Passive Cyber Defense as a Norm Preservation Tool: Romania's Behaviour as a Norm Antipreneur in Cybersecurity

Răzvan-Ovidiu CEUCA
'Babeș-Bolyai' University of Cluj-Napoca
ceucarazvan@gmail.com, razvan.ceuca@ubbcluj.ro

Abstract: The complex challenges of cyberspace have pushed the states of the world to promote cybersecurity approaches addressing these challenges. While some states advocate for the contentious new active cyber defense approach, others continue to rely on the current passive cyber defense strategy. Previous contributions in literature have identified the technical, legal, and political elements impacting state-level decision-making, while omitting normative incentives. Therefore, this study aims to explain why Romania normatively employs passive cyber defense. Empirical evidence shows that Romania acts as a norm antipreneur, promoting a passive cyber defense that cultivates the civil society's resilience through cybersecurity research, training, and dissemination of information of public interest.

Keywords: active cyber defense, cybersecurity, norm antipreneur, norm change, norm preservation, passive cyber defense, resilience, resilient cyber defense.

INTRODUCTION

Cyberspace has evolved into a critical arena and focal point of international relations. The sophistication of cyberthreats (Kesan & Hayes, 2012; Rid, 2013; Virvilis & Gritzalis, 2013), the diversity of malicious actors (Deibert & Rohozinski, 2010; Lachow, 2013; Vacca, 2014), the variety of cybercrimes (Brenner 2001; Brenner 2004), and the tendencies of certain states to sovereignize the Internet (Shen, 2016; Glen, 2021) are just a few issues that have been put on national, regional, and international political agendas. To solve them, the states of the world support the adoption of two key cybersecurity approaches: active cyber defense (ACD) and passive cyber defense (PCD) (Denning, 2014; Dewar, 2014; Dewar, 2017). The more complicated and sophisticated cyberspace threats have driven some of these state actors to argue for a shift to the former approach, even though the latter suited the states' cybersecurity demands. Other states, however, continue to adopt the PCD approach (Chabinsky, 2013; Herpig, Morgus

https://doi.org/10.54851/v5i2y202302

& Sheniak, 2020), despite efforts by some governments to make ACD a recognized and internalized norm. Despite the fact that past research has revealed technical, legal, and political reasons impacting state decision-making, no contributions have provided normative grounds for states' resistance to the ACD norm. This study seeks to fill this gap by investigating how Romania promotes its PCD both internally and externally, as well as answering the following research question: why does Romania act as a norm antipreneur in relation to state-level cybersecurity approaches?

The process of norm change is maintained in the international system by four categories of actors: two agents of change, norm entrepreneurs and competitor entrepreneurs, and two agents of resistance, norm antipreneurs and creative resisters (Bloomfield, 2015). This study contends that Romania acts as a norm antipreneur in cybersecurity because it lacks the technical, legal, and political capabilities to be a norm entrepreneur advocating the use of ACD means, and thus it aims to enforce its PCD in relation to the actual realities of the digital ecosystem. Based on this argument, this study is structured as follows. The second section summarizes previous research on ACD and PCD. The third discusses how state actors react in instances of norm life cycles using Alan Bloomfield's conceptual framework. The fourth section goes into detail about the methodological design, and the fifth one covers a case study, in which Romania is empirically researched based on its vision and objectives of the National Cyber Security Strategy (NCSS) for the 2022-2027 period, as well as Facebook posts uploaded by three key cybersecurity institutional actors: the National Cyberint Centre, the National Cyber Security Directorate (NCSD), and the Romanian Association for Information Security Assurance (RAISA). Finally, the last section of this study includes the conclusion of this paper, indicating that Romania is a cybersecurity norm antipreneur, cultivating its resilient cyber defense on a home level while advocating the PCD approach on a regional and international level and rejecting the rising ACD norm.

ACD AND PCD ON A NORMATIVE CLASH

Although PCD has been used as a cybersecurity approach by states over time, given the considerably more complicated reality and threats in cyberspace, ACD has emerged as a key cybersecurity norm in the last decade for technical, legal, and political reasons.

Given the scarcity and low level of sophistication of cyberthreats in the early days of cyberspace, PCD was the most common cybersecurity approach adopted by all parties controlling this domain. Malwares used to prey on single- or multi-user systems. Malwares can now infect new targets and take over Internet-connected equipment as the digital world evolves (Lehtinen et al., 2006). Furthermore, at the time, the most evident threat to the Internet was posed by mischievous youths wanting to earn or develop a reputation in the hacking community (Amoroso, 2011). PCD means were (and still are) judged adequately in that context for reducing the harm caused by successful intrusions (Dewar, 2017; McLaughlin, 2011). Cyber hygiene techniques, such as the correction of software weaknesses, can assist victim nations in mitigating the effects of low-level cyberattacks (Lachow, 2013). Additionally, because these attacks often target critical components of national infrastructure, certain states have a tendency to develop resilient cyber defense techniques. Under these conditions, the primary purpose of states is to ensure that critical infrastructure systems continue to function during a malicious cyber incident (Dewar, 2017; Herpig et al., 2020). As a result, it was assumed that strengthening the fortification and resilience of state, private, and individual digital assets would be sufficient to combat and neutralize the primitive cyberthreats of the time while also keeping up with cyberspace transformations (McLaughlin, 2011; Chabinsky, 2013; Dewar, 2014; Flowers & Zeadally, 2014).

Nonetheless, a new cybersecurity norm has evolved in the previous decade, along with new digital transformations: ACD. Simply said, according to Yağlı & Dal (2014), ACD is 'a range of actions to respond to attacks with offensive options' (p. 7). As it is stated by Rosenzweig (2013), it can also be depicted as 'the synchronized, real-time capability to discover, detect, analyse, and mitigate threats' (p. 2). Because of the advent of the 'advanced persistent threat' phenomena (Virvilis & Gritzalis, 2013; Munish et al., 2019), both state-level and private players are being compelled to re-evaluate their current cyber defensive strategies (Lachow, 2013; Pattison, 2020; Wong, 2011). This is how hack-back techniques, white worms, honeypots, port and address hopping, and others became popular (Shi et al., 2007; Lu, Xu & Yi, 2013; Denning, 2014; Zheng, Lu & Xu, 2015; Dewar, 2017). Of course, the fundamental advantage of these proactive (and occasionally offensive) techniques is their capacity to trace cyberattacks for the defender (Locatelli, 2011; Rid & Buchanan, 2015; Turunen & Kari, 2020). Because cyberspace is amorphous and anonymous blackhats utilize plausible deniability to obscure digital traces of their activity, harden digital forensics, and avoid punishment (Maurer, 2015; Cormac & Aldrich, 2018). As a result, states have been forced to invest technological, financial, and human resources in proactive security measures in order to respond to the developing cyberthreat landscape.

A primary set of considerations supporting the normative change from PCD to ACD is related to both the beneficial and negative impacts of technical processes occurring in cyberspace. The sophistication of attacks is the key technological reason for nations' rising choice for ACD (Kesan & Hayes, 2012; Rid, 2013; Virvilis & Gritzalis, 2013). Malwares are programmed to become more complex and intelligent (Wong, 2011). Moreover, the multiplicity of blackhats forces authorities to take a proactive approach. State-sponsored groups have emerged as advanced persistent threats, relying on system administrators' ignorance of their methods of operation to conduct cyber espionage activities and elude discovery (Lachow, 2013; Vacca, 2014). All of these variables have contributed to an imbalance in offensive and defensive tactics. Because network systems are interconnected, malicious codes are automatically amplified, whereas passive defensive methods are not since they are reactive. Likewise, offensive activities are low-cost and have a high payback for the offence, whereas defensive operations are costly and ineffective (Lu, Xu & Yi, 2013; Zheng, Lu & Xu, 2015). Consequently, the infrastructure of the cyberspace has developed in a way that strengthens the attacker and weakens the defender, prompting the latter to employ ACD.

The second set of grounds for the application of the ACD approach is the legal ambiguity surrounding the applicability of international law in cyberspace and the necessity to hold blackhats accountable. The growth in politically motivated cyberattacks has pushed states to build an international normative framework that allows the use of ACD (Sklerov, 2009; Cook, 2018). Cyber analysts distinguish between computer network exploitations or passive cyberattacks and computer network attacks or active cyberattacks. Passive cyberattacks include internal monitoring and the theft of confidential information without the approval of the owner or system administrator. Active cyberattacks employ information technology to disrupt and impair the essential infrastructure of the target state (Nye, 2016; Engli, 2020). Additionally, politically motivated cyber attacks, as well as inadequacies in the application of international law in cyberspace, force states to limit the deployment of ACD methods through the use of the laws of war (Sklerov, 2009). Given the existence of some digital norms and principles, as well as the unknown origins of these cyberattacks in the first place, states can employ proactive strategies to identify the blackhats (Schulzke, 2018; Tran, 2018). This process is known as attribution (Hare, 2012; Schulzke, 2018; Assumpção, 2020). In international law, there are several doctrines that address how to deal with state culpability in cyberattacks. According to the State Responsibility Doctrine, a state is liable for a non-state actor's wrongdoing if one of two conditions is met: (1) the non-state actor behaves as if it were a state organ, or (2) the non-state actor acts in accordance with the state's instructions, directions, and control (Tran, 2018). At the national level there are two types of attributions. Technical attribution deals with direct evidence of a cyberattack, particularly forensic evidence. It requires looking into things like the malware's source code, network activity during the event, language artefacts, the software that powers it, and the vulnerabilities that were exploited. Strategic attribution requires investigating the attacker's geopolitical context, history, politics, and intelligence in order to assess the attacker's likely influence and sponsorship from hostile state actors (Rid & Buchanan, 2015). Because of the lack of clarity in the international legal structure governing responsible state behaviour in cyberspace, some states have developed national legal frameworks mandating the use of ACD.

Finally, the third group of factors pertains to political decisions to implement ACD in order to sovereignize the Internet, in the case of authoritarian regimes, or to employ it during cyberwars fought inside kinetic regimes, in the case of democratic governments fighting to resolve conflicts. In the first scenario, isolated authoritarian regimes employ ACD to asymmetrically challenge US hegemony (Ventre, 2012; Domańska, 2019). Since the US has hosted the Internet's physical infrastructure since its inception, it is assumed that it should be defended at all costs (Deibert 2008). However, several nations that the West has publicly chastised and sanctioned participate in disruptive activities in order to oppose what they perceive to be US hegemony in cyberspace (Ventre, 2012; Domańska, 2019). The second scenario involves territorial conflicts that drive certain states to use ACD. When one state claims the territory of another state, problems develop within the international system (Ebert & Maurer, 2013). Territorial disputes are one of the most telling evidence that competing states are rejecting the international order (Engli, 2020). Consequently, Israel has created an offensive strategy known as the 'campaign between the wars' approach, which signifies a continuous attempt to face potential opponents and reduce their ability to hurt Israel in the future conflict (Herpig, Morgus & Sheniak, 2020). Drawing on previous contributions, internalization of the ACD norm is therefore sensitive to the political goals pursued by both authoritarian and democratic regimes.

AGENTS OF CHANGE AND AGENTS OF RESISTANCE TO NORM CHANGE IN CYBERSECURITY

Although some states have made international efforts to implement cybersecurity approaches in terms of proactive and offensive means, others tend to defy this trend by employing their own approaches in terms of reactive and defensive measures, therefore, these actors can be classified based on a spectrum that includes four types of normative roles: norm entrepreneurs and competitor entrepreneurs, respectively norm antipreneurs and creative resisters.

ACD is a proactive and offensive cybersecurity approach that includes tools, techniques, tactics, and procedures, both technical and human in character, that are designed to fend off or defeat cyberthreats and sustain the existence of an open, free, secure, and stable cyberspace. Technically, ACD contains white worms (Lu, Xu & Yi, 2013), honeypots (Heckman et al., 2013), address hopping (Shi et al., 2007), canary traps, and hack-back capabilities (Kesan & Hayes, 2012; Rosenzweig, 2013). Various interpretations emerge when it comes to the extent to which states are permitted to hack back at the offenders. Three increasingly worse scenarios are shown here. The defender can participate in 'active threat neutralization' in the first one. This requires halting an ongoing attack in order to neutralize it without retaliating against the attacker (Kesan & Hayes, 2012). The second scenario presupposes that the attacker can be hacked back. This comprises infiltrating the attacker's network, scanning it, seeing how the systems interact, and even identifying prospective new targets (Dewar, 2017). The third and worst-case scenario authorizes some state actors to retaliate through 'forcible actions' in conformity with international law (Hathaway, 2014).

Nonetheless, certain nations continue to adhere to the PCD norm. Its range is separated into two categories: fortified cyber defense and resilient cyber defense (Dewar, 2014; Dewar, 2017). As Dewar (2014) states, constructing 'systemically secure communications and information networks in order to establish defensive perimeters around key assets and minimize intentional or unintentional incidents or damage' (p. 15) is part of fortified cyber defense. Further on, according to Dewar (2014), too, resilient cyber defense consists of 'ensuring the continuity of system functionality and service provision by constructing communications and information networks with the systemic, inbuilt ability to withstand or adapt to intentional or unintentional incidents' (p. 16). From a different perspective, PCD incorporates both a technological and a human component. It covers technological instruments such as data access controls and system access controls, as well as secure system designs and security administrations on the human side (Lehtinen, Russell & Gangemi Sr., 2006). Legally speaking, PCD does no harm because it only uses the defender's own network and systems (Sklerov, 2009).

This worldwide conflict in cybersecurity between agents of change and agents of resistance has influenced normative interactions between states according to Alan Bloomfield's norm entrepreneurs - norm antipreneurs continuum. Bloomfield (2015) states that norm entrepreneurs are those 'actors who promote new global norms' (p. 310). Pure norm entrepreneurs are states which are determined to making ACD an accepted and internalized norm, including its retaliatory, intrusive techniques (Himma & Dittrich, 2011; Hare, 2012; Hathaway, 2014). In the same gamut however, Bloomfield (2015) states that competitor entrepreneurs 'agree [that] change is necessary but [...] disagree on the content of the new norm' (p. 332). In the light of the current debate, competitor entrepreneurs argue that, given the controversy surrounding some of its aggressive measures, ACD should be adopted with certain constraints, limiting its usage solely within the defender's network and systems. These constraints typically advocate for restricting the employment of retaliatory and deterrent tactics against cyberattackers in order to minimize potential escalation into cyber arms races (Viganò, Loi & Yaghmaei 2020; Herpig 2021). At the other end of the spectrum, norm antipreneurs represent, according to Bloomfield (2015), 'actors who defend the entrenched normative status quo against challengers' (p. 321). Within the conflict between the two cybersecurity approaches, these are the states that continue to deploy PCD, drawing on the ongoing discussion about ACD and the efficiency of reactive measures in fighting cyberthreats (Chabinsky, 2013; Iasiello, 2014; McLaughlin, 2011). Finally, creative resisters come from the same normative community as pure norm antipreneurs, but they agree that some changes must be made to the normative status quo while still maintaining it because they have been persuaded by pure norm entrepreneurs or are simply being forced by the circumstances (Bloomfield, 2015). Between ACD and PCD, creative resisters continue to emphasize the latter's importance while accepting and implementing certain tools from the former's toolbox. Furthermore, legally and politically, the normative frameworks of creative resisters legitimize the use of PCD while permitting other actors to utilize lawful responses with some constraints (Moret & Pawlak, 2017; Bendiek, 2018).

METHODOLOGY

Because of the dominant nature of the discipline, the cybersecurity literature is polluted by a predisposition to experimentally explore only the most recent technological developments (Craigen, Diakun-Thibault & Purse, 2014). In comparison to computer science contributions, empirical investigation of political issues caused by the adoption and usage of these technologies is undervalued. This is also true in Romania, where the majority of contributions promote the country's role as a digital hub while very few discuss its cybersecurity regulations and processes. Romania was selected for a case study in this paper for three key reasons. The first is related to the literary contribution. Theoretically, the cybersecurity spectrum is characterized by ACD and PCD, however empirical contributions on governments utilizing these techniques have concentrated on significant participants in the international system such as the US, China, Russia, the United Kingdom, Germany, and Israel. As a result, Romania is left out of the equation. The second factor is Romania's position as a regional cybersecurity supplier. The third and last rationale is Romania's role as a norm agent in Central and Eastern Europe. Romania strives to maintain this benchmark because its most recent National Cyber Security Strategy (NCSS) and cybersecurity military, civil, and governance institutions place a higher priority on building the nation's resilience against cyberthreats rather than on creating ACD means.

Empirical evidence supporting this assertion was collected from two sources: the NCSS of Romania for the period 2022–2027 and the posts uploaded on the Facebook pages of three cybersecurity institutions: the National Cyberint Centre, the NCSD, and the RAISA. The NCSS of Romania 2.0 is divided into five sections, including an introduction, a vision for the years 2022–2027, guiding principles, goals, and definitions. Only the sections related to principles and goals are examined because the goal of this study is to explain Romania's position with regard to the two cybersecurity approaches. The selected Facebook posts have been compiled using the Facepager application programming interface (API) tool. The user is able to compile all the relevant information and metadata about social media public pages. The default 'get posts (v13.0)' preset has been used for this study in order to precisely gather the posts' content and creation time. Only two of the three aforementioned institutions have Facebook pages dedicated to them. The Romanian Intelligence Service (RIS) page is used by the National Cyberint Centre to advertise its activity. The dates when the Facebook pages were created and the date of 1 July 2022 were used for compiling all of the posts. Facebook pages for RIS, NCSD, and RAISA were established on 22 February 2013, 14 July 2011 and 22 March 2013, respectively. The NCSD does, however, make a methodological exception in this case. The posts` collection timeline was between 1 July 2022 and 27 September 2021, the date the Romanian government's decision to create the NCSD was officially announced. This is because it is the successor to the now-defunct CERT-RO, which had fewer activities and duties than the newly founded Directorate. In the first instance, a total of 1023 posts were gathered, but only 77 of them are applicable to the National Cyberint Centre because it shares a social media page with the RIS. In the second case, a total of 382 posts about the NCSD's activity were collected, and finally, in the case of the RAISA, a total of 92 posts were collected.

The posts were broken down into three categories of analyses - research, training, and dissemination - and analyzed using the quantitative-qualitative method of content analysis. The posts that discuss scientific contributions edited or published by the aforementioned organizations or by foreign academics and institutions fall under the research category. This category includes posts that discuss academic studies, books, journals, and reports. This one is significant because it both promotes international research and describes Romania's scientific accomplishments in the area of cybersecurity. On the one hand, the training category includes posts about courses, recommendations, and trainings, and also, conferences, thematic meetings, webinars, debates, cyber exercises, and collaboration platforms. Domestically, courses, recommendations, and trainings are designed to strengthen civil society's resilience to cyberthreats. Externally, those regional or international events are intended to bring together other allied states and train their cybersecurity teams and policymakers in order to face cyberspace challenges. Last but not least, the dissemination category includes posts about the heads and experts who manage these institutions' media appearances as well as weekly news about the most recent developments in cybersecurity trends and challenges. This one is crucial because it demonstrates how these actors inform and educate the general public about the intricate reality of cyberspace.

ROMANIA'S BEHAVIOUR AS A NORM ANTIPRENEUR IN CYBERSECURITY

Romania is a norm antipreneur in cybersecurity, promoting the PCD approach and cultivating its resilient cyber defense on multiple levels: technically, legally, and politically. This is due to the fact that, in its domestic policy, it lacks the capability to become a typical norm entrepreneur that enforces ACD, but is attempting to adapt to the new realities of cyberspace by constructing its resilient cyber defense on three main pillars: the strategic, institutional, and societal one. The NCSS of Romania for the years 2022–2027 serves as the strategic pillar and serves as the foundation for additional technical, legal, and political cybersecurity reforms that the government hopes to put into place in the future. This strategy is based on the actual cyberthreat landscape as well as on regional and international trends regarding cyberspace governance. All governmental and non-governmental organizations that ensure proper maintenance of the country's cybersecurity make up the institutional pillar. The National Cyberint Centre, the NCSD, and the RAISA are the only three of these actors that stand out from the rest in Romania, despite the fact that there are many of them. Last but not least, the societal pillar focuses on how Romania markets itself as a norm antipreneur to both domestic and foreign audiences, as it is shown by the Facebook posts of the aforementioned institutions.

The Strategic Pillar

The NCSS of Romania for the period 2022–2027 provides the strategic foundation for Romania's resilient cyber defense. Romania has created two significant cybersecurity strategies since 2013. Eight major guiding principles were envisioned in Romania's first national cybersecurity strategy: coordination, cooperation, efficiency, prioritization, dissemination, protection of values, assumption of responsibility, and network separation (Luiijf et al., 2013). The second one, which made significant improvements and additions to the first, is based on five guiding principles that are better suited to current concerns about the regulation of cyberspace:

- everyone involved in cybersecurity is responsible for it, including public authorities and institutions, private businesses, and individual citizens;
- cybersecurity is a prerequisite for the smooth operation of the state and society, the improvement of the competitiveness of the national economy, and the growth of national capabilities in R&D and innovation;
- an elaborate normative framework serves as the foundation for cybersecurity;
- cybersecurity is consolidated through pragmatic international cooperation;
- cybersecurity is ensured by maintaining an open, free, secure, and stable cyberspace and upholding the rule of law, along with the protection of individual liberties and personal information (Guvernul României, 2022:pp.13–15).

As a result, this Strategy outlines three key dimensions of Romania's strategic approach to cybersecurity: the technical, legal, and political one.

The NCSS of Romania 2.0 aims to improve the security and resilience of networks and systems on the technical side of the resilient cyber defense, as it is stated in the Strategy's first objective. The implementation and operationalization of adequate cybersecurity policies, including quality standards, technical investments, and human resource allocation, are required of public authorities and private actors in this sense. Therefore, six measures are intended to be used to achieve this goal. According to Guvernul României (2022), the first step entails putting in place cybersecurity policies and methods for responding to and being resilient to cyber incidents, such as recovery plans, procedures for testing and auditing the level of cybersecurity, and updates to critical infrastructure hardware and software. The development of national detection, investigation, and counteraction capabilities, particularly through public-private partnerships, constitutes the second measure. The third measure deals with the effective distribution of technical, financial, and human resources through investments in technology and individual preparation, including knowledge of cyberthreats, ICT development, and how to respond to cyberattacks or cyber incidents. The fourth measure involves creating a system for reporting cyber incidents. The fifth measure entails the development of mechanisms for standardization, conformity, and certification. The supply chain security measure is the sixth and final one (pp. 16-18).

On the legal front, according to Guvernul României (2022), the NCSS of Romania 2.0 is meant to establish a normative and institutional framework, as it is specified in the second goal to be achieved. This goal raises the need for the development and optimization of strategic, tactical, and operational cooperation formats among all the involved stakeholders, as well as the optimization of information-sharing between public and private actors, all in accordance with the upcoming normative and institutional updates. Normatively, Romania requires a framework that is aligned with other international cybersecurity regulations and is adapted to the evolution of ICT. This should be accomplished by updating the current legal regime and ensuring the implementation of domestic cooperation mechanisms and procedures. The Law on Cybersecurity and Defense, in particular, must be promulgated because it establishes the foundation for the organization and execution of cybersecurity and defense activities, as well as the cooperation mechanisms and the attributions of public authorities in this field, among other things. Furthermore, legal cybersecurity frameworks must be in accordance with international law and must include procedures for holding malicious actors accountable. Institutionally, Romania needs to strengthen the Cyber Security Operative Council (CSOC) and the NCSD. To coordinate the National Cyber Security System's activity and offer expertise to policymakers, the CSOC's priorities must be noticeably adjusted in the first scenario. In the second instance, the NCSD must accomplish the objectives outlined in its governing law and encourage collaboration models among civil society, businesses, and academia (pp. 19–21).

On the political front, according to Guvernul României (2022), the NCSS of Romania 2.0 identifies three main goals: a pragmatic public-private partnership, resilience through proactive approach and deterrence and Romania as an important actor within the framework of international cooperation.

The first goal calls for five main actions:

- public and cybersecurity awareness raising through programs for both public and private entities and for the civil society through information campaigns, brochures, dedicated websites, and cyber hygiene guides;
- cybersecurity educational programs through pre-academic, academic, and post-academic study programs;
- professional training programs for those working in the field within the Cyber Security Training Centre;
- the growth of the national cybersecurity industry;
- the development and consolidation of cybersecurity research and development.

The second goal entails the following set of measures: the development of computer emergency response teams (CERTs) and security operations centers (SOCs) for creating cybersecurity norms and procedures intended for all ICT operators, the organization of cybersecurity drills, and the development of proactive, reactive, and deterrent capabilities in accordance with international law of responsible state behaviour. Last but not least, the third goal includes four measures: Romania's role consolidation at the international level as a state actor promoting an open, free, secure, and stable cyberspace, Romania's role consolidation at the regional and bilateral levels within the EU, NATO, OSCE, and the Council of Europe, the consolidation of the role of cyber diplomacy, and the consolidation of the role of the regional expertise transfer capability (pp. 21–27).

The Institutional Pillar

Since the country's adherence to and integration into the Euro-Atlantic community, Romania's institutional architecture for cybersecurity has grown to be diverse and complex, serving as a significant indicator of the country's advancement in this area. Over time, a web of ministerial and subministerial organs has been established under the control of the Supreme Council of National Defense (SCND) for the development of policy and oversight. For example, the Ministry of Communications and Information Society (MCIS) is in charge of completing the tasks and activities outlined by the NCSS. Other subministerial bodies take part in this task as well. Through its Centre for Coordination of Critical Infrastructure Protection (CCCIP) and General Directorate for Communication and Information Technology (GDCIT), the Ministry of Internal Affairs (MIA) is responsible for a number of cybersecurity duties. The Romanian Armed Forces include the Directorate of Communications and Information Technology (DCIT) as well as the Command of Cybernetic Defense (CCD). Furthermore, in response to the evolution of the digital ecosystem and international regulations, the following CERTs have been established: the Romanian National Computer Security Incident Response Team (CERT-RO), the Military Computer Emergency Response Team (CERT-MIL) within the Ministry of National Defense (MoND), and the Special Telecommunication Service's (STS) Operational Response Centre for Security Incidents (CORIS-STS) (Crelier, 2020). Despite this intricate institutional structure, only three key players stand out at the national and international levels: the National Cyberint Centre of the Romanian Intelligence Service (RIS) on the military side, the NCSD on the civil side, and the RAISA on the governance side.

The SCND decided to create the National Cyberint Centre as a RIS entity in 2008, but it was not until 4 June 2015 that it was officially opened. Its objectives include spotting and averting cyberthreats as well as defending against, responding to, and managing the fallout from cyberattacks. Additionally, the center offers a platform for cooperation with similar NATO structures as well as a platform for collaboration with all institutions within the national security system with responsibilities related to cybersecurity and defense. In order to identify the legal beneficiaries and provide them with the information they need to manage cyber incidents and their effects on ICT systems while maintaining the proper operation of the country's critical infrastructure, it carries out these responsibilities by relating technical defense systems to intelligence capabilities. The National Cyberint Centre concentrates on four types of cybercriminals from the viewpoint of malicious actors posing a threat to Romania: states, cybercrime groups, extremist (hacktivist) groups, and terrorist organizations (Serviciul Român de Informații, 2015).

The NCSD, which was established in 2011 under the control of the MCIS, is Romania's primary civil computer emergency response team. Its initial official name was CERT-RO, but in 2021 its personnel and attributions were changed and adjusted to the new international standards for cybersecurity, leading to the name change to NCSD. It was set up as a government structure for cybersecurity research, development, and expertise. Additionally, it is in charge of preventing, analyzing, recognizing, and responding to cyber incidents. It also develops and disseminates public policies for the prevention and mitigation of instances that pose a threat to the nation's critical infrastructure. As a result, it serves as a national hub for similar structures. Furthermore, four policies and two services provide the framework for its operations. With regard to policies, the NCSD is empowered to respond to all types of incidents, to offer complete assistance based on the nature and seriousness of the incident, to cooperate, interact, and share information, as well as to communicate and identify the most effective techniques for secure information transfers. As services are concerned, the NCSD offers incident response services and proactive initiatives. The first category of services consists in: incident triage by investigating whether an incident really occurred, assessing and prioritizing the incident, and conducting an investigation; incident coordination by determining the involved organizations, contacting the involved organizations to investigate the incident and take the appropriate steps, facilitating contact to other parties which can help resolve the incident, and contacting or facilitating contact to appropriate law enforcement officials, if necessary; and incident resolution through technical assistance and analysis of compromised systems, support in restoring the affected systems and services to their previous status, and collecting statistics and evidence about incidents, that could be used for protection against future attacks. The second category of services includes auditing services, security incident records, and the coordination and upkeeping of educational and information events. Last but not least, as a civil institution for cybersecurity, it provides channels of communication for users to report malicious activities (Directoratul Național de Securitate Cibernetică, 2021).

On the governance side, the RAISA was established in 2012 as a project devoted to promoting information security. It is a professional, non-governmental, a politically non-partisan, and non-profit association. Its mission is to contribute to the development and dissemination of knowledge and technology in the field of information security by fostering research and education in this area. In this way, it brings together academics from prestigious universities and Romanian institutions, as well as PhD, MA, and BA candidates, and businesses in the IT sector. In other words, it aims to establish a community of stakeholders adhering to the following values: ongoing investment in their education, openness to new techniques for information security, participation in the fight against the phenomenon of cybercrime; focus on facts, and the pursuit of excellence. Therefore, it aims to: collaborate with the Romanian and foreign academic community to organize conferences, scientific seminars, and workshops to present the development and implementation of effective measures for improving information security; cooperate with research centers, associations and companies from Romania or abroad to organize information events in the field of information technology security; support activities and institutions that contribute to the development and implementation of information security measures; organize educational programs for personnel in the field of electronic information management; launch initiatives against cyberattacks and cybercrime; disseminate information on existing vulnerabilities and newly identified national and international threats; publish academic journals in the field of information security and cybercrime; coordinate and promote books, textbooks, articles and specialist works in the field of security and cybercrime; provide financial support for participation in conferences, scientific meetings, and workshops in this field; and award prizes, scholarships or grants to people with outstanding merits in the field of information security (Romanian Association for Information Security Assurance, 2012).

The Societal Pillar

The majority of societal actors, including businesses, people, and governments, must participate in the development of cyber resilience at all organizational levels. As a result, they are interconnected and choose the best cyber resilience strategies based on their values and preferences (Hausken, 2020). Due to the ownership of the nation's critical infrastructure by the private sector, this cooperation has over time resulted in complex public-private partnerships in the areas of intelligence, security, and resilience. Additionally, efforts to legislate and impose legal obligations to service providers as a means to improve state-level resilience have also resulted from this cooperation (Herrington & Aldrich, 2013). This approach aims to ensure that all four resilience phases—prepare, absorb, recover, and adapt—are completed (Hausken, 2020). Empirical evidence demonstrates that in the case of Romania, the three main institutional actors in cybersecurity also follow this path, both independently and jointly, by promoting and enacting the three main categories of public cyber resilience policies: research, training, and dissemination.

On the research front, all three organizations advertise in their Facebook posts both international studies and scholarly publications they have edited. Due to its military orientation, the National Cyberint Centre is the least likely to post about recently published contributions. There are only two posts mentioning studies related to cybersecurity on the Facebook page of RIS. The first one refers to an analysis that was presented at the CJS Mobile Security workshop about how Android-based mobile phones are more vulnerable to online threats like remote control malware. The second alerts readers to the release of a report on cybercrime in Romania in 2019 that was created by the RIS and the cybersecurity company Mandiant. However, the NCSD, a civil cybersecurity organization, is more enthusiastic about supporting both domestic and foreign research. Four posts on its Facebook page mention the following contributions: the publication of the book 'Keep your Information System Safe (KISS): Practical Steps for Implementation Best Practices and Legal Considerations' in conjunction with the ISACA Romania Chapter; the endorsement of the book 'Cybersecurity – Challenges and Perspectives in Education' under the auspices of RAISA; the distribution of the cyber awareness report of the European Union Agency for Cybersecurity in conjunction with the European Cybersecurity Month 2021; and a proper contribution of the Directorate with regard to the publication of the volume 'The Strategic Resilience of the European Union, Technology and Digital Fields Included: Future Scenarios and Romania's Contribution' volume. Last but not least, the RAISA published nine posts detailing its work in the area of cybersecurity research: three posts announce the publication of the 'Considerations on Challenges and Future Directions in Cybersecurity' and 'Cybersecurity: Challenges and Perspectives in Education' studies, two other posts invite readers to the official launch of the second book's Romanian translation, one post announces the publication of the International Journal of Information Security and Cybercrime, and three posts mention a call for papers for the ninth edition of the International Conference on Cybersecurity and Cybercrime (IC3).

The approach to training of the three aforementioned institutions has both a domestic and an international component. Internally, they offer trainings, recommendations, and courses to the civil society. The RIS, which operates under the auspices of the National Cyberint Centre, has 27 Facebook posts alerting the public about various cyber incidents like Wipbot/Epic, botnet attacks, and social engineering. It also has posts devoted to its Cyberint Newsletter and other threat intelligence reports. By contrast, the NCSD, as a civil institution, has 195 Facebook posts about software updates, courses, webinars, cyberattack awareness in relation to the conflict in Ukraine, vulnerability and threat awareness, and cybersecurity measures in various cyber incident scenarios. The 'cyber dictionary term of the day' posts, in which the organization explains technical cybersecurity concepts to a large audience, represent one particular type of NCSD content in the field of cyber education. Last but not least, the RAISA published 54 posts, the majority of which focused on training sessions and guides against cyberthreats and malicious actors that the Association has organized or developed. Externally, they highlight Romania's participation in or organization of national and international thematic meetings, webinars, conferences, debates, cyber exercises, and collaboration platforms. The National Cyberint Centre has posted 40 times on Facebook on RIS's participations in national, regional, and international events such as the 'Cyberintelligence', 'Cyberthreats', 'The Euro - Atlantic Security and the Security in the Cyberspace,' 'Cybersecurity - approach in Romania's national security plan' Conferences, the 'Regional Summit for Cybersecurity', the 'Cybersecurity in Romania' Congress, the 'European Cyber Championship 2015', the 'Cyber Coalition 2015' exercise, the 'European Cyber Security Championship 2016', the 'European

Cyber Security Championship 2017', the 'Cyber Coalition 2020' exercise, and the 'Cydex2021' war games. The NCSD published 141 posts about the hosting, participation, and awards obtained by Romanian cybersecurity teams at international and national events like those previously mentioned, while some of them were exclusively promoted on the Directorate's Facebook page, such as 'UNbreakable Romania', 'Cyber Europe 2020', 'EESTEC Olympics 10', 'Unbreakable Romania 2022' and 'Locked Shields 2022'. Along with these hackathons and cyber exercises, the Directorate has been very active in hosting webinars, conferences, and discussions about a variety of topics, including the Digital Europe Program, financial intelligence, the European Cybersecurity Skills Framework, the MIE-Digital Program, the NIS Directive's implementation in Romania, and others. Finally, the RAISA posted 29 times about national or international cybersecurity events such as the 'CyberCon Romania' International Conference, the 2021 Bucharest Summit: Cooperation for Development, the 'Lessons learned from cybersecurity experts. Perspectives from Romania and the United States of America' online event, the 'Digital Power. The Word in Action' Conference, and the International Conference on Cybersecurity and Cybercrime (IC3). By posting about its accolades in the framework of the Cyber Outstanding Security Performance Awards (Cyber OSPAs), it also describes its performance in the area of cyber resilience and awareness.

As dissemination is concerned, the three entities' primary responsibility is to stay in touch with the domestic civil society and inform it of relevant topics, such as recently identified malicious cyber operations, fresh Romanian cybersecurity reforms, and weekly press magazines containing articles on global cybersecurity. On this occasion, the National Cyberint Centre has posted seven times. These posts primarily refer to the RIS press releases and interviews with some of its leaders and experts on topics like the value of human resources in cybersecurity, how to combat financial crimes and other malwares, and details on the cloud infrastructure used by the Romanian government. The NCSD has posted 50 times about its media appearances, demonstrating that it has the strongest connection to civil society. These posts provide an overview of the goal of raising cyber awareness in partnership with national media outlets like Kanal D, ProTV, Digi24, Antena 3, or Radio Free Europe by informing users of potential cyberthreats that have been identified by the Directorate and its allies. Additionally, the NCSD published 40 posts intended to promote its weekly press magazines. Aiming to educate the general public about current trends, research, technicalities, national and international events, laws, and threats to cybersecurity, this type of context is unique to the Directorate. Finally, the RAISA did not publish any posts about media appearances, in contrast to the other two institutions.

CONCLUSION

In conclusion, building on the research question of this paper, this analysis explains that Romania behaves as a norm antipreneur in cybersecurity by continuing to focus on the PCD resilient cyber defense approach and rejecting the ACD norm that is emerging because it lacks the capacity to accept and internalize it as well as to put its technicalities, regulations, and policies into practice. The findings, which come from the National Cyberint Centre, the NCSD, and the RAISA, three key players in the field of cybersecurity, reveal that Romania places a higher priority on cyber resilience than on using proactive measures like white worms, honeypots, and even identifying and hacking back the offenders. This is due to the fact that resilient cyber defense, which has a broader meaning than the strictly technical one defined by Robert Dewar, is ensured in Romania by drawing on the strategic pillar represented by the NCSS of Romania 2.0, which, even though it recognizes other states' efforts to promote ACD, still believes PCD to be appropriate for the complex reality of cyberspace and the high level of cyberthreats' sophistication.

Romania may, nevertheless, evolve into a creative resister in the future, continuing to support the PCD approach while also acknowledging the need for some ACD means. This is based on the norm entrepreneur – norm antipreneur spectrum. In line with national and international law regarding responsible state behaviour in cyberspace, the NCSS of Romania 2.0 emphasizes the goal of developing offensive response capabilities in the future. While excluding interviews with policymakers and practitioners who might know anything about potential future national regulations and technological innovations related to Romania's adoption of ACD, this study is restricted to Facebook posts outlining how Romania domestically cultivates its resilient cyber defense and how it promotes it externally. Despite this, future research will concentrate on Romania's position as a potential creative resister or even as a norm entrepreneur promoting the currently widespread norm of cyber resilience.

REFERENCE LIST

Amoroso, E. (2011) *Cyber attacks: Protecting National Infrastructure*. Oxford, Burlington, Butterworth-Heinemann.

Assumpção, C. (2020) The Problem of Cyber Attribution Between States. *E-International Relations.* 1–6. https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/.

Bendiek, A. (2018) The EU as a force for peace in international cyber diplomacy. *SWP Comment. 19*. https://www.swp-berlin.org/en/publication/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy.

Bloomfield, A. (2015) Norm antipreneurs and theorising resistance to normative change. *Review of International Studies.* 42(2), 310–333. doi:10.1017/S026021051500025X.

Brenner, S.W. (2001) Is there such a thing as 'virtual crime'? *California Criminal Law review.* 4, 1–72.

Brenner, S.W. (2004) Distributed Security: Moving Away from Reactive Law Enforcement. *International Journal of Communications Law & Policy.* 9, 1–43.

Chabinsky, S. (2013) *Passive Cyber Defense: The Laws of Diminishing and Negative Returns.* https://acdemocracy.org/passive-cyber-defense-the-laws-of-diminishing-and-negative-returns/ [Accessed 23rd February 2021].

Cook, C. (2018) Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook. *Stanford Law & Policy Review.* 29(2), 205–236.

Cormac, R. & Aldrich, R.J. (2018) Grey is the new black: covert action and implausible deniability. *International Affairs.* 94(3), 477–494. doi:10.1093/ia/iiy067.

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review.* 4(10), 13–21. doi:10.22215/timreview835.

Crelier, A. (2020) Romania's National Cybersecurity and Defense Posture. Policy and Organizations. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-10-Romania.pdf [Accessed 15th June 2022].

Deibert, R.J. (2008) The geopolitics of internet control: censorship, sovereignty, and cyberspace. In: A. Chadwick & P. Howard (eds.). *Routledge Handbook of Internet Politics (1st ed.). London, UK, Routledge*. pp. 339–352. doi:10.4324/9780203962541-30.

Deibert, R.J. & Rohozinski, R. (2010) Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*. 4(1), 15–32. doi:10.1111/j.1749-5687.2009.00088.x.

Denning, D.E. (2014) Framework and Principles for Active Cyber Defense. Computers & Security. 40, 108–113. doi:10.1016/j.cose.2013.11.004.

Dewar, R.S. (2017) Active Cyber Defense. *Cyber Defence Trend Analysis.* https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/181743/Cyber-Reports-2017-03.pdf?sequence=1) [Accessed 15th April 2021].

Dewar, R.S. (2014) The "Triptych of Cyber Security": A Classification of Active Cyber Defence. In: P. Brangetto, M. Maybaum and J. Stinnisen (eds.). *2014 6th International Conference on Cyber Conflict, CyCon 2014, 3-6 June, 2014, Tallinn, Estonia*. NATO CCD COE Publications. pp. 7–21. doi:10.1080/09700160903354450.

Directoratul Național de Securitate Cibernetică (2021) *Legislație.* https://dnsc.ro/pagini/legislatie [Accessed 12th August 2022].

Domańska, M. (2019) Gagging Runet, silencing society. 'Sovereign' Internet in the Kremlin's political strategy. *OSW Commentary.* 313. https://www.osw.waw.pl/sites/default/files/commentary_313.pdf.

Ebert, H. & Maurer, T. (2013) Contested cyberspace and rising powers. *Third World Quarterly.* 34(6), 1054–1074. doi:10.1080/01436597.2013.802502.

Engli, W.F. (2020) *Factors Determining Cyber Strategy: the Differences Between Active and Passive Cyber Attacks.* Thesis in fulfilment of the thesis requirements for the degree of Master of Arts In Political Science, University of Waterloo.

Flowers, A. & Zeadally, S. (2014) US policy on active cyber defense. *Journal of Homeland Security and Emergency Management.* 11(2), 289–308. doi:10.1515/jhsem-2014-0021.

Glen, C.M. (2021) Norm Entrepreneurship in Global Cybersecurity. Politics and Policy. 49(5), 1121–1145. doi:10.1111/polp.12430.

Guvernul României (2022) *Hotărârea nr. 1321/2021 privind aprobarea Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027, precum şi a Planului de Acţiune pentru implementarea Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027.* https://www.cybercommand.ro/webroot/fileslib/upload/files/conducere/hotararea-nr-1321-2021-privind-aprobarea-strategiei-de-securitate-cibernetica-a-romaniei-pentru-perioada-2022-2027-precum-si-a-planului-de-actiune-pentru-implementarea-strategiei-de-securitate-ciberne%20(1).pdf [Accessed 10th May 2022].

Hare, F. (2012) The significance of attribution to cyberspace coercion: A political perspective. In: Czosseck, C., Ottis, R. and Ziolkowski K. (eds.) *Proceedings of the 2012 4th International Conference on Cyber Conflict (CYCON 2012), 5-8 June 2012, Tallinn, Estonia.* Tallinn, Estonia, NATO CCD COE Publications. pp. 125-139.

Hathaway, O.A. (2014) The drawbacks and dangers of active defense. In: P. Brangetto, M. Maybaum, & J. Stinnisen (eds.) *2014 International Conference on Cyber Conflict, CYCON.* Tallinn, Estonia, NATO CCD COE Publications. pp. 39–50. doi:10.1109/CYCON.2014.6916394.

Hausken, K. (2020) Cyber resilience in firms, organizations and societies. *Internet of Things.* 11, 1–9. doi:10.1016/j.iot.2020.100204.

Heckman, K.E., Walsh, M.J., Stech, F.J., Boyle, T.A.O., Dicato, S.R. & Herber, A.F. (2013) Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers & Security.* 37, 72–77.

Herpig, S. (2021) Active Cyber Defense Operations. An analysis supported by the Transatlantic Cyber Forum. https://www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf [Accessed: 10 February 2022].

Herpig, S., Morgus, R. & Sheniak, A. (2020) Active Cyber Defense - A comparative study on US, Israeli and German approaches. https://www.stiftung-nv.de/sites/default/files/active_cyber_defense-_a_comparative_study_on_us_israeli_and_german_approaches.pdf [Accessed 9th April 2021].

Herrington, L. & Aldrich, R. (2013) The future of cyber-resilience in an age of global complexity. *Politics.* 33(4), 299–310. doi:10.1111/1467-9256.12035.

Himma, K.E. & Dittrich, D. (2011) Active Response to Computer Intrusions. *SSRN Electronic Journal.* 664–681. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585. doi:10.2139/ssrn.790585.

Iasiello, E. (2014) Hacking Back: Not the Right Solution. Parameters. 44(3), 105–113. doi: 10.55540/0031-1723.2732.

Kesan, J.P. & Hayes, C.M. (2012) Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law & Technology.* 25(2), 429–543.

Lachow, I. (2013) *Active Cyber Defense: A Framework for Policymakers.* https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446 [Accessed 2nd February 2020].

Lehtinen, R., Russell, D. & Gangemi Sr., G.T. (2006) *Computer Security Basics* (2nd ed.). O'Reilly Media, Inc.

Locatelli, A. (2011) The Offense/Defense Balance in Cyberspace. *Strategic Studies.* 35(1), 1–10.

Lu, W., Xu, S. & Yi, X. (2013) Optimizing Active Cyber Defense. In: S.K. Das, C. Nita-Rotaru, & M. Kantarcioglu (eds.). *2013 International Conference on Decision and Game Theory for Security, GameSec 2013, 11-12 November, 2013, Fort Worth, Texas, USA.* Cham, Springer. pp. 206-225.

Luiijf, E., Besseling, K. & De Graaf, P. (2013) Nineteen national cyber security strategies. I*nternational Journal of Critical Infrastructures.* 9(1–2), 3–31. doi:10.1504/IJCIS.2013.051608.

Maurer, T. (2015) Cyber Proxies and the Crisis in Ukraine. In: Geers, K. (ed.) *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence, pp. 79-86.

McLaughlin, K.L. (2011) Cyber attack! Is a Counter Attack Warranted? *Information Security Journal: A Global Perspective.* 20(1), 58–64. doi:10.1080/19393555.2010.544705.

Moret, E. & Pawlak, P. (2017) *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime [Accessed 23rd February 2022].

Munish, P., Megan, F., Kyle, H., Dana, M., Suzel, S., Christensen, G., Pipps, N., Tony, P., Aaron, H. & Clare, B. (2019) *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar.* https://nsiteam.com/social/wp-content/uploads/2019/11/191119-AEP_Commodification-of-Cyber-Capabilities-Paper.pdf [Accessed 20th January 2020].

Nye, J.S.J. (2016) Deterrence and Dissuasion in Cyberspace. *International Security.* 41(3), 44–71. doi:10.1162/ISEC.

Pattison, J. (2020) From defence to offence: The ethics of private cybersecurity. *European Journal of International Security.* 5(2), 233–254. doi:10.1017/eis.2020.6.

Rid, T. (2013) *Cyber War Will Not Take Place* (1st ed.). New York, Oxford University Press.

Rid, T. & Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*. 38(1–2), 4–37. doi:10.1080/01402390.2014.977382.

Romanian Association for Information Security Assurance (2012) *RAISA Presentation.* https://www.raisa.org/ [Accessed 12th August 2022].

Rosenzweig, P. (2013) International Law and Private Actor Active Cyber Defensive Measures. *Stanford Journal of International Law.* 47, 1–13.

Schulzke, M. (2018) The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. *Perspectives on Politics.* 16(4), 954–968. doi:10.1017/S153759271800110X.

Serviciul Român de Informații (2015) *SRI inaugurează noul sediu al Centrului Naţional Cyberint, în prezența Președintelui României, domnul Klaus Iohannis.* 4 June 2015. https://www.sri.ro/articole/sri-inaugureaza-noul-sediu-al-centrului-national-cyberint-in-prezenta-presedintelui-romaniei-domnul-klaus-iohannis-04-06-2015-15-21 [Accessed 11th August 2022].

Shen, Y. (2016) Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review.* 1, 81–93. doi:10.1007/s41111-016-0002-6.

Shi, L., Jia, C., Lü, S. & Liu, Z. (2007) Port and Address Hopping for Active Cyber-Defense. In: C.C. Yang, D. Zeng, M. Chau, K. Chang, Q. Yang, X. Cheng, J. Wang, F.-Y. Wang, & H. Chen (eds.). *Intelligence and Security Informatics, Pacific Asia Workshop, PAISI 2007, 11-12 April 2007, Chengdu, China.* Berlin, Heidelberg, Springer. pp. 295-300.

Sklerov, M.J. (2009) *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent.* Thesis, in partial satisfaction of the requirements for the Degree of Master of Laws (LL.M.) in Military Law, Judge Advocate General's School, Charlottesville, Virginia, USA.

Tran, D. (2018) The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *Yale Journal of Law & Technology*. 20, 376–441. https://yjolt.org/law-attribution-rules-attributing-source-cyber-attack.

Turunen, M. & Kari, M.J. (2020) Cyber deterrence and Russia's active cyber defense. In: Eze, T., Speakman, L. & Omwubiko, C. (eds.) *Proceedings of the 19th European Conference on Information Warfare and Security, ECCWS 2020, 25-26 June, 2020, Virtual conference*. ACPIL. pp. 526-532. doi: 10.34190/EWS.20.038.

Vacca, J. (2014) *Network and System Security* (2nd ed.). Oxford, UK, Syngress Publishing, Inc.

Ventre, D. (2012) Cyber Conflict. Competing National Perspectives. London, Wile-ISTE Ltd. doi:10.1007/978-3-030-11795-5_76-1.

Viganò, E., Loi, M. & Yaghmaei, E. (2020) Cybersecurity of Critical Infrastructure. In: M. Christen, B. Gordijn, & M. Loi (eds.). *The Ethics of Cybersecurity.* London, UK, SpringerOpen, pp. 157-177. doi:10.1007/978-3-030-29053-5_8.

Virvilis, N. & Gritzalis, D. (2013) The big four - What we did wrong in advanced persistent threat detection? In: *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, 2-6 September, Regensburg, Germany.* IEEE. pp. 248-254. doi:10.1109/ARES.2013.32.

Wong, T.P. (2011) *Active Cyber Defense: Enhancing National Cyber Defense*. Thesis, Naval Postgraduate School, Monterey, California.

Yağlı, S. & Dal, S. (2014) Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures. *International Journal of Computer and Systems Engineering*. 8(4), 909–913.

Zheng, R., Lu, W. & Xu, S. (2015) Active Cyber Defense Dynamics Exhibiting Rich Phenomena. In: *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security, HotSoS '15, 21-22 April 2015, Urbana, Illinois, USA.* New York, NY, United States, Association for Computing Machinery. pp. 1-12.