's countries that report to their respective countries and implement CS and CI measures for their country.

This organization is to be headed by a combination of regional experts and outside experts to provide a variety of perspectives. Each country has its representative(s), which serve as advisers to their national governments and other entities, such as public/private sectors. Note that the broader organization simply serves to provide guidance, information sharing, and guiding cooperation between countries where applicable. For instance, it provides questions such as those proposed by Novotny et al. (2016) for individual country representatives and their governments to use to assess their CS and CI needs. In addition to points made by by Novotny et al. (2016), the organization must also consider the disruption impact (structural, social, economic, political) as a result of cyber attacks, data breaches, or ransomware, how other sectors or sub-sectors are affected (their interdependence), costs of CS/CI investments vs. costs of attacks, and risk assessments on a country's critical sectors. This also helps governments in

Southeastern Europe assess current and potential CI sectors in light of emerging CS threats and CS measures. With these criteria combined, this organization is likely to be more successful rather than having too broad of a focus and not providing a place for discussions.

VII. Current and Emerging Threats

Currently, Southeastern Europe faces different threats, which will evolve in the coming years. During the current period of a global health crisis, cyber threats have gone up in the region. For example, "all Western Balkan national CERTs have reported an increase of phishing attacks [on] individuals . . . the health care sector [particularly government healthcare agencies] e-commerce and e-businesses" (Achten, 2021, p. 4). Radunovic (2021) adds that the government and health sectors can be vulnerable to personal data breaches. In Serbia, these threats are similar as they include cyberattack exploitation, a high degree of disinformation, and ransomware (Pavlovic, 2021). Moreover, human factors are also a key vulnerability where there are people working on CI projects but lack security awareness/knowledge, software/hardware is not updated, and the government not prioritizing CS and CI (Pavlovic, 2021). This can result in personal data and other infrastructures being susceptible to attacks. One case of a cyber attack happened in the Serbian city of Novi Sad where the institution's information was encrypted, thus leaving people unable to use its services (Pavlovic, 2021).

Note that Serbia is also participating in China's Belt and Road initiative, involving various projects that are "interdependent directly or indirectly [meaning that] serious problems in one vital CI [sector] . . . could cause serial interruptions in linked [project structures in Serbia and in the region]" (Todorovic, 2018, p. 254). The high level of interlinkage in the region is also another area of potential threats that actors with malicious intent can exploit, which calls for greater attention to national and regional CS and CI. There is also the lack of cooperation

between institutions that will pose a problem. In the EU, several countries have various national authorities "pursuing fragmented policies [with] significant lack of cooperation between national governments and EU institutions [setting up coordinated emergency responses] to potential threats [despite] interdependent . . . cross-border [CI]" (Gaiser, 2018, p. 50-51). This lack of cooperation is also a vulnerability for non-EU members in the region given the interdependence of infrastructure, making domestic and transnational cooperation essential. Lastly, the protection o f election infrastructure, a key infrastructure in countries around the world, is not being prioritized enough in Southeastern Europe. There have been notable attacks on election infrastructure, as seen in the United States, Western Europe, and North Macedonia, affecting the integrity of these systems, how people view them, and to varying extents, the functioning of their respective governments. However, these trends are slowly changing around the world as more countries begin to prioritize election infrastructure as critical (Radu, 2021). With this in mind, national governments in Southeastern Europe will also need to incorporate election infrastructure as part of CS and CI strategies. In general, current potential threats to the region include cyberattacks such as phishing, ransomware, data vulnerability and breaches, disinformation, lack of knowledge on CS, CI, the digital world, and lack of cooperation, threats which will evolve over time.

To mitigate these risks, countries in Southeastern Europe have adapted awareness raising via "informational materials," public warnings along with country CERTs launching "education aimed at young professionals in order to increase expertise in the region, and technical capacity-building training of CERT staff" in the domestic context (Achten, 2021, p. 4-6). These serve as ways to increase awareness of the threats the region's countries are facing. CS and CI PPP in the region are also another way to mitigate risks, both serving as initial steps in increasing

protection from cyberattacks and CI attacks. The effects of these attacks must be understood to find ways to protect from them, which means understanding how attacks work. While each cyber attack will look differently from another, generally, cyber attacks involve identifying a vulnerability, exploiting, payload, infection, and launching the attack (Limba et al., 2017, p. 563). Making this type of information widely available can also assist national campaigns in further educating its population about the digital world, how cyber attacks happen, how to protect oneself from one, and why it is important to implement robust CS and CI measures.

Cyber attacks also have consequences in the physical world given the high interconnectedness of the physical and virtual components. These attacks can "take place quickly to shock and avoid adaptive response [leading to a] loss of system control . . . situational awareness, ineffective coordination, and [low confidence for a] government to mitigate the damage" (Pfeifer, 2018, p. 30). In Southeastern Europe, where political tensions are high, trust in governments is generally low, and where some countries have limited development and PPP, such attacks would have ripple effects in one region to the rest given the interconnectivity of CI. The types of attacks and their methods also depend on the final goal of intrusion and the social aspects of the attack (Radu, 2021). For instance, an attack on a country's energy sector disrupts energy use in the affected region or country, and the goals of the attack may be for criminal, political, social, economic, or military warfare motivations. Radunovic (2021) also pointed out that in the case of Serbia, some XI sectors are better prepared to handle cyber attacks to its CI, which means that CI sectors less prepared are more vulnerable to attacks or greater consequences as a result. Note that cyber attacks on CI between states are not common, though their frequency is likely to increase along with the scale of targeted attacks (Radu, 2021). This is because state actors have "the most capable threat, as they have the ability to funnel significant resources and

talents into these efforts" (Henry, 2010, p. 3). However, the role of non-state actors cannot be disregarded. While they may not have as many resources as state actors and/or state-sponsored actors, non-state actors can still pose substantial threats to states. For instance, these actors can target different CI at once via coordinated cyber attacks, and with several small attacks, this can overwhelm the national authorities' response and untilatemy cause similar or higher levels of disruption as a state-sponsored attack.

Something else to consider is the difficulty of tracing an attack to the perpetrator(s). Responsibility can be more easily traced to state actors, but for non-state actors that operate anonymously or across national borders, it becomes difficult for states to assign responsibility for costly damages to CI and adequately respond given the use of fake IP addresses, pseudonyms, and increasingly easy ways to destroy data that may trace to the identity of the perpetrator(s). This highlights the importance of risk assessment by national governments and agencies. How costly are cyberattacks per sector? What are the likelihoods of being cyber attacked by a state actor versus a non-state actor? Can responsibility ever be attributed to an entity? National governments in Southeastern Europe must assess these questions as they implement CS and CI measures to consider the various types of threats that CI faces, which will only grow in the coming years.

Despite the potential threats, there are ways to protect and increase existing robustness of laws, CS and CI. One important point is to assume that systems are vulnerable, also referring to the "Zero Day Vulnerability" (Klopfer, 2021; Buzatu, 2021). By assuming that systems are vulnerable at all times, it allows for constant improvement and development of CS and CI in the region; complacency can have major consequences. While there is now more general awareness of the importance of CI and its vulnerabilities, governments, public and private sectors must also

be transparent about their work. Sometimes, actors in these sectors do not announce vulnerabilities to the public or government, stockpile them, or keep it a secret (Buzatu, 2021). Not knowing this information makes it challenging to plan effective CS and CI strategies that can further protect a country's infrastructure and overall CS. For broader measures, domestic and international cooperation on CS and CI must also be at the forefront of Southeastern European governments. This can be done through agreements on protecting CI and defining standards for information sharing, addressing complexities, and acknowledging shared risks (Henry, 2010, p. 15-19). Reducing complexities and facilitating cooperation among states will become increasingly important in light of the growing complexities of attacks and protection measures.

To protect from threats, there must also be guarantees by states to look out for one another. One of the proposals by the "Open Ended Working Group," a group under the United Nations Human Rights Council, has norms for states to not attack CI of another state and for states to ensure that their CI is secure (Buzatu, 2021). Limba et al. (2017) proposes a CS management model for CI that considers the following: legal regulation, good governance, risk management, security culture, technology management and incident management, with initial, moderate, and full integration levels of management (p. 566). This model incorporates various important considerations for CS and CI measures that are lacking in Southeastern Europe. While it is not the answer to all the problems, it provides a more robust response and approach to address the region's CS and CI shortcomings. These models must also address the roles of non-state actors, which can also pose equal, if not, greater risks in terms of cyber attacks.

VIII. Conclusion

In sum, the general state of CS and CI in Southeastern Europe requires improvements in how CS and CI needs are addressed. Some countries do not have a comprehensive strategy, and

given the interconnectedness of CI in the region, it makes it susceptible to cyber attacks on CI. While some sectors may be more lucrative targets for attackers, all sectors are vulnerable. However, by implementing PPP in the region that addresses each country's needs, the likelihood of cyber attacks on CI will be reduced, though not completely gone. A regional organization overseeing these efforts is necessary to ensure progress monitoring in the form of check-ins and for general guidance, with the respective countries leading their focused efforts. As technology continues to evolve, the organization's role and the country's PPP will also evolve, providing ways to navigate an environment where attack perpetrators are increasingly difficult to track, act alone or in coordination, and cause extensive damage. This is where trust building, information sharing, transparency, and between governments and public/private sectors will become essential in order for PPP to succeed and improve upon existing PPP.

Moving forward, the role of national governments will remain crucial in promoting new PPP across different CI sectors. Not only that, but CI legislation will also have an important role in advancing new proposals, amending current laws, and promoting digital awareness campaigns. Moreover, adapting different types of awareness campaigns will serve more useful than launching a single form of campaign, which also includes using different platforms to disperse the messages. The private sector must also make use of its already important role in promoting these efforts within the partnerships it has in Southeastern European countries and across the region. These strategies and recommendations combined will not resolve the existing and other underlying problems in the region, though it can pave the way for model-setting initiatives that benefit the region's countries' current and future CS and CI measures.

IX. Abbreviation List

ALCIRT – Agjencia Kombëtare për Sigurinë Kompjuterike (National Security Computer Agency)

AKCESK – Autoriteti Kombëtar Për Certifikimin Elektronik Dhe Sigurinë Kibernetike (National Authority for Electronic Certification and Cyber Security)

BCSP - Beogradski Centar za Bezbednosnu Politiku (Belgrade Center for Security Policy)

CERT – Computer Emergency Response Team

CI – Critical Infrastructure

CS – Cybersecurity

DCAF – Geneva Centre for Security Sector Governance (Democratic Control of Armed Forces)

EU – European Union

ISBB – Information Systems Security Bureau

IT – Information Security

KOSOVO* – "This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo declaration of independence." This is borrowed as found in Minovic et al. (2016).

MoU – Memorandum of Understanding

NATO – North Atlantic Treaty Organization

NIS – Network Information Systems

OSCE – Organization for Security and Cooperation in Europe

PPP – Public Private Partnership(s)

RATEL – Regulatory Agency for Electronic Communications and Postal Services

Bibliography

Achten, N. (2021). *Cyber Threats During the COVID 19 Outbreak and Activities of National CERTs in the Western Balkans*. DCAF - Democratic Control of Armed Forces.

Azmi, R., & Kautsarina. (2019). Revisiting Cyber Definition. *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, 22-30.

Bardzieva, L. (2017). The role of the private security in the critical infrastructure protection in some of the balkan states. *Bezbednosni Dijalozi, 2*(2), 75-89.

Bund, J., and Esteve-González, P. (2020). *Cybersecurity Capacity Review: Republic of Kosovo*. Global Cyber Security Capacity Centre; University of Oxford.

Buzatu, A. M. (2021, Dec. 1). *Interview on The Role of Public and Private Sectors in Protecting Critical Infrastructure in Southeastern Europe* [One-on-one interview]. Conducted via zoom in Nyon, VD, Switzerland.

Davidovic, D., Kesetovic, Z., & Pavicevic, O. (2012). National critical infrastructure protection in Serbia: the role of private security. *Journal of Physical Security*, *6*(1), 59-72.

DCAF. (2021). *National Cybersecurity Strategies in Western Balkan Economies*. DCAF - Democratic Control of Armed Forces.

Decision No. 1084. (2020). *On Adopting The National Cybersecurity Strategy And Its Action Plan 2020-2025*. Deputy Prime Minister Erion Braçe; Government of Albania.

Gaiser, L. (2018). European critical infrastructure protection: The need for a regional approach and a cyber constant contact strategy. *National security and the future, 19*(1-2), 45-63.

Gallais, C., & Filiol, E. (2017). Critical infrastructure: where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. *Journal of Information Warfare, 16*(1), 64-87.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2014). Cybersecurity Investments in the Private Sector: The Role of Governments. *Georgetown Journal of International Affairs*, 79–88.

Harašta, J. (2018). Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protection, 21*, 47-56.

Henry, J. (2010). Reducing the Threat of State-to-State Cyber Attack against Critical Infrastructure through International Norms and Agreements.

Herman, K., and Avila, O. N. (2019). *Cybersecurity Capacity Review: Serbia*. Global Cyber Security Capacity Centre; Department of Computer Science, University of Oxford.

Klopfer, F. (2021, Oct. 29). *Interview on The Role of Public and Private Sectors in Protecting Critical Infrastructure in Southeastern Europe* [One-on-one interview]. Conducted via zoom in Nyon, VD, Switzerland.

Kruglov, V., Latynin, M., Horban, A., & Petrov, A. (2020). Public-private partnership in cybersecurity. *CEUR Workshop Proceedings* (2654), 619-628.

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Journal of Entrepreneurship and Sustainability Issues 4*(4), 559-573.

Minovic, A., Abusara, A., Begaj, E., Erceg, V., Tasevski, P., Radunovic, V., & Klopfer, F. (2016). *Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities*. DiploFoundation.

Novotny, P., Markuci, J., Rehak, D., Almarzouqi, I., & Janusova, L. (2016). Critical infrastructure designation in European Union countries: Implementation of systems approach. *Communications-Scientific letters of the University of Zilina*, *18*(2), 163-169.

Pavlovic, M. (2021, Nov. 24). *Interview on The Role of Public and Private Sectors in Protecting Critical Infrastructure in Southeastern Europe* [One-on-one interview]. Conducted via zoom in Geneva, GE, Switzerland.

Pfeifer, J. W. (2018). Preparing for cyber incidents with physical effects. *The Cyber Defense Review, 3*(1), 27-34.

Poposka, V. (2016). The Urge for Comprehensive Cyber Security Strategies in the Western Balkans. *Information & Security*, *34*(1), 25-36.

Radu, R. (2021, Nov. 3). *Interview on The Role of Public and Private Sectors in Protecting Critical Infrastructure in Southeastern Europe* [One-on-one interview]. Conducted via Microsoft Teams in Nyon, VD, Switzerland.

Radunovic, V. (2021, Oct. 21). *Interview on The Role of Public and Private Sectors in Protecting Critical Infrastructure in Southeastern Europe* [One-on-one interview]. Conducted via zoom in Nyon, VD, Switzerland.

Rizmal, I. (2018). *Guide Through Information Security in the Republic of Serbia 2.0*. OSCE - Organization for Security and Cooperation in Europe.

Tasevski, P. (2015). Macedonian Path Towards Cybersecurity. *Information & Security, 32*(2), 3204(1)-3204(11).

Todorovic, B. (2018). “The One Belt, One Road” Initiative Related Critical Infrastructure Protection at a Crossroads in Balkans. In V. N. Cvetković (Ed.), *The New Silk Road: European Perspectives: Security Challenges/Risks Within the Initiative 16+1* (pp. 243-257). Belgrade, Serbia: University of Belgrade – Faculty of Security Studies.