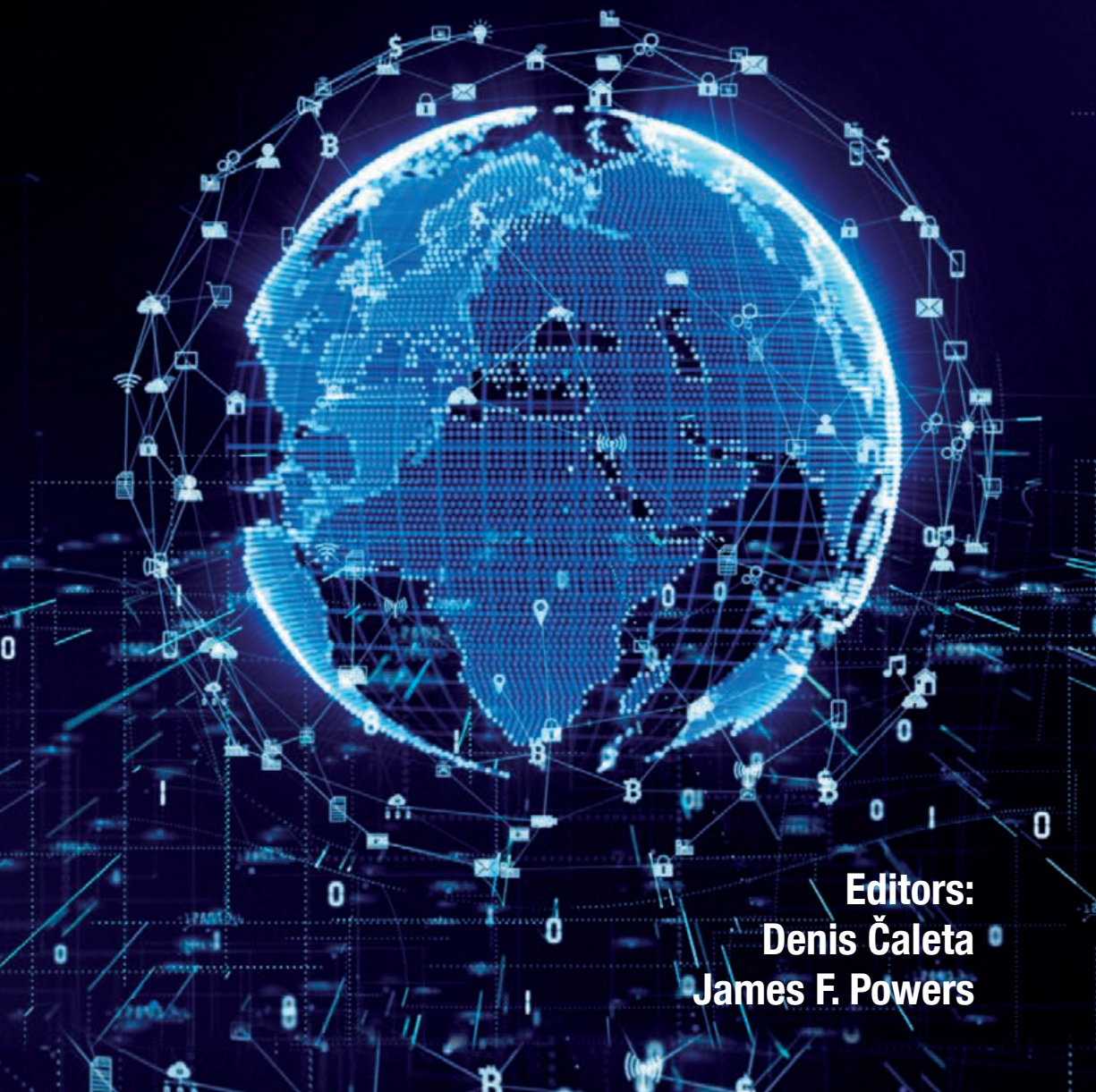
Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection



Editors:
Denis Čaleta
James F. Powers

Publishing of this publication was funded by the Regional Fellowship Program.

Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection

Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection

Editors: Denis Čaleta and James F. Powers Jr.

Ljubljana, September 2020

Colophon

Editorial: Denis Čaleta, Ministry of Defense Republic of Slovenia and James F. Powers Jr., Joint Special Operations University from Tampa

Reviewers: Oliver Bakreski, Brane Bertoncelj, Aljoša Kandžič, Arnold Kammel, Atanas Kozarev, Žiga Podgoršek, Milan Tarman, Dragan Trivan, Jaka Vadnjal, Milan Vršec, Miran Vršec, Žiga Podgoršek

Publisher: Ministry of Defense Republic of Slovenia, Slovenia, Joint Special Operations University from Tampa, USA and Institute for Corporative Security Studies, Ljubljana, Slovenia

Translation: School of Foreign Language, Ministry of Defense

Proofreading: School of Foreign Language, Ministry of Defense

Design & Graphic: Gra Pha Co and Institute for Corporative Security studies

Print: In Slovenia

Edition: E-edition

Location: https://dk.mors.si

Email address of Editor: denis.caleta@ics-institut.si

Note: The authors opinions expressed in this book do not necessary reflect the views of the institution in which they are employed.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID=31817219

ISBN 978-961-94444-8-1 (Ministrstvo za obrambo, pdf)

ISBN 978-961-94011-2-5 (Inštitut za korporativne varnostne študije, pdf)

Contents

Editorial

Denis Čaleta

The complexity of the security environment confronts us constantly with important dilemmas about the effectiveness of our risk management operations. The global security environment is becoming more complex than ever before. In addition to traditional national and international actors, who have had a major impact on the regulation of geo-political relationships in the international security environment until recently, non-state entities have been arriving on the scene. They have gained special importance in terrorism, one of the most significant security threats at the beginning of the 21st century, and present a threat to undisturbed functioning of the wider social community. However, terrorism has not been the only serious security risk recently. We have witnessed a whole range of complex security threats posed by constant migration pressure to the external EU borders and, consequently, the adoption of more restrictive border measures at the Schengen border, as well as cyber risks and large-scale hacker attacks, a wide range of risks facing commercial organizations, coronavirus pandemic, and geopolitical shifts we experience almost daily and present us with the constantly changing dynamic of a stable security environment we were accustomed to in the past. Because of all this, the professional public is confronting dilemmas about seeking appropriate responses to the changed security trends.

However, an in-depth analysis of risk factors facing democratic societies in Europe quickly reveals that threats are not only linked to external factors, but are, particularly major ones, also found within democratic social communities themselves. Even a superficial analysis of terrorist acts committed over the last 15 years in Europe shows that most acts were carried out by citizens of European countries, who had, on the basis of their political, religious and other views, radicalized to the extent that they were prepared to enforce their views by committing terrorist acts. In addition to casualties, which were certainly a tragic product of these processes, Western democratic societies were shaken by the realization that, sociologically speaking, they were left without any suitable answers about to how it was possible for individuals in such environments to become so radicalized as to be willing to risk their own lives and harm fellow citizens on account of their beliefs. The approach taken after 11 September 2001, when excessive attention was focused on strengthening security mechanisms in the intelligence and security field, indicated with every subsequent terrorist act that these measures were ineffective in and of themselves, and failed to produce desired results in relation to financial and other resources used. Sociological processes taking place in democratic societies which are increas-

ingly reflected in the marginalization of certain social groups, increased stratification and, in some cases, segregation, and consumerism as a value which has superseded all other values and alienated individuals of the community, are only a few of the negative factors directly contributing to a favorable environment for radicalization. Our societies will have to change their awareness of the importance of appropriate coordination for the effectiveness of the system of countering terrorism. All of the above factors and challenges gain an additional dimension and importance when seen through the prism of the regional perspective of terrorism suppression. In the field of preventing radicalization and extremism, a specific role has now moved to the institutions of the society which were formerly not directly regarded as active actors of countering terrorism. The educational system, social services, religious communities, non-governmental organizations and a whole range of civil society movements have become crucial in the process of perceiving radicalization factors in individual persons. All these segments of society must, together with national security authorities, form a comprehensive and an effectively functioning system of identification and prevention of processes that lead to extremism and radicalization of individuals or groups.

When the informatization and digitalization of society are added to the discourse, it can be stated with certainty that the functioning of society, in addition to other problems, has become heavily dependent on new technological solutions. On the one hand, they enable the virtuality of interpersonal relationships which is based on the internet and all existing social networks. On the other hand, technical solutions are one of the means enabling radicalization processes in groups and individuals. The functioning of a modern society also requires the provision of basic infrastructural capabilities, which are defined as critical infrastructure. They are divided into a range of sub-sectors, of which the provision of electricity and information and communication technologies are of central importance, since their co-dependent functioning affects all other sub-sectors and has a special significance for the functioning of a wider social community. This is the reason why the cyber security has important role in protection of critical infrastructure.

If modern security threats posed by international terrorism and associated radicalization of individuals or groups are indeed as complex as content of this publication describes, it is justified to ask several questions, such as: what can a modern state do for its national security system to respond quickly and effectively to terrorist threats; how should the national counter-terrorism system be structured; what roles and powers do security authorities of individual states have within this system; and, especially, are security and other state institutions appropriately organizationally structured, prepared and equipped to be capable of carrying out the activities of countering threats, such as terrorism. Without a stable and well-functioning system of public-private partnership, whose processes include corporate security of organizations managing critical infrastructure, it will be very difficult to prevent radicalization processes in these organizational environments.

The aim of this publication is to find answers to some of the above questions. The combination of different approaches, concepts and analyses of different cases, as well as the role of national security entities in countering terrorism, provide specific solutions to the majority of the issues including cyber security and critical infrastructure protection, which, however, does not exclude further scientific and professional considerations.

Ljubljana, September 2020
Denis Čaleta, PhD

James F. Powers Jr.

Following the 9/11 terrorist attacks on American soil, the US Government transformed the existing 1960's emergency management protocols and created a new methodology for thinking like our adversaries—what assets (targets) are critical and likely to influence or damage national political objectives and thus cause psychological fear and embarrassment. Physical barriers to protect critical infrastructures are not only expensive, but also flawed. Never will any public- or private-sector owner of critical infrastructure have sufficient resources to protect every designated site. The focus on protection from external physical intrusions should now shift to internal cyber protection measures—personnel surety and Red Teaming.

A post-9/11 Approach: Empowered with a plethora of legislation, President George W. Bush issued a series of executive orders and directives to frame how America would proceed in identifying and protecting America's critical infrastructures. His vision was clear, succinct and unambiguous: Focus not only on potential terrorist attacks, but rather on any hazard that might damage, destroy or otherwise incapacitate America's critical infrastructures. The Rationale: regardless of the cause of incapacitation, the consequences will be the same.

Bush's vision resulted in today's All-Hazards Approach—terrorist attacks, major disasters, and other emergencies. This approach leads planners to consider myriad factors—designating and grouping infrastructures by sector, historical analysis of the most-likely scenarios impacting infrastructures, emerging intelligence threats, available resources, prioritization of infrastructures, ownership (public- and private-sector) of infrastructures, criticality criteria, stakeholders associated with infrastructures, existing vulnerabilities of infrastructures, consequences associated with damage or destruction of infrastructures, available resources and overall risk management. The Intent: apply the available resources to the most-likely threat.

The result of this approach produced the US National Infrastructure Protection Plan. The current plan (2013) designates 16 sectors; the Information Technology Sector is orchestrated by the Department of Homeland Security. For cyber-specific issues, the newly created

(2018) Cybersecurity and Infrastructure Security Agency has responsibility to coordinate efforts from the federal government level to the local level—and includes owners/operators and all stakeholders.

Since sufficient resources to physically protect critical infrastructures will never be available, the imperative to ensure due diligence in appropriating federal, state, local and private-sector funds for protection efforts is paramount. Today's protection efforts are multidimensional—not simply armed guards and barriers protecting a building or system. Protection efforts are characterized and prioritized by human, physical & cyber considerations; the National Planning Scenarios; determination of criticality; intelligence; and risk (stated as a function of threats, vulnerabilities and consequences). Moreover, it is a dynamic rather than a passive process—what is critical today may not be critical tomorrow. And intelligence informs all stakeholders of emerging concerns. The factors and considerations previously-mentioned are interlinked like a watchwork. When one factor changes, the others are impacted to some degree.

Considering what practitioners have learned since 9/11, here's where the focus should be:
1. Historically-based (national planning scenarios) versus crime-related (this includes terrorism) threats. For example, cyber-systems are much more vulnerable to weather and natural disasters than to terrorist threats.
2. Monitoring of cyber intrusion attempts and determining origin for possible prosecution.
3. Developing threat-based cyber capabilities to detect, deter, mitigate, respond to and recover from cyber intrusions
4. Investing in personnel surety versus software. Aside from personnel costs, the second largest expenditure for most companies is information technology. It's time to re-evaluate the expenditures for physical protection versus the costs required for personal surety. Why? It's easier to gain access to a cyber system via someone on the inside than hire a cyberhacker to break into the system. Background checks must become more comprehensive—and this may include periodic and unannounced polygraph tests, drug testing, and personal financial reviews. The weakness of any cyber system lies not in the software, but in the integrity of those operating the system. Owners/operators of CI should establish Red Teams—teams of company-owned, experienced cyberhackers—whose sole mission is to hack into the company's systems. The intent here is to hire better hackers than the adversary.

Nation-states will forever endure extremist and radical ideologies—and these labels are all culture-based. Disagreement in beliefs and ideologies does not necessarily constitute criminal motivation or likelihood of criminal behavior. When actions of any group—ideology notwithstanding—become violent and break the laws of that sovereign nation-state, then those acts, however, constitute criminal behavior.

It is unlikely that any nation-state permits identification theft, cyber hacking, cyber intrusions, etc. Whether these violations are considered as violent is a matter for the particular nation-state. Many Americans do not consider cybercrime violent but rather something less than violent—a white collar crime—but a crime, nonetheless.

As threats increase, so should protection efforts. And the greater the assets, the greater the need for cybersecurity systems. The very nature of being designated critical usually infers that the site has vast assets—and an information technology system to help facilitate opera-

tions. Thus, the larger and more critical the asset, the likely degree of dependence on information technology—and thus the greater degree of risk from cyber-hackers.

The three protection priorities—human, physical and cyber—can be dealt with individually to identify and reduce vulnerabilities and consequences. Physical measures such as barriers, ballistic curtains, bollards, armed guards, etc. are easy, albeit expensive methods for protecting human and physical assets. However, cyber protection has as many solutions as the number of experts discussing it.

Since 9/11 and the ever-expanding capabilities of today's cyber world, damage and destruction efforts are focusing more on cyber-attacks than physical attacks—particularly if the site depends on and shares data with a large number of stakeholders. What this portends for owners and stakeholders is a more internal versus external focus on protection—the personnel having access to the cyber systems that support and facilitate day-to-day operations. Respect the capabilities of potential adversaries. Strengthen personal surety and Red Team systems—physical measures are limited.

Tampa, September 2020
James F. Powers Jr.

Section I.

Extremism, Radicalization and Cyber Threats as an Important Security Factors for Countering Terrorism Processes

1 Re-assessing Online Jihadi Extremism: Reasoning for a Marketing Approach to Counter-Radicalization

Paul S. Lieber

1 Introduction

The recognition that the lifeblood of European jihadi violent extremism resides in online domains is anything but a new concept. For over a decade, Al-Qaeda and subsequently ISIS have displayed a seemingly omnipresent global reach, one empowered through social media based tools (Lieber & Reiley, 2019). These tools remain incredibly adept at the recruitment and sustainment of devotees, and are also quick and clever at dancing around attempts to reduce both access to and effectiveness of extremist communication.

While the physical structures and geographic footholds of jihadi extremist groups have considerably diminished, this has not been mirrored online (Brzuszkiewicz 2017). The likelihood of extremist splinter cells fomenting, the re-emergence of terrorist groups as new entities, and/or the emergence of a new threat organization entirely all remain real problems for European nations. Moreover, the influx of returning foreign fighters and/or advocates from warzones only compounds this potential. Disgruntled, potentially excommunicated, and with unstable support systems, these oftentimes military-capable individuals are simply waiting for a call to action to re-engage, but now on their home soil against a 'far enemy' (Brzuszkiewicz, 2018). Brzuszkiewicz posited that the current ISIS strategy is now a deliberately homegrown effort: "ISIS propaganda has gradually evolved towards more insistent exhortations for its supporters to stay where they are and fight the kuffār (infidels) where it hurts the most – that is, in their own countries." Due to close border proximity, this creates a realistic threat potential spanning the entire European continent.

Greater threat awareness has led to increased pressure on European nations from their constituents to respond to jihadi online extremist group communication (Meleagrou-Hitchens, 2017). Still, there remains miniscule evidence of the effectiveness of counter-messaging within Europe, if at all (McCants, 2015). Compounding this problem is that even when gains are made, it is near-impossible to tether success to a particular action or intervention (Briggs

& Feve, 2013). Perhaps Melagrou-Hitchens (2017) put it best, in "proving that any specific such measure directly contributed to someone not becoming a terrorist, which in other words is attempting to prove a negative, is patently impossible."

2 Extremist Social Networks

Corresponding to the strategic shift of the extremists, the majority of European counter-extremism resources are now directed towards a better understanding of the online domain (Melagrou-Hitchens, 2017). Social network analysis remains a preferred online assessment tool, even more so when it has the necessary global focus. By assessing who speaks to whom and how frequently, social network analyses can semi-independently identify leadership roles within a Jihadist organization's communication structure (Lieber & Lieber, 2017). Combined with textual analysis (from social media sites) mapped to these same individuals, uncovered patterns and trends can also comfortably label the resonance of particular ideas within a social network. This is an integral part of identifying burgeoning threats and grievances, as tracking individuals and ideas in tandem can better isolate and rank preferred geographic attack locations.

Moreover, a closer look at social network ideas can also elucidate how specific concepts are framed around particular themes. This framing data becomes a helpful guide in gauging public sentiment for/against established governance and/or alternative power structures (that threat networks reside in). Mass media, in most instances, will follow suit, or vice-versa. Mass communication theory refers to this phenomenon as second and third level agenda setting theory. These theories reason that mass media determines which issues are most salient (agenda setting theory), also how audiences should reason about such items (second level agenda setting theory), and finally which issues should be linked together (third level agenda setting theory) (McCombs et al., 2012).

3 Grievances

As grievances do not emerge in a vacuum, this is an especially salient point in understanding the motivations for violent jihadi extremist groups within Europe. These groups form, sustain, and grow on foundations of actual and perceived grievances. Their ability to recruit is a product of: a) the seeming legitimacy of such grievances, and b) a willingness by others to declare them as legitimate.

Brzuszkiewicz (2018) divided European extremist grievances into two categories. The first she described as 'a narrative of self-pity,' of unfair injustices Muslims the world over face (including in primarily Muslim countries). Savary and Dhar (2020) discovered that individuals struggling with concepts of self are more likely to stay loyal to [even] a [destructive] premise, especially concepts foundational to self- identity. Perhaps not surprisingly, these same individuals are also less likely to accept a new [and potentially helpful] premise that deviates from their established self-identity.

The second extremist grievance category was one Brzuszkiewicz (2018) saw as a desire for 'empowerment' and 'redemption'. Specifically – and for violent extremists – a longing for

religious pardon of terrorism act sins. This second grievance is perhaps most salient for those who – on returning to Europe from warzones– now find themselves marginalized and in prison environments.

Social network analysis – for all of its potential – does not directly consider grievances in its structure equation modelling calculations about violent extremist networks1. Even when grievance-associated themes and frames are linked to such assessments (via textual analysis), they are only considered as a mathematical sorting of ideas and individuals based on their frequency and likelihood of connection. Thus, while they are useful data points, there is no way to validate such online patterns as representative of a violent extremist population (notably offline) writ large. Even the best social network analysis data of jihadi extremists (captured over longer periods of time and featuring abundant data points) is not fully predictive or even indicative of offline interactions.

What contextual focus exists in the current battle against online jihadi violent extremism lies in countering extremist narratives. This approach is derived from a presupposition that grievances can be satiated or reframed by offering prosocial alternatives housed within a competing message. Not only does this subscribe to long-dismissed mass communication inoculation theory, that messages – upon receipt – are automatically infused and adopted within a population's core belief systems (McGuire, 1961), it also assumes a population keen to consider duelling aspects of the said grievances from which to form ultimate, reasoned opinions. Lastly, there remains limited attempts to synchronize counter-narrative efforts with those on the ground, the latter essential reinforcement criteria in establishing the legitimacy of all intervention activities (Reed, 2018).

4 Counter-Extremism Policy

Policy efforts to address European violent extremism suffer from similar maladies. Despite an abundance of statutes clearly recognizing a global online extremist issue, most European policies – unintentionally or otherwise – do not require joint solutions either within a country or across the region (Hussain & Saltman, 2014).

Also – and in an effort to best address online violent extremism – an array of newer governmental organizations emerged with seeming expertise in influence and cyber nuances. With more manpower, however, comes an increased risk of both task redundancy and strategic disconnect. Thus, there is a glaring need to formulate more inter-departmental coordination mechanisms, and an incentive (and forcing function) for individuals to work together towards common solutions. This mindset, however, needs to overcome a multitude of authority-based roadblocks, as well as disclosure restrictions for when partner nations are factored in.

Jihadi extremist groups are well aware of these paradigms and shortcomings. Notably, counter-extremism efforts pre-suppose threats from larger scale, well-funded and globally connected individuals. There exists a very real possibility that European violent extremists will instead turn to low-cost, poorly planned, and terrorist acts below the planning threshold. This

[1] Structure equation modelling is an advanced statistical technique where pathways of prediction are indicated by numerical confidence. For social networks, it would be the confidence one has in a node (e.g. an individual person) within a network to engage with another as part of the said network.

may explain the rise in European knife attacks, as well as those using vehicles to run over pedestrians (Brzuszkiewicz, 2018).

Similarly, diplomatic channels provide invaluable sounding boards for the potency of interventions on audiences abroad, and individuals outside domestic boundaries but potentially shaping attitudes and opinions of those ripe for terrorist group recruitment at home. These channels, however, are also limited in their ability to extend findings beyond a small circle.

Looking wider, threat finance trends serve as important benchmarks for the potential of action and organizational legitimacy, as does an increase/decrease in incidents of contact or related activities within a social network of analysis. Once more, even these finance-based data points are – at best – correlated to extremist potential, not action.

Critiques of the above are not intended to discredit efforts, but rather to highlight a glaring oversight in current approaches. Despite a seeming abundance of resources, interest and collected data intended to tackle the jihadi violent extremism problem in Europe, the continent remains wedded to solutions founded in data points and/or counter-narratives. Europe is anything but alone in this mindset; machine learning and artificial intelligence expenditure across the globe is rapidly on the rise (Columbus, 2019). For this problem, this expenditure, by increasing computational power, is intended to maximize data prediction towards lowering future violent extremist instances and the associated risks. In doing so, however, they also ignore what lies behind the numbers. Bigger and faster does not equate to better or smarter.

5 Marketing Counter-Radicalization

Marketing researchers continue to explore ways to best create and disseminate persuasive message campaigns capable of eliciting the strongest attitudes and opinions about products, services and ideas in niche audiences. The internet, of course, has only increased the potential of marketing campaigns. Nearly every form of online interaction and communication is now tracked, mapped, and sorted into assessable audience and individual patterns.

Despite countless everyday instances of marketing campaign success, there is surprisingly limited, if any, application of these concepts to counter-radicalization. This is a glaring oversight, as jihadi extremists – if Brzuszkiewicz' (2018) explanation of a two-pronged grievance schema is an accurate picture of the sentiment landscape – should be prime candidates for marketing-driven campaigns emphasizing non-violent alternatives.

5.1 Nets for Trust

For example, in their analysis of the Ukranian banking industry, Kuznetsova et al. (2019) devised a four-stage marketing model to address the Ukranian population's lack of trust in this sector. The model – which they termed 'nets for trust' – is based on principles derived from the 'boiling frog effect' (Hoffman, 2003) which, as its name suggests, describes how to successfully boil a living frog. If the frog is suddenly placed into boiling water, it will immediately jump out, due to the extreme temperature contrast. If this same frog is placed in tepid water slowly brought to a boil, it instead fails to see the inherent danger, and ultimately will be cooked to death. Through an extremist lens, this effect highlights the fallacy of dramatic

counter-narrative approaches to combating online violent extremism, and instead reasons for a gradual change to a knowledge environment, one capable of more subtle achievement of the intended goals.

Kuznetsova et al.'s (2019) 'nets for trust' model expands the boiling frog effect into four stages. The first stage, 'preparing the nets', sees 'anger and mistrust' as core sentiments in a distrustful population, including a lack of faith in formal governance structures. This stage also reasons that, due to this strong anger and mistrust, individuals would be eager and willing to engage in discussions about their dissatisfactions at the earliest opportunity. For extremists, this may be evidenced via in a rise in online interactions with peers.

The second stage, 'throwing the nets', is a 'what if?' focus on uncertainty and lostness. Impacted individuals begin to question whether their prior stage sentiments are fully justified. This would be an anticipated form of reasoning for foreign fighters returning to a host country, and now with competing identities.

The third stage, 'dropping a lure' or 'adoption', would now find disenfranchised individuals more regularly engaging with the world around them. In contrast to purely radicalized views, extremists may begin to accept more of their former nationalistic identity, and become more active members of society. Still, and despite this increased participation, distrust is evident. This stage, according to the model, is the make or break point. Individuals will either progress to integrating their identities and away from an extremist mindset, or find the conflict too high a hurdle to overcome. (They would then fall back into the prior two stages.) The fourth and final stage, 'pulling out the fish' or 'proponent', would be the adoption of a more peaceful identity, devoid of tendencies towards radicalization.

Using the 'nets for trust' model as an example, counter-radicalization efforts could be segmented into four stages of intervention. Supporting assessment criteria would evaluate transitions across the stages, and also areas of weakness of opportunities. Social network analysis data could point to the (non-)effectiveness of efforts by shifts in social and communication structures at different stages of the model.

5.2 Customer Relationship Management

Along a different vein but arguably just as applicable to counter-radicalization, Kaur (2019) proposed a new approach to marketing (of business degrees), emphasizing a customer relationship management focus. Kaur called for 'customized personalization' versus 'mass customization' in marketing message techniques, and, by doing so, sought to foster more meaningful and sustained interactions with audiences. This would empower candidates to overtly question justifications and motivations for the degree selection decision, and also to shape degree experience to fit initial decisions.

While Kaur's model was designed to increase enrolment and retention, it features strong potential if considered in a counter-radicalization context. At present, nearly all counter-radicalization efforts focus on mainstream counter-arguments. This allows alternatives to emerge, but does so in a universal, black versus white, all or nothing context. Resonance increases reach, but not necessarily effectiveness.

Adopting a customer relationship model to counter-radicalization campaigns instead encourages impacted individuals to internally examine the principles most important to them, which may or may not include jihadism. By widening the lens to focus on 'why', as against 'what,' the conversation becomes more personal, rather than ideological. There is, of course, no guarantee that better clarity on intent will produce fundamental shifts in one's alignment with a jihadi mindset. At the least, however, it could encourage vulnerable individuals to explore a wider spectrum of wants/needs and with it increased potential for a more positive path.

Similarly, survey and focus group data collection about violent extremism can adopt a customer relationship driven model in devising questions and discussion frames. Exploring the motivations and reasoning strategies behind extremist thinking can yield more accessible ways to reduce its potency. Data collection can also serve as a subtle, additional interaction primer to encourage vulnerable populations to consider a different approach to reasoning about violent extremism.

5.3 Communication-Based Marketing

A third way to reconsider counter-radicalization messaging is to shift the emphasis entirely from a persuasive to a communication-based marketing model. Duncan and Moriarty (1998) reasoned that the modern era of communication places interactivity at a premium, and marketers should adjust their efforts accordingly. Also, it should be remembered that every form of communication has the potential to strengthen or weaken relationships.

Several shifts would be required to carry out this more interactive approach. Firstly, target audiences should be perceived not as recipients but as stakeholders. Secondly, as part of this alternative approach, known, formal mechanisms for stakeholders to meaningfully communicate back and forth with communicators must be available. Thirdly, communication efforts must be cross-functional, i.e. they should purposefully include other trusted entities with a vested interest in access to these same stakeholders.

From a counter-radicalization perspective, this would be a potentially dramatic shift. Similarly to Kaur's (2019) marketing model rooted in customer relationships, a communication-based marketing approach would emphasize back and forth interaction rather than persuasive messaging as a primary purpose. It would also require other organizations – including religious ones – tied to stakeholders to serve as active participants in the communication process. Daouda et al. (2020) highlighted the potency of such endogenous communication channels to engender mass credibility and wider acceptance.

Still, much like the customer relationship management premise (focused on 'why'), there is no guarantee that increased interactivity will lead to a more prosocial attitude and opinion change about radicalization. It could, however, establish increased venues to encourage and discuss such change, and assessment opportunity potential stemming from these new venues. Related, increased interaction can reduce perceived injunctive norm barriers, or the extent to which people feel pressured to engage, or not engage, in a particular behaviour (Lim et al., 2018) – in this instance, to reduce violent extremist affiliations and action.

6 Conclusion

While these are but three examples, the 'nets for trust' (Kuznestova et al., 2019), customer relationship management (Duncan & Moriarty, 1998) and communication-based marketing (Kaur, 2019) models all provide validated and alternative approaches to reasoning and addressing violent extremism in Europe. Current counter-radicalization paradigms, while data-based, sorely require more contextual foundations to both resonate with audiences and to create longer-term effects.

Violent extremist organizations, with the strongest ideological resonance and reach, will continue to rely upon these assets to further their causes. It is therefore imperative for current counter-radicalization mindsets to accept this reality, to adjust thinking, policy and expenditure accordingly, and, in doing so, to accept the limitations of existing approaches, and to consider ways to better infuse partners and mechanisms to buoy efforts. At a minimum, there should be acknowledgement that there are untapped avenues to explore in addressing the problem.

7 References

1. Briggs, R. & Feve, S. (2013). *Review of Programs to Counter Narratives of Violent Extremism, Institute for Strategic Dialogue*, Institute for Strategic Dialogue London, https://apo.org.au/sites/default/files/resource-files/2013/12/apo-nid37101-1211651.pdf, Accessed 20 February 2020.
2. Brzuszkiewicz, S. (2018). Radicalisation in Europe after the fall of Islamic State: Trends and risks, *European View*, 17(2): pp 145-154.
3. Brzuszkiewicz, S. (2017). *Is the Islamic State likely to return to the al-Qaeda model?* Al-Mesbar Studies and Research Center, 15 November. http://mesbar.org/islamic-state-likely-return-al-qaeda-model/. Accessed 20 February 2020.
4. Columbus, L. (2019). *State Of AI And Machine Learning In 2019*, Forbes.com. https://www.forbes.com/sites/louiscolumbus/2019/09/08/state-of-ai-and-machine-learning-in-2019/#be9ef181a8d0, Accessed 20 February 2020.
5. Daouda, F.B.; Barth, P. & Ingenbleek, P.T. (2020). Market Development for African Endogenous Products, *Journal of Macromarketing*, 40(1): pp 13-30.
6. Duncan, T. & Moriarty S. E. (1998). A Communication-Based Marketing Model for Managing Relationships, *Journal of Marketing*, 62(2): pp 1-13.
7. Hussain, G. & Saltman, E.M. (2014). *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it.* London: Quilliam.
8. Hoffman, R. R., & Hanes, L. F. (2003). The boiled frog problem [knowledge management]. *IEEE Intelligent Systems*, 18(4): pp 68-71.
9. Kaur, G. (2019). Is obsession with data and analytics making future marketers analytical researchers? A conceptual customer relationship marketing model for customized marketing education, *Journal of Education for Business*, 94(8): pp 569-575.
10. Kuznetsova, S.; Kuznetsov, K. & Kuznetsov A. (2019). How to Increase Public Confidence in Understanding and Use of the Banking System: Marketing Model 'Nets for Trust,' *Financial & Credit Activity: Problems of Theory & Practice*, 2(29): pp 13-20.

11. Lieber, P.S. & Lieber, Y. D. (2017). *Re-conceptualizing Radicalized Groups and their Messages*. Joint Special Operations University Press.

12. Lieber, P.S. & Reiley P. J. (2019). Psychological Operations to Counter Online Radicalization, in C. Marsh, J. Kiras & P. Blocksome (Eds.) *Special Operations: Out of the Shadows.* Lynne Rienner Publishers, pp 125-136.

13. Lim, J.S.; Makana Chock, T & Golan, G.J. (2020) Consumer perceptions of online advertising of weight loss products: the role of social norms and perceived deception, *Journal of Marketing Communications*, 26:2: pp 145-165.

14. McCants, W. (2015). Experts Weigh in: Can the United States Counter ISIS Propaganda, Parts 1-6, Brookings Institute, 2015, https://www.brookings.edu/blog/markaz/2015/06/17/experts-weigh-in-can-the-united-states-counter-isis-propaganda/, Accessed 20 February 2020.

15. McCombs, Maxwell E.; Shaw, Donald L.; Weaver, David H. (November 2014). New Directions in Agenda-Setting Theory and Research, *Mass Communication & Society*. 17(6): pp 781-802.

16. McGuire, W. J. (1961). Resistance to persuasion conferred by active and passive prior refutation of same and alternative counterarguments, *Journal of Abnormal Psychology*. 63(2): pp 326-332.

17. Meleagrou-Hitchens, A. (2017). The Challenges and Limitations of Online Counter-Narratives in the Fight against ISIS Recruitment in Europe and North America, *Georgetown Journal of International Affairs*, 17(3): pp 95-104.

18. Reed, A. (2018). An inconvenient truth: countering terrorist narratives – fighting a threat we do not understand. International Centre for Counter-Terrorism. The Hague, 2 July. https://icct.nl/publication/an-inconvenient-truth-countering-terrorist-narratives-fighting-a-threat-we-do-not-understand/. Accessed 20 February 2020.

19. Savary, J. & Dhar R. (2019). The Uncertain Self: How Self-Concept Structure Affects Subscription Choice, *Journal of Consumer Research*, 46, pp 887-903.

2 Extremism and Radicalization in the European Environment – Security Challenges of Return Foreign Fighters

Denis Čaleta, Sara Perković

1 Introduction

In this section, the main focus will be on those foreign terrorist fighters (FTFs) who were part of the war conflicts in Syria and Iraq and who were part of the organization called the Islamic State (IS, also known as ISIS). But who are these foreign fighters? David Malet describes foreign fighters as "non-citizens of conflict states who join insurgencies during the civil conflict. I build on this formulation and describe a foreign fighter as an agent who (1) has joined, and operates within the confines of, an insurgency, (2) lacks citizenship of the conflict state or kinship links to its warring factions, (3) lacks affiliation to an official military organization, and (4) is unpaid" (Hegghammer, 2013, p 57). Returning foreign fighters have been well recognized as a potential problem: "As regards the problem of departures, the biggest concern of intelligence and security services and the police were the process of return of EU citizens to their home countries. There are legitimate fears that the return of radicalized individuals with the knowledge of how to use weapons and with traumas from crisis areas could create a serious security risk related to terrorist threats" (Čaleta, 2016, p 18).

The research of this paper will be based on several specific European countries, even though the issue of FTFs has been detected more widely, across all European countries. The many FTFs who have returned from the Islamic State have led to increasing questions about them posing a threat to Europe. The problem of returning FTFs is in the idea that they did not leave their radicalized ideas in the conflict zone, but are returning with a will or a plan to develop terrorist activities. They are returning brave, after seeing many violent situations, and with a broad military knowledge. Other than terrorist activities, a further danger of returning FTFs is that they could radicalize others and make them want to join terrorist organizations in the future. This analysis will look into whether FTFs pose a real danger to European security, knowing that the potential threat is always possible.

2 Foreign Fighters as a Security Threat

When we speak of the return of FTFs from the perspective of the governments of the states they are returning to, it is not wrong to say that there are almost no countries that are willingly letting foreign fighters back in. Some countries have asked for the annulment of citizenship for FTFs (Canada, Australia), while others have shown more moderate approach in dealing with them. Governments have a fundamental responsibility to provide security for their citizens. Fear of the FTFs' return is something that has forced local and state governments, judiciaries, and others in the decision-making process to seek mechanisms on how to deal with them.

While both governments and citizens of countries fear the return of foreign fighters, research shows that FTFs are not prone to carrying out terrorist attacks on their return. "My data indicate that only one in nine foreign fighters returns because of an order to carry out an attack on Western societies" (Hegghammer, 2013, p 7). Besides this, "it is important to realize that not all foreign fighters represent the same level of danger" (Bos et al., 2018, p 12). At least initially, those who have travelled to Syria are less likely to see themselves as domestic terrorists than those IS sympathizers who stayed at home. They generally appear to have a stronger desire to join something new than to destroy something old.

As a result, returnees have, so far, proved a more manageable problem than was initially anticipated (Barret, 2017, p 14). There have always been a handful of foreign fighters in every conflict who engage in militant activity when they return, and the events in Paris, Brussels and elsewhere demonstrate that some of these will certainly be mass casualty attacks. However, there are unlikely to be mass numbers of foreign fighters who launch major attacks. If there were, the hundreds of thousands of returnees from Syria would have already made the attempts (Renard and Coolsaet, 2018, p 17). This is something that is confirmed in Europol's annual EU Terrorism Situation and Trend Report (TE-SAT, 2018), which states that jihadi attacks are primarily committed by "local" terrorists who have been radicalized in their own states without travelling to join a terrorist organization, and that they often do not have a direct link with the Islamic State or any jihadi organization. Of course, "recent attacks in Europe have, for the main part, been committed by lone individuals who have not been to a conflict zone – but who may have been inspired by terrorist propaganda and/or the extremist narrative, as well as by other successful attacks worldwide" (TE-SAT, 2018, p 27).

The Radicalization Awareness Network (RAN, 2017) explains how, in general, FTFs are not likely to commit terrorist attacks when returning to their own countries. However, they also mention that when we speak of returning fighters, we are talking about two generations of fighters. The first generation is composed of those who joined the conflict for humanitarian reasons to fight the Assad regime. These people are less violent; when talking about the differences between returning foreign fighters, these are the people who do not have the intention to commit any crimes. The second generation of returners is more ideologically inclined, and it is possible that they arrive with violent motives to harm EU citizens. Hegghammer states that "My tentative data indicate that militants usually do not leave intending to return for a domestic attack, but a small minority acquire that motivation along the way and become more effective operatives on their return" (Hegghammer, 2013, p 1). Finally, foreign fighters may not want to carry out attacks back in their home countries for the simple reason that such attacks could endanger their family and friends (Byman and Shapiro, 2014, p 21).

However, even though most experts will agree that foreign fighters do not represent a danger by themselves and that in most cases they do not return to carry out a terrorist attack in their own country, the danger of their return is not imaginary, and that is a reason why opponents of their return are not positive about them coming home. Brutal combat hardens the fighters, making them steady under pressure and giving them a deep sense of loyalty to their comrades-in-arms. They also gain immediate and practical skills (Byman and Shapiro, 2014, p 8). We must bear in mind that these people have completed hard training, been on the battlefield, seen and experienced many things, and learned how to use weapons. Besides this, "EU Member States reported that returnees to Europe may have a certain amount of combat and operational experience; gained an enhanced capability to commit acts of terrorism; and be particularly dehumanized and prone to violence upon their return. They also serve as role models and might be involved in recruiting and radicalizing others" (TES-AT, 2018, p. 27).

2.1 Terrorist Attacks Carried Out by Returning Foreign Fighters

At the moment, most research concerning foreign fighters, some of which has been mentioned in the previous sections, talks about FTFs not being a danger to the broader society. However, opponents of allowing foreign fighters to return to European countries will say that just one person is enough to bring death to a large number of people if they decide to commit a terrorist crime after they return. Besides this, it can be said that FTFs are a risk for radicalizing other people. Even just one person who returned to Europe with the desire to carry out a terrorist attack is enough to make us change our opinion on whether foreign fighters are dangerous.

Unfortunately, even though most of the returnees have not been inclined to carry out a terrorist attack, IS has been an inspiration to many of these people when thinking about terrorist crime. Statistics find that since declaring its caliphate in June 2014, the self-proclaimed Islamic State has conducted or inspired more than 140 terrorist attacks in 29 countries other than Iraq and Syria, where its carnage has taken a much deadlier toll. Those attacks have killed at least 2,043 people and injured thousands more" (Lister et al., 2018, e-source). Most of these attacks were carried out by people who were inspired by IS, not those who were under their direct command, and nor are there data stating that they participated in war conflict in Islamic State territory. However, there have been a large number of terrorist attacks committed by people who participated in the conflict as a member of IS and as a foreign fighter.

- "Three people were killed and another seriously injured in a shooting at the Jewish Museum in Brussels, Belgium. The suspect was identified as Mehdi Nemmouche, a 29-year-old Frenchman from Roubaix in the Pas-de-Calais region of northern France. Nemmouche, who had spent a year in Syria, is a radicalized Islamist, according to the chief prosecutor of Paris." (Lister et al., 2018, e-source).
- On 13 November 2015, eight attackers attacked Paris. They killed and/or wounded more than 400 people. Six of the attackers had returned from Islamic State where they had participated as foreign fighters.
- A returnee from Islamic State carried out an attack on an Amsterdam-Paris train in August 2015.
- In 2016 "two explosions at Brussels airport and another at a subway station in the Maalbeek district of the Belgian capital left at least 32 people dead and scores injured. In a statement posted online by several prominent supporters and by the ISIS-affiliated Amaq news agency, ISIS claimed that its fighters had carried out the attacks." (Lister et al., 2018, e-source).

All these attacks were carried out by foreign fighters of the Islamic State, resulting in the deaths of hundreds of people.

Outside Europe, attacks that have been carried out directly by fighters of IS can be found in Libya where "an attack on the luxury Corinthia Hotel in Tripoli, Libya, killed at least 10 people. The Libyan branch of ISIS claimed responsibility for the assault, which killed five foreigners" (Lister et al., 2018, e-source). The Libyan branch of the Islamic State has been responsible for several more terrorist attacks in which several hundred people have died. Attacks by Islamic State terrorists have occurred in Turkey, Saudi Arabia, and Kuwait. Other attacks which carried out by the Islamic State or by their supported group Boko Haram were instigated in Egypt, Ethiopia, Tunisia, and other countries all over the African continent.

All these examples demonstrate that even though there is no clear certainty that FTFs will carry out some of these attacks, experience shows that the possibility is there and it is real.

2.2 Legal Prosecution of Returning Foreign Fighters

In this section, we discuss ways of dealing with the return of foreign fighters to their countries of origin, and we can conclude that most countries are using two different ways to deal with them. One is the so-called soft approach, which includes processes of de-radicalization, rehabilitation, and re-integration. The other is a "hard" approach; this primarily means criminal prosecution. There is still an assumption that foreign fighters are danger to society when they return to their home environments. We should consider that these people have been part of a terrorist organization and participated in conflict.

Whereas not all foreign fighters (FFs) are foreign terrorist fighters (FTFs), the United Nations Security Council (UNSC) does not distinguish between the terms, but only uses FTFs. This shows that for the UN, the problem of FFs is mainly viewed from a counterterrorism (CT) perspective. The very first reference to FTFs was made in UNSC Resolution 2170 of 15 August 2014, without defining them (or terrorism). This (legally binding) Resolution called upon all UN Member States "to take national measures to suppress the flow of foreign terrorist fighters […] and bring [them] to justice" (Paulussen and Pitcher, 2018, p 5). The fact that UN sees these people from a counter-terrorism point of views says that it is necessary to make their return noticed, even though some of them perhaps did not plan their future actions to be dangerous to their surroundings, and did not participate in the most dangerous crimes.

The first thing that is necessary when foreign fighters return is to identify and question them and to evaluate the risk that this person represents, in order to reduce any danger and the possibility of an individual carrying out a terrorist attack. European Union countries have few solutions for what to do with returning foreign fighters, and certainly do not have good answers for the situation; nor do they know what to do with fighters, their citizens, who are still in Syria and Iraq, and have not yet returned. "Until now, European countries have not been willing to take back their citizens who have been in camps in northern Syria for some time. There are numerous obstacles to their repatriation. Numerous European countries fear that they could be released because there is a lack of evidence on their illegal activities in Syria " (Dnevni list, 2019, e-source).

There is still one indisputable fact that we have mentioned before, and that is that people have the right to return to their countries of origin, even if they have been part of a foreign con-

flict. What to do with them when they use that right and actually return, is another question. Politically, of course, it is easier to arrest them than to re-integrate them: a terrorist who acted after security services had passed on a chance to arrest them would embarrass the service and enrage the public (Byman and Shapiro, 2014, p 26). European countries are not willing to take back foreign fighters.

The world had a strong reaction to this question from the American President, Donald Trump, at the beginning of 2019. Hundreds of IS foreign fighters were imprisoned in areas controlled by Kurdish forces. In one of his Twitter posts, Trump said that the USA was asking the UK, France, Germany and all the other European allies to take on more than 800 IS fighters that had been captured in Syria and put them to trial. What had a negative echo around the European continent was the fact that Trump said that if they did not take their citizens back, the USA would set them free. This was also confirmed by Kurdish forces: the SDF – Kurdish-led forces that control north-east Syria with the backing of the USA – were holding 800-1,000 foreign fighters in prison, including Britons, Americans, French and Germans, according to a senior Kurdish official. Ilham Ahmed, co-chair of the Syrian Democratic Council, the political wing of the SDF, told the Financial Times that about 4,000 of their relatives, mainly women and children, were in camps. Ahmed said that the SDF had been urging Western countries to take back their nationals captured in Syria, warning that it could not put them on trial and process them. But the Kurdish-led authorities had not received responses (Peel at al.,2019, e-source). Until these responses from President Trump and the Kurdish forces, many European officials were able to ignore the situation of the return of their citizens who were part of this conflict, but the warning from Trump forced them to think about it. However, it did not show them what to do. "France will not fulfil the claim of American President Donald Trump to his European allies to take back fighters from Syria, but will look at it case by case," said France's Minister of Justice, Nicole Belloubet. Germany also remained cold towards Trump's claim, with the note that is hard at the moment to organize the return of foreign fighters of IS from Syria to Europe (Al Jazeera, 2019, e-source). European countries do not want the return of their foreign fighter. They expect that judgements will be made in criminal courts of countries where criminal acts were committed. This is not illogical, because their courts will investigate and prosecute crimes that have been committed based on the principle of territoriality. This is something that governments of European countries want, and is also in correlation with the intention of Barham Salih, the Iraqi president, who said that people who were involved in crimes that were committed in Iraq, should be prosecuted in Iraq: "Those who have engaged in crimes against Iraq – we are seeking them and seeking their trial in Iraqi courts" (Cornish and England, 2019, e-source).

However, it is hard to believe that courts in Syria and Iraq can fulfil this commitment in a satisfactory way. The courts have been working overtime and have in place very poor legal protection. So far, trials in Iraqi courts for people that were involved in Islamic State have been 10 minutes long, with a verdict in just a few minutes. "It is estimated that around 3,000 suspected members or supporters of IS are awaiting prosecution by Iraqi courts, the majority of whom will be prosecuted by a specialized criminal court of the first instance in Qaraqosh on terrorism charges. The court hears up to 50 cases a day in brief sessions, mostly male fighters that were picked up as the military defeated IS strongholds in the north... From Europe alone, around 100 foreign fighters are being held by Iraqi courts, most of whom face the death penalty based on the Anti-Terrorism Law no. 13" (Mehra, 2017, p 2). Besides this, "suspects are tried under a law that makes no distinction between a person who "assists terrorists" and one who commits

violent crimes on behalf of an extremist group. The conviction rate is around 98%" (Taub, 2018, e-source). Prisoners have been put together in small rooms, in inhumane conditions, with families afraid to visit them because of the fear of being put to trial themselves.

The main part of the research of this article involves foreign fighters that have returned to their countries of origin, alone or with the help of others. Cases of returning foreign fighters clearly show that, for most foreign fighters (for those who return have been registered), after their return comes custody and an investigation that leads to a trial. Foreign fighters give themselves up or are reported by family members or friends. There is also the possibility that governments find them when they want to return through state borders. At the moment most countries arrest suspects, and they then look for evidence to be able to put the returning foreign fighter to trial. In the past few years, even those countries which had anti-terrorist laws before, and where those laws included a section on joining foreign military formations, have begun to drastically tighten their laws to be able to put foreign fighters behind bars.

Punishments depend on the law of each country individually, and all the possible crimes that have been committed by returning foreign fighters have been prosecuted by local rather than international laws. However, as a European Parliament briefing of 2015 stated, "With all EU Member States having ratified and implemented the Rome Statute of the International Criminal Court (ICC), foreign fighters could be made accountable for 'international crimes' (war crimes, crimes against humanity, and genocide) committed outside EU borders (within the limits of the ICC's jurisdiction though, which is not universal)... As to 'ordinary' and terrorism-related offences (defined in criminal codes or specific counter-terrorism legislation), they may be prosecuted by individual Member States under condition that the offence has been committed on their territory (principle of territoriality), by their nationals (active nationality principle) or against their nationals (passive nationality principle)... In line with the Council Framework Decision 2008/919/JHA ('FD 2008'), national criminal laws cover a series of terrorism-related offences. Those include participation in a terrorist group, public incitement to commit a terrorist crime, recruiting terrorists and providing training to them. Some countries − such as Belgium and Germany − have gone a step further and criminalized receiving such training. The use of these provisions to prosecute individual foreign fighters seems problematic, as travelling to a conflict area is normally not a crime *per se*, unless there are grounds to prove an attempt at committing a specific offence" (Europarl, 2015, p 7). Unfortunately, though, "Another trend that can be identified is that the penalties for crimes are not standardized and thus the sentences for crimes are not uniform across states, even where conduct is arguably similar. Indeed, UNSC Resolution 2178 only requires that States "establish serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence" thus leaving the actual penalties entirely to the discretion of States (Paulussen and Pitcher, 2018, p 22).

Even countries that are members of the EU do not have standardized punishments, and not even a standardized way of prosecuting foreign fighters. The EU has tried to standardize this process of prosecution of foreign fighters by adopting additional regulatory framework. Still, we are left with questions such as what to do about people who left for Syria as the partner of a foreign fighter, or what will happen to children who are born there? Is it necessary to make a distinction between people who participated in the Islamic State as chefs or drivers, helping the organization in a supporting role, and those who were military personnel of the Islamic state? Iraq's Anti-Terrorism Law (Law no. 13 of 2005) is very strict when it comes to this

question. According to Article 4, both the perpetrators of terrorist acts and those who have assisted will receive the same punishment. This means that there is no distinction between a taxi driver working for IS or an IS fighter involved in executions; both face – if convicted – the same punishment" (Mehra, 2017, p 2).

2.3 Prisons as Places of Re-Recruitment

At the moment the number of prisoners suspected of being part of the Islamic State organization is accumulating. Because of this, special attention is being given to the question of how to lower the danger of stronger radicalization of people who find themselves in the prison system. History shows us that prisons can be very dangerous in terms of the stronger radicalization of prisoners. "Studies of past jihadi waves show that veteran fighters can play a crucial role in perpetuating the jihadi movement from one generation to another, often starting from their prison cells, where many returnees from Syria and Iraq now serve their sentences" (Renard and Coolsaet, 2018, p 3). This means that as in the past, so also today, prisons represent places where it is easy to radicalize individuals. Even the founder of Islamic State, al-Zarqawi, was radicalized in prison. An example of a prison in which prisoners were additionally radicalized is Guantanamo Bay; because of the special brutality to prisoners and behaviour towards them as soon as they were released from jail, they soon found themselves in one of the terrorist groups. Weiss and Hassan (2015, p 11) state that "prisons are one of the main ISIS recruiting centres and organization hubs." How important prisons are in the process of radicalization is shown by al Baghdadi itself, in the times before Islamic State, when he was using prisons to radicalize his supporters. "Prisons are frequently described as "hotbeds" of radicalization, because they are places in which (predominantly) young men experience personal crises and are cut off from traditional social relationships, such as family and friends" (Neumann, 2017, p 48) "Since the founding of the Islamic State in 2014, several of Europe's biggest terrorist attacks were led by former prison inmates, some of whom became radicalized while behind bars" (Mekhennet and Warricka, 2018, e-source). Prisons are places where new people can learn about radical ideas, where they can become more extreme, and where they can learn additional things about radical ideas and meet new contacts in the world of terrorism.

For all these reasons, special attention should be given to prisons and the possible stronger radicalization of people who are in prison because they were a member of the Islamic State. "According to the information of Iraqi government, 17 of the 25 most prominent leaders of ISIS who were in the war in Iraq and Syria spent some time in prison institutions under the administration of the US between 2004 and 2011" (Gerges, 2018, p 156). In an article in the Washington Post entitled "ISIS behind bars", authors Mekhnnet and Warrick (2018) said that "within the regular prison populations, officials watch for changes in behaviour that suggest radicalization is underway, such as when inmates modify their prison uniforms in jihadist style, or insist on wearing underwear when taking a shower, a reflection of conservative Islamist views about covering the body. In such cases, officials encourage inmates to meet with moderate imams and counsellors who work with the prisons on a voluntary basis." As time goes by and as more and more people receive prison sentences, danger of radicalization even includes people who up to now have not shown any signs of radicalization. "Some prisoners may perceive convicted returnees from Syria and Iraq as proven leaders and even heroes; and an influx of returnee prisoners could create a new platform for ideological radicalization and recruitment in a prison system unprepared for their admission" (Azinović and Jusić, 2016, p 83). For all of these reasons it is clear that the prison environment should be closely looked at, and stronger radicalization should be prevented. Prisons could and should be places of a

controlled environment that can be used to create successful deradicalization programmes, so we can re-integrate FF into society.

2.4 Programmes of De-Radicalization of Foreign Fighters

As countries have adopted stronger measures towards returning foreign fighters, some have used softer measures alone, or used these soft measures in combination with other methods of dealing with returning foreign fighters. These soft measures are mostly deradicalization programmes or reintegration of foreign fighters into society. Programmes of deradicalization are based on the principle of helping returning foreign fighters not to return to the terrorist organization. When going back to their own countries foreign fighters are faced with lots of challenges. Aside from the obvious ones, such as facing possible legal punishment and criminal prosecution, these challenges include meeting their families, friends, fellow citizens, and larger community once again. But in spite of this, there are potential ways to make their return easier. One of these ways is deradicalization; almost a necessary first step so that the foreign fighter can return to society. "De-radicalization is aimed at radicalized individuals. It is based on the assumption that not everyone who becomes radicalized remains committed to their cause, and that every extremist movement has disillusioned followers who have doubts, or simply want out" (Neumann, 2017, p 20). However, it is a fact that deradicalization lacks a pure definition and that there is no consensus on what constitutes successful deradicalization. Academics and practitioners use the terms deradicalization and rehabilitation interchangeably to refer to a cognitive disassociation from violent group identity and ideology. Reintegration refers to the re-establishment of social, familial, and community ties, and positive participation in society.

Developing successful reintegration programmes is crucial, not only to preventing recidivism among returnees, but also to mitigating further radicalization among the youth population and building overall community-level resilience to violent extremism (Holmer and Shtuni, 2017, p 2). Successful deradicalization programmes result in a change in beliefs and attitudes which lead to people no longer posing any danger to the society that they are returning to. It is possible that people stay with the same beliefs, even if they leave foreign territory; so, in deradicalization, it is not crucial not only to change behaviour, but also to change the deep beliefs of the person. Even those who serve prison punishment can walk out with the same or an even larger degree of radicalization. "Deradicalization means programmes that are generally directed against people that have become radicalized, with the aim of their reintegration into society or at least of deterring them from violence. Deradicalization is not a process that can be carried out alone by security personnel, but it is necessary that the whole community is involved" (Ogrizović, 2018, e-source). Further, "rehabilitation is defined here as 'a purposeful, planned intervention, which aims to change the characteristics of the offender (attitudes, cognitive skills and processes, personality or mental health, and social, educational or vocational skills) that are believed to be the cause of the individual's criminal behaviour, with the intention of reducing the chance that the individual will re-offend".

Reintegration is defined as 'a safe transition to the community, by which the individual proceeds to live a law-abiding life following his or her release and acquires attitudes and behaviours that generally lead to a productive functioning in society" (Heide and Geenen, 2017, p 8). Successful deradicalization must be carried out by teams of experts, and it is necessary for it to contain one of the following measures: "Well-articulated and inspiring counter-messaging, which effectively undermines extremist narratives, can prove powerful when prompting

extremists to reflect on their position. Using image and audio-based material on social media sites is particularly effective when communicating positive messages. Moreover, grass-roots initiatives which open up a dialogue between experts and society allow people to feel engaged and respected, while also producing valuable insight and rich discussion. Developing personal resilience can enable society to deal with the difficulties and adversaries it encounters, leaving people less susceptible to extremism. Supporting people through times of transition, via outreach programmes in schools, universities and local communities, can contribute towards healthy behaviours and develop more supportive and cohesive communities" (Manning and La Bau, 2015, p 13).

Other than those mentioned above, one successful means of deradicalization can be communication between newly-returned foreign fighters and people who have already undertaken deradicalization before them. Communication with people who know exactly what the problems were may be one of the very best ways: "Each testimony highlighted the importance of these personal stories when delivering counter-narratives." (Manning and La Bau, 2015, p 27). When we study terrorism, extremism and violent extremism we often focus heavily on tactics and strategy; yet we can learn a great deal if we look at the cognitive and emotional behaviour which underlines a particular set of beliefs (Ibid., p. 12) In the end, returning foreign fighters and those who have been deradicalized can be the ones who are of help in creating programmes for other foreign fighters: "returning foreign fighters can contribute to intelligence capacities and help in designing better deradicalization programmes (Leduc, 2016, p 18).

With regard to the Islamic State, one of the most successful ways of deradicalization can be to demonstrate how not all Islamic State studies and their theoretical teachings are in harmony with what they do. Equally, challenging their ideology can be of use. However, deradicalization must be directed towards an individual in order to be successful, and this may be the hardest thing to achieve. Depending on the individual success of each person can be tough for the programme in general, because it means that even if a certain programme succeeds with one person, it does not mean that it will be successful with others. There are so many factors on which the success of deradicalization programmes depends. Therefore, it is hard to believe that deradicalization, in ways of talking to and trying to change the beliefs of foreign fighters, can bring about a complete separation of individuals from the terrorist organization, and, of course, some people will not be able to be rehabilitated by any means. Deradicalization is not and cannot be a simple process, because governments may not have the resources necessary for the supervision and monitoring of large numbers of individuals all at once and for making sure that they have all been in programmes.

2.5 Ways of Reintegration

When discussing the return of FFs, rehabilitation and reintegration must be seen as a vital step. Today there is much more information on this subject than there was in the past, and this attitude is the best way for these programmes to be successful and achieve their purpose. Programmes of deradicalization and reintegration have generally been avoided by the countries of the western world, so they were first developed in the East. "The first-generation deradicalization programmes tailored to Islamist militants were designed and developed in response to the September 2001 terrorist attacks carried out by al Qaeda in the United States and the October 2002 bombings by Jemaah Islamiyah in Indonesia. These experimental deradicalization programmes, part of soft counterterrorism strategies, were rolled out primarily in Middle East and Southeast Asia in countries like Saudi Arabia (Prevention, Rehabilitation and After Care

in 2004), Yemen (Committee for Dialogue in 2002), Singapore (the Religious Rehabilitation Group in 2003), and Indonesia (2003)" (Holmer and Shtuni, 2017, p 7). Developed countries with problems around returning foreign fighters can learn lessons from these programmes. What became clear in the developing programmes is that each one can and must be adjusted to the foreign fighter, their surroundings and their experience, and adapted to the environment they are returning to; this is crucial for any programme to be successful.

Programmes that help to deradicalize and reintegrate returning foreign fighters into society are important for more reasons. It is essential not to let people returning from the Islamic State be left to themselves, without making any effort to help them. When returning to their countries, whether or not they are criminally prosecuted, they are returning to life circumstances similar to those they had before they left. If these life circumstances were enough to make them leave and join the Islamic State once, it is evident that the return will not be easy. In most cases they are returning into the same environments, but mentally the people are not the same. They have been in battles, and have experienced exceptionally unpleasant things, many of them life-threatening. Many may say that FFs chose to join the Islamic State and that they do not deserve help, but countries must take on responsibility for their citizens and try to make their return easier. This is for many reasons, one of which is not to let this situation happen again. We must bear in mind that the reasons for them leaving can occur again; something could trigger them, and then the first thing to cross their minds could be to leave, to pack their bags and their families and join another terrorist organization. If they begin to feel as if they do not belong in their community, or feel judged and separate from society, they cannot integrated into society.

These thoughts are based on experience where this is exactly what happened. "When the Afghanistan war ended, hundreds of Arab mujahidin fighters were blocked from returning home. This is why they decided to continue the fight, wherever and whenever they saw the opportunity to do so" (Debuef, 2019, e-source). The contrast between the sense of purpose, power, and feeling part of a community which was granted by being a member of a strong organization such as the Islamic State, and then returning to a society that possibly judges and discredits them, with a government that is not helpful, is a sure recipe for failure and for making people think that their lives as a member of the Islamic State made much more sense. So, rehabilitation, deradicalization, and reintegration of foreign fighters must be approached responsibly and, above all, with a plan. Currently, states are trying to find the best strategies towards the deradicalization and reintegration of returning foreign fighters. At this moment, one of the non-binding recommendations giving advice on how to deal with this is the "Malta Principles for Reintegrating Returning Foreign Terrorist Fighters", written by the Hedayah centre, which has published a programme scheme and principles for reintegrating foreign fighters.

3 Return of Foreign Fighters and Countries of Europe

The European Union came together on joint values such as human dignity, freedom, equality, and solidarity; democracy and the "rule of law" are two more. Any action that is not in harmony with these values is in direct dispute with EU law. Terrorist activity is one of the acts that violates the values on which the EU is based; this is why one of the most prominent threats to the EU is terrorism. In the EU it is very important to have a common position of every Member State towards certain questions; one of these is foreign and security policy. The

importance of this question is related to the fact that terrorism knows no boundaries, and this is especially highlighted here in the EU, where one of the most important values is the free movement of goods and people.

Ten years ago we might have said that "every member of the EU is solving the problem of terrorism in its own way, more or less successfully" (Prodan, 2009, p 11): so, the "Italian government introduced extensive additional legal powers to help to fight terrorism in the mid-seventies" (Wilkinson, 2002, p 113), while the German authorities were doing something else, and the French had their own system against terrorism. However, Prodan (Ibid., p 15) stated that there is no complete and effective common security and defence politics. The EU considers that Member States are responsible for all the challenges around the fight against radicalism and recruitment, but the EU can help with a certain framework to coordinate national politics, share information, and be successful in fighting against terrorism. This is how the EU thinks that fighting together can be most successful and is why it began to react with a common foreign policy so that it can protect European citizens. In 2001 the "EU adopted an Action Plan to Fight against Terrorism. Improvement in cooperation in the segment of arrests and extradition of terrorists has been accomplished by the Council Framework Decision 2002/584/JHA, by which the EU adopted the European arrest warrant" (Ibid., p 13). This Act was supposed to represent the main document of the EU on fighting terrorism.

A few years later, in 2004, the EU adopted a Declaration on Combating Terrorism, and soon afterwards an Action Plan for Fighting Terrorism. As Prodan mentions (2009, p 13), the goals of this plan were "to disable terrorists from having access to financial and other economic resources; to increase the efficiency of the working bodies of the EU and Member States when searching for terrorists, their prosecution in court, and when preventing terrorist attacks; to deepen international consensus and strengthen international participation in fighting against terrorism; to secure the safety of international traffic and the effective surveillance system of the outer borders, to increase the effectiveness of preventing terrorist attacks." In 2005 the Council adopted the EU Counter-Terrorism Strategy, which has four pillars (prevent, protect, pursue, respond).

As mentioned above, terrorism does not know borders, and this is certainly true in the case of the EU, because of the desire of the Union to have open borders. But apart from the aforementioned surveillance of external borders, an important aid in their maintenance has been the Schengen Information System (SIS). Since 2016 this system has carried "terrorism-related activity" information. Besides this, the SIS has begun to use "Stronger and Smarter Information Systems for Borders and Security" technology, which utilizes photos of people's faces. Following the last large migration wave, many people began to talk about open borders being death to European security, and because of this, some of the Schengen countries have instigated border controls. To preserve border safety, the EU has developed Frontex, the European Border and Coast Guard Agency. Frontex is necessary to secure the borders of the EU and was of great assistance during the migration crisis. The numbers of people crossing the borders and coming to Europe are changing every year. "Every attempt to quantify the number of migrants can give only a momentary and shaky figure that can be outdated after several days. According to the European Frontex agency, there are six main migrant routes: Western African, Western Mediterranean, Central Mediterranean, Eastern Mediterranean, Western Balkan, and Eastern land route" (Kešetović and Ninković, 2016, p 101). Frontex's main function is to oversee the borders, and with Regulation No. 2016/1624, it will be able to use all the prevention measures and detection of terrorism that are required.

The EU believes that it is vital that all information received is shared, not only with Europol, but with every relevant authority figure in all the Member States. The EU has approved this type of action with Article 47 in the aforementioned European Border Coast Guard (EBCG) regulation. As they must be involved in European protection from terrorism, Europol has founded the European Counter Terrorism Centre (ECTC). The European Council has control over the Centre, and its purpose is to become the main hub for the fight against terrorism. Apart from support in investigations and aid if a terrorist attack does occur, the ECTC has access to Europol bases that can be checked, if necessary, for the purpose of investigations. Exchange of information can also occur through the information base of Europol, the Europol Information System (EIS), and the European Criminal Records Information System (ECRIS), which is used so that states can share information related to any event in any criminal activity, both on suspects and convicted criminals; in other words, to any information that can keep the EU a safer place. This type of information comes to Europol through the Member States, and is later published in the EIS. Considering that this information is very confidential, the program SIENA (Secure Information Exchange Network Application) is used so as not to compromise it in any way.

In discussing the exchange of information, FADO is also beneficial; the False and Authentic Documents Online is a website managed by Geospatial Service Centre (GSC) which has in its database more than 3000 examples of false identities, travel documents, visas, stamps and so on. Another useful component of the EU's anti-terrorist work is the Terrorism Finance Tracking Program (TFTP), which helps Europol to detect the financing of terrorism. In 2015 the Council and the European Parliament adopted new rules to prevent money laundering and terrorist financing, and in 2016 the European Commission released a proposal to amend those rules to strengthen the fight against the financing of terrorism.

Finally, it does not matter that the EU offers some frameworks to deal with returning foreign fighters; the Member States are still the ones who must take full responsibility and prosecute or find successful ways to deal with foreign fighters.

Next, we will present some individual state approaches to the issue of returning foreign fighters.

3.1 Case Study: Germany

During the second half of the 20th century, Germany did not have a successful anti-terrorist policy. Germany has very strict laws about privacy that reduce the possibilities for counter-terrorism actions. One of these restrictions was the forbidden surveillance of public spaces without a concrete court order. The situation began to change when, in the 1970s, "the main German anti-terrorist laws were adopted. The main changes were in the area of arresting suspects and improving the coordination activities of police forces in the fight against terrorism. In parallel with this was the establishment of centralized structures for co-ordination and control in anti-terrorist security and police activities. A special anti-terrorist unit was formed inside the Federal Criminal Police (BKA). The German BKA has primary jurisdiction on internal national security in the area of counter-terrorism activities. GSG9 was founded in 1972 as an elite anti-terrorist special unit" (Wilkinson, 2002, p 114). Since 1989 there has been a law for the fight against terrorism called "Gesetz zur Bekampfung des Terrorismus".

A stronger reaction by the German authorities began after the attack in 2001. At this time being a part of a terrorist organization in Germany was criminalized; there was already a

list of forbidden organizations. From 2014 the Islamic State was included in this list, which meant that if anyone was caught sharing any promotional materials of the group, they could be prosecuted, including any symbols or raising money for them through social media. Other than promotion, the German authorities also made surveillance stronger for specific groups of people: "After the attack on the United States on September 11, 2001, the German police decided to use the same tool for the identification of people on the basis of demographic and socio-economic criteria taken from the profile of terrorists from 9/11" (OSCE, p 64). Besides this, Germany created the *Gemeinsames Terrorismusabwehrzentrum* (GTAZ), a common centre for the coordination of counter-terrorism.

Germany had great problems with its citizens who travelled to Syria and Iraq because of the war conflict. "According to findings of the German security authorities, more than 960 individuals have left the country to travel to Syria or Iraq out of Islamist motivation, although the actual number could be higher. The number of departures per quarter has fallen since the third quarter of 2015 and has generally been dropping since late 2014. The peak was in mid-2014, with almost 100 departures a month (Heinke and Raudszu, 2018, p 43). Heinke and Raudszus added that most of the foreign fighters who have travelled from Germany are men (79%), aged 13-62; most are between 22 and 25. Further, they said that the women who left were younger than the men, and this means that the number of minors who left for Syria and Iraq was greater among women than men. In the German example it is an interesting fact that a large number of German citizens left to go to Syria and Iraq to fight in the conflict, but *against* the Islamic State. Germany has a large Kurdish community, and it is thought that the largest number of recruits were from Germany, especially in the fight for the city of Kobanî. "We know of 204 residents that have left Germany to fight against the Islamic State in Iraq and Syria, 69 of whom are German citizens" (Heinke and Raudszus, 2018, p 48).

The German public has been quite alarmed at the thought of foreign fighters returning. In the last few years Germany has accepted a large number of refugees who have asked for asylum. Because of this the Chancellor of Germany, Angela Merkel, and her Government have received much criticism, due to the concerns of the public that there would be many more terrorist attacks. Cases such as that of the young Tunisian who came to Germany as a refugee, asking for asylum, and later carried out a terrorist attack in 2015 which killed 12 and injured 56 people in Berlin, intensified not only the way of treating refugees and asylum seekers, but also the way of looking at returning foreign fighters, especially when the responsibility for this terrorist attack was admitted by the Islamic State. Germany was faced with a large number of foreign fighters who had left for Syria and Iraq: "Germany's domestic intelligence service, the BfV, estimates that since 2013 more than 1,050 Islamists have left the country for Iraq and Syria. The BfV has found that about a third of those German Islamists have now returned to Germany, with another 200 thought to have been killed in Syria and Iraq. Of those who have returned, more than 110 played an "active part" in the fighting and remain "the subject of police and judicial inquiries", the BfV said in a statement" (Peel at al., 2019, e-source). To be more precise, "more than 1,050 Foreign Terrorist Fighters (FTFs) have left Germany for Syria and Iraq of whom, to date, 350 have returned and 200 have died. Additionally, at least 42 FTFs, a high number of women and a minimum of 59 children identified as German dual-citizens are currently detained, the vast majority in Syria and northern Iraq" (Roithamaier, 2019, e-source).

When talking about them returning, we can say that "it is difficult to predict how many more FTF will eventually return to Germany. As has been mentioned before, so far, the number of returnees has stayed relatively constant; i.e. the collapse of the IS has not yet translated into a wave of returns. The exact number of FTF remaining in the Levant is equally unknown, but about 150 German residents involved with jihadi groups are believed to have been killed in Syria and Iraq, according to recent findings. The data collected by security authorities on the motivation for returning to Germany sheds some light on this situation. About 10% came back because they grew disillusioned and frustrated with their situation; another 10% followed calls by family and friends to return home. It is believed that 8% travelled back to Germany for logistical reasons such as to procure supplies, raise funds or rest. Another 6% returned due to health issues" (Heinke and Raudszus, 2018, p 46).

Just like all the other EU countries, Germany is trying to find the right solution to deal with returning foreign fighters. Germany uses both soft and hard approaches; for the hard approach, first of all someone who joins a foreign conflict could lose their citizenship[1]. Further, "if an individual can be proven to have fought in the ranks of a terrorist group, he or she could already be prosecuted under Art. 129a, 129b of the German Criminal Code, which prescribes imprisonment between one and ten years for membership in a terrorist organization" (Rothamaier, 2019, e-source).

In general, "Germany attaches very great importance to the fight against terrorism. For this reason, considerable weight is given to effective criminal prosecution and successful prevention within rule-of-law standards. From the German point of view, it is also indispensable to work together closely at international level in the fight against terrorism... Individual terrorist acts are punished in accordance with the provisions of the general criminal statutes (as a rule, homicide and bodily harm, criminal offences against personal liberty, criminal offences against public order and criminal offences dangerous to the public, such as arson, creating an explosion and poisoning)... Section 129a of the Criminal Code contains a special provision concerning terrorist organizations. Whoever participates in an organization as a member or forms an organization, the objectives or activity of which are directed towards the commission of murder, manslaughter, hostage-taking or other serious criminal offences, shall be punished with one to ten years' imprisonment... Whoever supports a terrorist organization as defined in the Criminal Code or recruits members or supporters for such an organization shall be punishable by six months' to five years' imprisonment. Anyone supporting a so-called threatening organisation shall be punishable by up to five years' imprisonment or by a fine... In the event that the case involves a foreign organization outside the Member States of the European Union, prosecution shall only be possible in the event that there is a domestic connecting factor set out in law (e.g. the suspect's activity is exercised in Germany, the alleged perpetrator or a victim is a German national or is within Germany)" (Committee of Experts on Terrorism, 2016, pp 3-6).

Germany, like most other EU countries, does not allow foreign fighters who are not in prison in Syria and Iraq to return without very strict vetting procedures. The German authorities can decide on a case-by-case basis. However, there is definitely no chance for returning FFs to come home without official procedures and a clear decision by German government institutions. The figures show that there are about 60 men and women waiting for their trial to begin in the area of Syria and Iraq.

[1] This is only the case if the person has dual citizenship with the country they were fighting for, or the person could be without citizenship of anywhere at all.

It is clear that Germany has firmly decided to prosecute its returning foreign fighters, but Germany has concentrated more on deradicalization and preventing the radicalization of fighters in the first place than only on punishing them. When talking about German ways, we must remember that this is the country that had the problem of Nazism. In the present paper the story of Nazism is particularly interesting, because all the German programmes of rehabilitation of foreign fighters are based on the rehabilitation of Nazis after World War II. Put simply, the Germans have had problems with the far-right wing, or neo Nazis, who they also had to rehabilitate, and this has given them enough experience to not enter this situation unprepared. Germany realized at the time of rehabilitating the neo Nazis that it is necessary to use everything so that the fighters can be rehabilitated and the people restored to society. Re-socialization and de-radicalization are very important parts of the system in Germany. Even though the programmes are not standardized, Germany has a good social system in which there are many trained people who can help in deradicalization.

How important this is to Germany is shown by the data that "according to the investigation so far, the German government has spent $440,440 on the de-radicalization programme" (Svirsky, 2016, p 4).

The first German deradicalization programme, EXIT, has been active since 2000, and was founded by former police detective Bernard Wagner, together with ex neo-Nazi leader Ingo Hasselbach, to encourage people to leave neo-Nazi organizations. The Society for Democratic Culture is responsible for the EXIT programme; it is a civil society organization and a network of non-government organizations in Germany, which works on the promotion of democratic values and human rights against violence and extremism. The society does not have any political or religious standpoints, and its work is both theoretical and practical, while its focus is on all aspects of extremism. The goal of the EXIT programme is to give individual support to people who want to leave extremism, giving them specific help and support to start a new life. This programme assists not only the extremists themselves, but also to their families, officials and other people who have found themselves in close contact with extremism. EXIT is a partner of the German Federal Office for Immigration and Refugee Jobs, and the work of this programme has been recognized by the German government and the European Commission/European Social Fund.

The EXIT programme functions on the principle of offering new perspectives and new viewpoints of the world. The basic principle is that the individual must cut all ties with their former contacts in the world which they want to leave. However, EXIT does not give any assistance in finance or in court processes. It does not look for individuals to help, but people go to them; this is because the individual must have the desire to step away from radicalism. Some people think this is wrong attitude. "The research found that most Salafis do not want to be deradicalized and because the deradicalization programmes rely on cooperation they have limited impact" (Svirsky, 2016, e-source).

Building on the EXIT programme is al-Hayat, one of the most important programmes of deradicalization in Germany. Established in 2011, it was the first programme whose goal was the deradicalization of radical Islamists. Al-Hayat uses the methods, approaches, knowledge and experience of EXIT to work against Islamic radicalism. It concentrates on the family, friends, employers and all the other people who surround the radicalized person, as well as the radicalized individual themselves. "The German al-Hayat programme includes an assessment of

returned FTFs who are put through a process of counselling and reintegration if needed. The programme focuses on ideological and pragmatic elements (such as finding employment) as well as addressing the reestablishment of family relations and potentially finding an alternative social network" (Heide and Geenen, 2017, p 10).

These initiatives are based on advanced methods and approaches, in order to work with those close to radicalized people and stop the whole radicalization procedure, preventing radicalized Muslims from becoming foreign fighters in the first place. Al-Hayat seems very useful even though not everyone is convinced that it will succeed. "Hence, while Hayat's methods were demonstrably successful in combating neo-Nazi violence, it is not clear that such programmes work quite as well when it comes to radical Islamism" (Esman, 2016, p 5).
Germany, because of its role in the 2nd World War, has the burden of everything it does being examined in close detail. Germany understands that it is very important to use deradicalization and reintegration programmes and to learn from the past, using good practice in rehabilitating young neo-Nazis.

3.2 Countries of the Western Balkans

The Western Balkan region has proved to be fertile ground for the Islamic State, which used this area to successfully gather foreign fighters. "Overall, it is believed that from the end of 2012 until the end of 2017, some 1,000 individuals (men, women, children, and the elderly) from the Western Balkans travelled to Syria and Iraq. Approximately 300 have returned, more than 200 have been killed, and some 400 remain there. A number of individuals are also missing. And, following the collapse of the remaining ISIL/DAESH strongholds Mosul and Deir ez-Zor, we can assume that the ranks of current Western Balkans foreign fighting contingents have been further decimated..." (Azinović and Bećinović, 2017, p 7).

When talking about specific countries, "ICSR research indicates that volunteers from South-Eastern Europe include, at the last count, some 90 foreign fighters from Albania, 330 from Bosnia and Herzegovina, 150 from Kosovo, 12 from Macedonia, and 70 from Serbia" (Azinović, and Jusić, 2016, p 18). Recruitment in this part of Europe was very strong up to 2017. Recruitment was carried out in many different ways, one of them being through social media. The IS knew that this part of the world was important, so they even had media in local languages: "Apart from al-Naba', in 2017, IS officially endorsed propaganda outlets were the A'maq News Agency, the al-Hayat Media Centre, the al-Furqan Media Production Company, the al-Ajnad Media Production Company, the al Himma Library and al-Bayan Radio. Since its creation in 2014, A'maq News had acted as an independent news outlet, pretending to be a journalistic organ. By 2016 it had become one of the main tools for IS to claim attacks, including lone actor attacks in western countries. IS officially endorsed A'maq News in July 2017. The Nashir Agency is also suspected of belonging to the IS media apparatus, although it has not been formally or publicly endorsed by the IS. By the end of 2017, IS's main publication remained the weekly Arabic newsletter al-Naba' ("the news"). Starting in 2016 the organization launched Rumiyah. In 2017, Rumiyah was published in Bosnian, English, French, German, Indonesian, Kurdish, Pashto, Russian, Turkish, Urdu and Uyghur on a near monthly basis" (Tesat, 2018, p 30).

The pace of departure of citizens from the region to Syria and Iraq slowed down in 2015 and had almost completely stopped by mid-2016 (Azinović and Bećinović, 2017, p 7). There are several reasons for this:

- Intense regional and international efforts to criminalize foreign fighters and returnees;
- Increased fighting in conflict zones from which it is harder to step away;
- Decreased number of individuals from the region who want to fight in Syria and Iraq.

Although it seems unlikely, because of their internal political instabilities and different political and economic situations, the states of the Western Balkans have managed to deal with returning foreign fighters better than Western countries. "All the states of the Western Balkan countries have adopted strategic documents detailing the measures and procedures of states and overall social community in the fight against terrorism and violent extremism" (Ogrizović, 2018, e-source). Here a major role has been played by the Republic of Slovenia, where the need "to eliminate further duplications and overlapping in countering terrorism and violent extremism activities in the Western Balkans, has led Slovenia into the development of the Integrative and Complementary Approach to Counter-Terrorism and Violent Extremism in the Western Balkans in 2014... It is based on a joint list of priorities prepared on the basis of the actual needs of the Western Balkan countries identified in close cooperation with national authorities and with all relevant regional and international actors active in the region (altogether 52 partners) by utilising a "bottom-up" approach regarding the coordination of activities of these actors on the one hand, and by using a combined "bottom-up" and "top-down" approach in the process of needs identification" (Kozmelj, 2018, p. 34).

The fight against terrorism and securing safety is one of the most important tasks that the countries of the region must carry out, and all in different ways. "Cooperation and concerted action against the threat posed by violent extremism and terrorism is of key importance for success. International partners should not allow themselves to use this sensitive field of policy for a competition and elbowing for publicity and political advantages reflected in overlapping, duplication and investment in non-priorities, which will not be accepted by the community of donors in this difficult global economic situation... The security threats in the countries of the region are increasingly changing their national dimensions into international and transforming their nature from single type of criminal threat into horizontally interlinked criminal phenomena" (Kozmelj, 2018, p. 36).

The Government of the Republic of Kosovo has stated that it is very important to pay attention to the entire region because of the risk of radicalization. They say that movement between the borders of the countries of the Western Balkans is very fluid, and that because of that, recruitment is simplified. They highlight the parts of Kosovo, North Macedonia, Albania and the Sandžak region of Serbia which have mostly Muslim citizens living there.

"The role of the legislature and the judiciary is also important in the process of preventing violent extremism and terrorism, by passing stricter laws that criminalize activities related to terrorism and other extremist activities (incitement, recruitment, organizing, financing of terrorism and terrorist activities, illegal possession of weapons, trafficking of people, illegal crossings of the state border, forgery of travel and identity documents, going to foreign fronts). Laws sanctioning such activities have been enacted in all the countries of the Western Balkans region, especially when it comes to sanctioning departures to foreign battlefields and accessing foreign armed formations subject to a multi-year prison sentence, in order for such legal measures to show effectiveness and a positive result in prevention. Violent extremism and terrorism must be strictly enforced, and must not get into a situation, as shown by the cases from the Republic of Bosnia and Herzegovina, in which people who participated in the conflicts in Syria and Iraq on the side of terrorist Islamist formations redeemed their in-

nocence and avoided prosecution by paying "penalties" whereby such people were not prosecuted, although they were indisputably found to have committed these activities that the law incriminates. Such behaviour by state structures and the judiciary will not achieve the "deterrent effect", which is essentially the primary task of such a law in the process of preventing and combating violent extremism and terrorism" (Ogrizović, 2018, e-source).

3.3 Case Study of Bosnia and Herzegovina

The political situation in Bosnia and Herzegovina is very complex. Three nationalities live here: Croats, Serbs and Bosnians. This political division represents a huge problem for Bosnia and Herzegovina.

The war in Bosnia and Herzegovina (BiH) in the 1990s had foreign fighters for the first time; Mujahedin "FTFs have been coming to BiH since the beginning of 1992, led by the global jihad ideology, where that same ideology would lead its citizens to other countries with the same goals and motives" (Šikman, 2018, p 121). Since the war, due to the composition of the population, which has been predominantly Muslim for over 2000 years, BiH has been concerned about possible terrorist actions, including the development of illegal groups. It is known that there are many Wahhabi villages in BiH; one of the best known is a village called Maoča, the most infamous place of radical Islam. "The most famous and notorious preacher of radical Islam in Bosnia, who ended up behind bars, was Bilal Bosnic, who in his village of Gornja Maoca created an unofficial recruitment centre where people from all over Bosnia and Herzegovina, Serbia and Montenegro would come for what Bosnic described as religious education. Later, many of them would end up in Syria and Iraq." (Mejdini et al., 2017, e-source). "It was established during this research that the largest number of BiH volunteers in Syria and Iraq have come from well-known Salafi communities, such as in Gornja Maoca or Osve in the north-eastern part of the country. More than 60% have spent time in these communities, visiting or maintaining contact with residents" (Azinović and Jusić, 2015, p 37).

How serious the problem BiH has with terrorism is shown by the fact that one of the most wanted terrorists in the world, Mirsad Kadić, who was the self-styled "Head of the Intelligence Service" of IS, was arrested in BiH. Similarly to Kosovo, BiH has had problems with strong extremism and radicalism since the 1990s. Because of this situation, BiH was forced to bring in new laws to be able to include itself in the fight against terrorism; the New Strategy for the Fight Against Terrorism in BiH, and the Strategy for the Prevention of Money Laundering and Financing Terrorist Activities. The BiH Strategy leaned on the Strategy of the EU for preventing and combating terrorism.

The goals of the Strategy are:
- The prevention of crime, radicalism and terrorism in all their forms;
- Securing critical infrastructure;
- Improving procedures in investigations and processing terrorist violations and related crimes;
- The reaction to possible terrorist attacks and recovery afterwards.

Other than this, the Plan for Civil-Military Cooperation was made to respond to terrorist attacks and to deal with the consequences. This Plan has the goal of preventing and minimizing the consequences of possible terrorist attacks.

When talking about the citizens of BiH that have travelled to Syria and Iraq, we can say that "another difficulty in cataloguing BiH citizens that have gone to Syria and Iraq is the fact that a number of people from BiH, who still hold BiH citizenship, are living or working elsewhere... The results indicate that, between the spring of 2012 (with the first departure registered on 25 March 2012) and the end of 2014, a total of 156 male BiH citizens departed from BiH and other places. At the beginning of the summer of 2013, female BiH citizens started travelling to Syria as well (with the first departure registered on 17 June 2013), and a total of 36 women had departed by the end of 2014. Children have also been registered, usually accompanied by one or both parents, with at least 25 children having left BiH by the end of 2014. All told, this means that 192 adult citizens (male and female) and at least 25 children have travelled to Syria or Iraq in the period analyzed. Considering the BiH population of about 3.8 million people, the country has one of the largest contingents of foreign fighters in Europe by proportion, even when just counting the males who have departed – with more than 41 fighters per million residents" (Azinović and Jusić, 2015, p 32). This data is based on information from the police and security services. However, it is impossible to get complete data for every individual, and this represents a problem in a later phase if these people are to return to Bosnia and be processed.

As the data above shows, most of those who left for Syria and Iraq have been killed. However, all of those who are returning and who are known to have been part of the Islamic State will be prosecuted. This point was made by state Minister of Security, Dragan Mektić: "Something is prosecuted, something in phase of prosecuting. There is no one who has return, and that is not in the phase of prosecuting" (Hadžimusić, 2017, e-source). In BiH the duration of punishments is up to one year. Those who have been punished received their punishment on the basis of the prohibition against being part of foreign military formations: "Bosnia and Herzegovina introduced amendments to its Criminal Code in the summer of 2014, even before some of the states mentioned above. Article 162 (b) – Unlawfully establishing and joining foreign paramilitary or para-police formations – introduces sanctions for individuals that organize, lead, train, equip, or mobilized individuals or groups to join foreign military, paramilitary, or para-police formations that operate outside BiH territory" (Azinović and Jusić, 2015, p 48). BIH citizens that have gone to the Syrian battlefield, in the case of their return, as well as those that have returned, are realistic threat for carrying out a terrorist act or for recruiting other potential individuals for carrying out a terrorist act. This is the reason that these acts are concerning as illegal activities following legal acts in BiH such as Criminal Code, "in addition to the elementary criminal act of terrorism (Article 201), a new criminal act was introduced in 2003 for financing terrorist activity (Article 202), while in 2010 four more terrorist criminal acts were introduced: public promotion of terrorist activity (Article 202 a), canvassing for terrorist activity (Article 202b), training for carrying out of terrorist activity (Article 202c) and organizing terrorist groups (Article 202d)" (Šikman, 2016, p 171). Dnevni list quotes 46 people having been prosecuted (2019, e-source).

Further: "According to available information from the Court of BIH, 23 people were charged with the above crimes in BIH up to 2017, relating to BIH citizens leaving the country and becoming FTFs in Syria and Iraq. The majority of them were charged with Organizing a Terrorist Group, 14 in all, while eight of them were charged with Unlawful Establishing and Joining Foreign Paramilitary or Parapolice Formations. One person was charged with the criminal act of Encouraging Terrorism Activities in Public. Even though all of these individuals were charged and sentenced, the judicial politics seems troublesome, since in only five cases was the sentence within the stipulated penalty (the most lenient sentence being a prison term

of three years for this criminal act). In one case from the Court of BIH, one defendant was sentenced to a seven year term because he was a part of the Salafi community in BIH during 2013 and 2014. He went to a few cities in BIH for the purpose of propagating and spreading Islamic radicalism in BIH and the region. After that he left BIH and joined the terrorist organization ISIL in Syria and Iraq. In another case of the Court of BIH, the defendant was sentenced to a four-year because he was part of ISIL from 17.7.2013. to 11.8.2014. in Syria and Iraq" (Šikman, 2018, p 129). In the criminal prosecution of foreign fighters, "as mitigating circumstances, the Court usually mentioned their family circumstances, their admission to committing the criminal acts, a shorter time spent in Syria, sincere regret for the criminal acts, voluntary departures from the front, activities undertaken to deter people from going to Syria, and cooperation with the persecuting bodies. In eight of these cases there was a plea bargain deal with the defendants" (Šikman, 2018, p 129).

In the past few years some police actions have been carried out in the region. They have had the codenames "Svjetlost", "Damask", and "Ruben", and have arrested members of the Salafi movement who were brought together by terrorist activities and organized citizens of BiH to go to foreign battlefields (Ogrizović, 2018, e-source). The border police also have important role regarding entering process for all citizen in BiH.

As for soft measures, this is something that Bosnia struggles with; rehabilitation and deradicalization are not included in a sufficient amount. "Bosnia and Herzegovina must develop effective mechanisms for the repression and criminalization of this phenomenon; but must also understand that these measures alone cannot stop the spread of dangerous ideologies or discourage individuals from embracing them. It is imperative that BiH society abandon its voyeuristic attitude toward this phenomenon and work toward developing social responses. This will require strengthening remaining social correctives – from families, to schools and academia, to the media, to civil society – and developing a clear and universal system of values and norms" (Azinović and Jusić, 2015, p 80).

"In this regard, the issue of deradicalization of individuals and their integration into society is especially important. It means not only deradicalizing these individuals, but other like-minded people who pose a similar threat, which was best manifested in 2015 when there were three terrorist attacks in BIH where two soldiers and one police officer were killed... Although there are extensive recommendations on how to carry out deradicalization programmes in BIH, it seems that this process has not made much progress. Positive examples can be the call to closing down the para-jamaats by certain religious leaders, which was not well received by radicalized groups. Hence this issue seems to be the most important, but also the biggest challenge for BIH" (Šikman, 2018, p 131).

3.4 Case Study of Kosovo

The Republic of Kosovo, a country only 12 years old, has still not been recognized by some countries of the world, including five countries of European Union (Cyprus, Spain, Slovakia, Greece and Romania), large international forces such as China, India and Russia, and also her neighbour, Serbia. Not getting recognition is not surprising because of the way Kosovo was founded, declaring independence from Serbia. Kosovo was given help by NATO to gain independence. NATO's bombing of Serbia in 1999 was one of the reasons why "One of the strongest supporters of the US and the West, Kosovo is also one of the poorest countries in Europe with an unemployment rate around 40 per cent" (Haxhiaj and Nabolli, 2018, p 4).

At the time of the Balkan Wars, even though Kosovo was still part of Yugoslavia, its people were already facing ideological and religious sharing by different NGOs who were, certainly, sharing money and building Mosques, but also actually promoting radicalism. "Kosovo faces many challenges in its efforts to eliminate the causes and factors impacting on the spread of extremist religious ideology, violent extremism and Islamic radicalism. The post war situation, economic and social problems, unemployment, poverty, lack of perspective, crime and corruption are counted as a conductive factors utilized by political Islam elements in the spread of religious extremism and radicalism in Kosovo" (Arifi, 2018, p 110). However, sharing religious extremism ideology in Kosovo at that period was not so strong as we could see in he case of Islamic state. Islamic State propaganda was very quick to attract people from Kosovo because it began to share local problems and refer to local people. The Islamic State demonstrated the same manner of functioning in BiH – two countries which share a similar history and religious point of view.

The Government of Kosovo approached the problem of people being radicalized and joining Islamic State very seriously. In 2015 they approved a five-year Strategy on the Prevention of Violent Extremism and Radicalization leading to Terrorism. The Strategy shows that the Government of Kosovo understands how necessary it is to have complete and specific steps to successfully fight against terrorism. They also developed an action plan for implementing the Strategy, approved by the Government in 2016. The Strategy was written by a government working group which included representatives of the Prime Minister's office, the Ministry of Education, the Ministry of Justice, the Kosovo police, the Kosovo Intelligence Agency (KIA), the Secretary of Council Safety of Kosovo and other Government agencies, together with representatives of religious communities and NGOs. A role was even played by international partners such as OSCE and UNDP, in securing support from their experts in writing the Strategy.

The Government of Kosovo outlined four approaches in the Strategy:
- Early identification (cause, factors and targeted groups)
- Prevention (violent extremism and radicalism)
- Intervention (with the goal of preventing threats that came out from violent radicalism)
- Deradicalization and reintegration of radicalized individuals[2].

This is not the only strategy which tries to deal with foreign fighters and terrorism in general. There are a number of national strategies mentioned in the Government plan as the most important in helping bring about a solution to radicalism:
- National Strategy of the Republic of Kosovo on Crime Prevention and Action Plan 2013-2017
- National Strategy Against Terrorism 2012-2017 of Republic of Kosovo
- National Strategy and Action Plan for Community Safety 2011-2016
- National Strategy of the Republic of Kosovo for the Prevention and combating the informal economy, money laundering, terrorist financing and financial crimes 2014-2018 and Action Plan
- Kosovo Strategy for Youth 2013-2017 and Action Plan 2013-2015
- National Strategy on Integrated Border Management
- National Strategy against Drugs.

[2] Office of the Prime Minister; Strategy on the Prevention of Violent Extremism and Radicalisation leading to Terrorism 2015-2020, p 5

Azinović and Jusić presented strategic objectives of Kosovo government and put pursuit as one of the important factor. According to this Kosovo Government understand "pursuit, investigation and bringing to the justice individuals or groups who pose a terrorist threat or who commit terrorist acts.

- Preventing, hindering and investigating violent extremists or terrorists from influencing, recruiting, planning and building legitimacy within the territory of the Republic of Kosovo.
- Establishing partnership with the community, and inter-institutional, regional and international cooperation and coordination, and of international organisations.
- Establishing and strengthening the capacities of the Institutions of the Republic of Kosovo in identification, prevention, detection and pursuit (Azinović and Jusić, 2016, p 151)".

Poverty, the war that finished not that long ago, and the mostly Muslim citizens were all pluses for the Islamic State, which saw in this country potential fighters: "Nearly two decades after the war, following the establishment of the Islamic State in Syria and Iraq, many young people from Kosovo, some of them taking their wives and children, joined ISIS and the al-Qaeda branch, al-Nusra" (Haxhiaj and Nabolli, 2018, e-source). The Republic of Kosovo became, in a short period of time, a source country for members of the Islamic State. Looking at the figures, it is easily concluded that a large number of Kosovo citizens accepted the ideology of the Islamic state and went to fight on the side of this organization. The number appears even larger when we remember that Kosovo has only 2 million residents. Statistics confirm that more than 315 people from Kosovo, 120 from Albania and over 100 from Macedonia have joined the Islamic State in Syria and Iraq over the past few years. At least 65 of them were killed in the fighting, leaving their families in an even worse plight (Haxhiaj and Nabolli, 2018, e-source). This information has been confirmed by the Government of Kosovo; about 300 Kosovo citizens have been involved in the conflicts in Syria and Iraq. Reacting to the rise of foreign fighters, in 2015 the Government of Kosovo enacted a law that forbids any participation, financing, or recruitment in military conflicts outside the state territory.

According to official demographic data provided by the Kosovo police, "about 75 percent of Kosovar nationals of adult age (men and women) known to have travelled to Syria and Iraq after 2012 were born between 1984 and 1997. […] Police records indicate that of the 142 Kosovans for whom educational data is available, 3 percent have completed elementary education, 87 percent secondary education, and 10 percent tertiary education. The overwhelming majority of known foreign fighters from this dataset have moderate rather than poor formal education, contrary to what anecdotal evidence sometimes indicates. Put differently, it is not necessarily or primarily the less educated—and by implication more uninformed—segments of society who are recruited to fight in Syria and Iraq (Shtuni, 2016, p 3).

What has happened to all these people? "As of May 2016 about fifty-seven Kosovan men, some 18 percent of all nationals who have travelled to Syria and Iraq, are reported killed. No deaths among women and children have been reported. As many as 117 people (37 percent) have since returned to Kosovo. Returnees are overwhelmingly men; in other words, 45 percent of all men who travelled to Syria and Iraq have since returned. By contrast, only one in seven women, less than 14 percent, have returned to Kosovo. Given that most Kosovan women have reportedly travelled to Syria and Iraq with their husbands, this trend may indicate that the men who have travelled to the conflict theatre with their spouses are arguably more committed to the cause and less likely to return home. At the same time, it is more difficult for women to leave the conflict zone because they can travel only when accompanied by a man. When their

husbands are killed, widows are often forced to remarry. An estimated 140 Kosovar nationals, or 45 percent, were still in the conflict theatre as of May 2016" (Shtuni, 2016, p 3).

The reasons why Kosovo has become a very desirable ground for the recruitment of foreign fighters and for the expanding ideology of the Islamic State can be found not only in social issues such as the previously mentioned poverty, high youth unemployment, and social isolation, but also in not having a quality government, which is blamed by many for this situation. The government was not ready, from either a secular or a religious point of view, to solve the problems of a greater expansion of extreme ideology, especially in the rural parts of the country, where young people felt isolated and which were used by radical Imams who had been imprisoned before for spreading extremism.

The Kosovo Centre for Security Studies (2017) states that three main reasons for the story of Islamic State are:

- An externally-driven narrative that relies on an interpretation of Islam, the quotations from the Koran and a basic "clash of civilizations" worldview to justify the call to join IS in a bid to create the "caliphate" as an Islamic entity that would triumph over the secular state and the Christian world;
- An internally driven, locally tailored narrative that pits IS Kosovo Albanian leaders against the state and religious establishment in Kosovo in a bid to discredit them;
- An attempt to replace appeals to join IS from the pulpit by examples of direct action, often simply by appearing in the war theatre, but also by engaging in brutality (Kraja, 2017, p 20).

Every fighter carries a specific risk, so the government has had to approach this challenge very firmly. It seems that the government is very aware of the problem that they have with foreign fighters, so they have publicly said that they are being very strict in order to have a strong stand against terrorism, and that their main goal is to protect their citizens. As in many other countries, the main role must be in the cooperation of institutions. In Kosovo, a large role is played by the Kosovo police, who have not only arrested returnees, but also encouraged the arrests of Imams who have been recruiters. "From 2013 to July 2016, the Kosovo police have kept 292 individuals suspected of involvement in acts of terrorism or promoting religious extremism under surveillance. Criminal charges have been brought against 219, 119 have been arrested, and indictments have been filed against 92" (Shtuni, 2016, p 11).

The Government of Kosovo has indicated that in order to find out why people left to join the Islamic State, their intention will be to interview the people who are returning from the conflict. It will try to give better attention to prisons as potential places for the recruitment of new terrorist fighters, and also pay attention to families of the fighters. "Dritan Demiraj, a former Interior Minister of Albania and a graduate of the country's Military Academy as an expert in terrorism, said that the deradicalization of relatives of ISIS fighters remains a challenge for the authorities. 'The Albanian authorities should provide social assistance to their relatives, particularly to their children. Such service centres have been established in various countries. So it is made clear to them that they have no future with terrorism,' Demiraj told BIRN" (Haxhiaj and Nabolli, 2018, p 8). It is the government's intention for the public to know that the "prevention of violent extremism and radicalism remains a priority and a constant challenge for the institutions of Kosovo. The activities of law enforcement and security institutions have been intensified, and the causes and favourable factors for the spread of Islamic extremism and radicalism in Kosovo have also been identified" (Arifi, 2018, p 116).

Most citizens of Kosovo do not support the participation of their citizens in the conflict in Syria. They expect that the Government of Kosovo and the law enforcement agencies will do everything possible to provide them with security and at the same time respect their civil freedoms and human rights (Azinović, V. Jusić, M., 2016, p 144).

When talking about deradicalization, the Government of Kosovo thinks that it is a failure if it even reaches this step, as it means that they did not succeed in their intention of identification and prevention. They talk about helping individuals to turn away from extreme ideology and violence, and consider that risk assessment of returning foreign fighters is very important and must include a number of aspects, such as physiological help and support.

Kosovo needs a serious approach to dealing with returning foreign fighters. Apart from prison sentences, it is necessary to work on deradicalization and re-integration into society. It is crucial for Kosovo to become a state where all people can have a normal life.

4 Discussion and Conclusion

Foreign fighters, historically speaking, are not a new aspect to military action. However, in this conflict, because of the sheer numbers of them, they have brought a lot of insecurity and open questions for the states from which they came. When they first began to join the conflicts in Syria and Iraq, their states did not see this situation as alarming, even though it was analyzed and discussed a great deal, especially in the mainstream media, who saw this "foreign fighters" situation as very interesting from the beginning of the strengthening Islamic State. But this situation of not caring changed when the first foreign fighters began to return, now with war experience, military knowledge, and having taken part in violent action. All of this made governments react to this situation and begin to see it as alarming.

The countries included in the research part of this paper seem not to have any form of clear and consistent policy towards foreign fighters. They are countries with a large number of citizens who left their homes to join the Islamic State, so are particularly interesting for research.

The countries of Europe are doing their best to successfully deal with returning foreign fighters. Some are using soft approaches and some are using hard approaches, while others are mixing the two, but not one of these countries knows whether their decision will be successful in dealing with the problem.

Research has shown that it would be irresponsible to let people who come back from the Islamic State manage alone and without any support. This would not lead to the successful integration of foreign fighters, but only to a situation that creates problems in the future. For a successful process of deradicalization it is necessary to begin during the period of imprisonment of the foreign fighter, and to continue long enough for the community to be safe after they have left prison. The deradicalization and re-integration of foreign fighters is vital not only for the fighters and their families, but also for the other citizens and national security.

In general, it is important to increase communication between European countries; not only those in the EU, but also the non-EU Western Balkan countries that have had great issues with foreign fighters. Countries need to determine what punishment those who are involved

in conflict as foreign fighters can expect. it is clear that for the EU to be successful in this it is necessary to fight terrorism together – all the member states.

It is essential to share information between countries about foreign fighters, potentially dangerous returnees, ways of reintegrating returning foreign fighters, successful programmes, problems, and opportunities, and especially to have cooperation at levels of authority, from the government, intelligence and security services, ministries and judges, to social workers and local authorities. They must all work together for success in dealing with foreign fighters, especially local secular and religious authorities, because they are the ones with the best information about potential threats, and can be the first to notice individuals who are a potential threat or who are changing and becoming more radicalized.

Support must also be given to families of foreign fighters. They are crucial in helping someone who is being radicalized and in moving them from those surroundings. Family members must be educated in what to look out for. One of the reasons why people became radicalized was the feeling not being accepted; knowing this, governments must bear in mind that the only solution is to develop strategies against discrimination in society.

In the end, properly supported returning foreign fighters can be of great value to the countries they are returning to, not only because they will then no longer pose a danger, but also because they can provide critical information that only someone who was a member of a terrorist organization could know. Successfully deradicalized people can also have a vital role in mentoring others.

5 References

1. Arifi, K. (2018). The role of women in Countering Violent Extremism and Radicalization: the Kosovo perspective. Čaleta, D. (Ed.) and Robinson, A. Corinna (Ed.) Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats. Ljubljana: Ministry of Defence of the Republic of Slovenia, Joint Special Operations University and Institute for Corporative Security Studies, pp.31-44.
2. Azinović, V., Jusić, M. (2016). The new lure of the Syrian war – the foreign fighters Bosnian contingent. Sarajevo. Atlantic initiative. URL: file:///C:/Users/Denis/Downloads/The%20New%20Lure%20of%20the%20Syrian%20War%20%20The%20Foreign%20Fighters%20Bosnian%20Contingent.pdf
3. Barrett, R. (2017) Beyond the Caliphate: Foreign Fighters and the Threat of Returnees.The Soufan Center. URL: http://thesoufancenter.org/research/beyond-caliphate/
4. Bos, et al. (2018). Capacity Building Challenges: identifying progress and remaining Gaps in Dealing with Foreign (Terrorist) Fighters. ICCT Hague. URL: https://icct.nl/publication/capacity-building-challenges-identifying-progress-and-remaining-gaps-in-dealing-with-foreign-terrorist-fighters/
5. Byman D., Shapiro J. (2014) Be Afraid. Be a Little Afraid: The Threat of Terrorism from Western Foreign Fighters in Syria and Iraq. URL: https://www.brookings.edu/wp-content/uploads/2016/06/Be-Afraid-web.pdf
6. Committee of Experts on Terrorism (Codexter) (2016). Council of Europe. URL:https://rm.coe.int/1680641010

7. Cornish, C., England, A. (2019). Iraq to prosecute 13 French ISIS fighters captured in Syria. The Financial Times. 13.5.2019. URL: https://www.ft.com/content/7254c20a-3920-11e9-b72b-2c7f-526ca5d0

8. Čaleta, D. and Shemella, P. (2016). A comprehensive approach to counter radicalism and extremism: future challenges for counter terrorism process. Ljubljana: Ministry of Defence of the Republic of Slovenia; Institute for Corporative Security Studies; Monterey Center for Civil-Military Relations.

9. Čaleta, D. and Robinson, A. Corinna (2018). Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats. Ljubljana: Ministry of Defence of the Republic of Slovenia, Joint Special Operations University and Institute for Corporative Security Studies.

10. DCAF, Geneva Centre for the Democratic Control of Armed Forces (2015). National Security Policy. URL: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_9_National%20Security%20Policies.11.15.pdf

11. Debeuf, K. (2019). Trump right for once: Europe should take back foreign fighters. URL: https://euobserver.com/opinion/144196, 20.2.2019.

12. Directive (EU) (2017). On combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

13. DW Documentary: From Islamic State victim to terrorist hunter-Masoud`s list (2017) DW Documentary. Germany.

14. Esman, A. (2016) Europe Gambles on De-Radicalization Programmes as Terror Threat Rises. The Algemeinter. URL: https://www.algemeiner.com/2016/10/28/europe-gambles-on-de-radicalization-programmes-as-terror-threat-rises/ , 10.9.2018.

15. European Parliament (2015) Briefing. URL: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-548980-Foreign-fighters-FINAL.pdf

16. EXIT Deutschland(2016). EXIT-Germany. We provide the way out. De-radicalization and Disengagement. ZDK Gesellsharft Demokratische Kultur gGmbH. Bernard Wagner. 8.9.2018.

17. Gerges A. Fawaz (2018). Making the Arab World: Nasser, Qutb, and the Clash That Shaped the Middle East. Princeton University Press, USA.

18. Hadžimusić, A. (2017) Državljani BIH ne(odlaze)na strana ratišta. N1 BA. URL: http://ba.n1info.com/Vijesti/a154101/Drzavljani-BiH-ne-odlaze-na-strana-ratista.html 5.6.2020.

19. Haxhiaj, S. i Nabolli E. (2018). Parents of Albanian ISIS "Martyrs" Abandoned to Grief. Belgrade: Balkan Investigative reporting Network. URL: http://www.balkaninsight.com/en/article/parents-of-albanian-isis-martyrs-abandoned-to-grief-01-12-2018.

20. Hegghammer, T. (2013) Should I Stay or Should I Go? Explaining Variation in Western Jihadists` Choice between Domestic and Foreign Fighting. URL: https://pdfs.semanticscholar.org/b192/9b3d3118ffd982c83d6eacf67df3e69d329c.pdf?ga=2.77730836.1015348622.1592410624-280977485.1592410624

21. Heide, van der L. i Greenen, J. (2017). Children of the Caliphate. Young IS Returnees and the Reintegration Challenge. ICCT Hague. URL: https://icct.nl/wp-content/uploads/2017/08/ICCT-vanderHeide-Geenen-Children-of-the-Caliphate-2.pdf

22. Heinke, D.H, Raudszus, J. (2018). German foreign fighters in Syria and Iraq. CTC Sentinel, 2015/1, (8) 1, 18-43.

23. Holmer G., Shtuni A. (2017) Returning Foreign Fighters and the Reintegration Imperative. Washington. USIP. URL: https://www.usip.org/sites/default/files/2017-03/sr402-returning-foreign-fighters-and-the-reintegration-imperative.pdf

24. Human Security Now, Commission on Human Security. URL: http://www.gdrc.org/sustdev/husec/z-whatis.html, 18.6.2019.

25. Implementation of the counter-terrorism agenda set by the European Council (2016) Council of the European Union. Brussels.

26. Judgment. Federal Prosecutor v Hamza B, Harris C-K, Abdelfatah A, Younnes HA, Kamal A and Sami L. (2015) URL: http://www.internationalcrimesdatabase.org/Case/3288

27. Judgment. Prosecutor v Harun P. Germany (2015) URL: http://www.internationalcrimesdatabase.org/Case/3283

28. Kešetović, Ž., and Ninković, V. (2016). Migrants and Local Extremists in South-Eastern Europe, in Čaleta, D. & Shemella, P. (Eds.) A Comprehensive Approach to Counter-Radicalism and Extremism – Future Challenges for Counter Terrorism Process. Ljubljana, pp101-114.

29. Kozmelj, R. (2018). The Integrative Internal Security Governance Response to Radicalization in the Western Balkans Through the "Prevent-Refer-Address" Concept. Čaleta, D. (Ed.) and Robinson, A. Corinna (Ed.) Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats. Ljubljana: Ministry of Defence of the Republic of Slovenia, Joint Special Operations University and Institute for Corporative Security Studies, pp.31-44.

30. Kraja, G. (2017) The Islamic State narrative in Kosovo. Deconstructed one story at a time. Kosovar Center for Security Studies. Prishtina. URL: http://www.qkss.org/repository/docs/ISNinKosovo-eng_794656.pdf

31. Leduc R. (2016) Are returning foreign fighters dangerous? Re-investigating Hegghammer`s assessment of the impact of veteran foreign fighters on the operational effectiveness of domestic terrorism in the West. Url: https://www.researchgate.net/publication/330599121_Are_returning_foreign_fighters_dangerous_Re-investigating_Hegghammer's_assessment_of_the_impact_of_veteran_foreign_fighters_on_the_operational_effectiveness_of_domestic_terrorism_in_the_West

32. Lister, T, Sanchez, R. et al. (2018) ISIS goes global:143 attacks in 29 countries have killed 2,043. CNN. URL: https://edition.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html

33. Manning, R., La Bau, C. (2015). In and out of Extremism. Quilliam. URL: https://d3n8a8pro7vhmx.cloudfront.net/nmcve/pages/84/attachments/original/1514348329/in-and-out-of-extremism.pdf?1514348329

34. Martinović, Jovo (2017). Đihadisti sa Balkana se vraćaju kući. Datum pristupanja: URL: http://javno.rs/analiza/razbijene-iluzije-o-kalifatu--dzihadisti-sa-balkana-se-vracaju-kuci , 28.8.2019.

35. Mekhennet, S., Warrick, J. (2018) ISIS behind bars. The Washington Post.URL: https://www.washingtonpost.com/graphics/2018/world/europe-isis-prisons/?utm_term=.44466e085c50

36. Mejdini et. al. (2017) Balkan Imams Take Counter-Extremism Struggle Online. Belgrade: Balkan Investigative Reporting Network. URL : http://www.balkaninsight.com/en/article/balkan-imams-take-counter-extremism-struggle-online-07-04-2017

37. Mehra, T. (2017) Bringing (Foreign) Terrorist Fighters to Justice in a Post-ISIS Landscape Part I: Prosecution by Iraqi and Syrian Courts. ICCT. URL: https://icct.nl/publication/bringing-foreign-terrorist-fighters-to-justice-in-a-post-isis-landscape-part-i-prosecution-by-iraqi-and-syrian-courts/ 25.7.2019.

38. Neumann, Peter. (2017) Countering Violent Extremism and Radicalisation that Leads to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region. URL: https://www.osce.org/chairmanship/346841?download=true

39. Nacionalna strategija republike Kosova za sprječavanje i borbu protiv neformalne ekonomije, pranje novca, finansiranje terorizma i finansijskog kriminaliteta 2014-2018. Republika Kosovo. Prishtina.

40. Ogrizović, D. (2018). Centar bezbednosti. Proces suprotstavljanja nasilnom ekstremizmu i terorizmu (islamistički terororizam, Balkan). URL: http://www.centarzabezbednost.org/proces-suprostavljanja-nasilnom-ekstremizmu-i-terorizmu-islamisticki-terorizam-balkan/

41. Organizacija za evropsku sigurnost i saradnju (2014). Sprječavanje terorizma i suzbijanje nasilnog ekstremizma i radikalizacije koji vode ka terorizmu: Pristup kroz rad policije u zajednici. URL: https://www.osce.org/bs/secretariat/119226?download=true

42. Paulussen, C. and Pitcher, K. (2018). Prosecuting (Potential) Foreign Fighters: Legislative and Practical Challenges. ICCT. URL: https://icct.nl/wp-content/uploads/2018/01/ICCT-Paulussen-Pitcher-Prosecuting-Potential-Foreign-Fighters-Legislative-Practical-Challenges-Jan2018-1.pdf

43, Perteshi, S. and Qehaja F. (2017). Reintegration of returning foreign fighters: what approach best suits Kosovo? Kosovar Center for Security Studies. Prishtina.URL:http://www.qkss.org/repository/docs/Reintegration_842325.pdf

44. Prodan, T. (2009) Protuteroristička politika Europske unije. Polemos. URL: https://hrcak.srce.hr/47703

45. RAN, Centre of Excellence (2017). Responses to returnees: foreign terrorist fighters and their families. July 2017. URL:https://ec.europa.eu./home-affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf

46. Reed, A., Pohl., J (2017). NATO. Tackling the surge of returning foreign fighters. URL: https://www.nato.int/docu/review/2017/Also-in-2017/daesh-tackling-surge- programmes/EN/index.htm

47. Regulation 2016/1624 on the European Border and Coast Guard (Frontex) (2016). Frontex.

48. Renard, T. and Coolsaet R. (2018). Returnees: Who are they, why are they (not) coming back and how should we deal with them? Assessing policies on returning foreign terrorist fighters in Belgium, Germany and the Netherlands. Egmont paper. URL: http://www.egmontinstitute.be/returnees-assessing-policies-on-returning-foreign-terrorist-fighters-in-belgium-germany-and-the-netherlands/

49. Roithamaier, Kilian (2019) Germany and its Returning Foreign Terrorist Fighters: New Loss of Citizenship Law and the Broader German Repatriation Landscape. ICCT. URL:https://icct.nl/publication/germany-and-its-returning-foreign-terrorist-fighters-new-loss-of-citizenship-law-and-the-broader-german-repatriation-landscape/

50. Shtuni, A. (2016) Dynamics of Radicalization and Violent Extremism in Kosovo. United States Institute of Peace. URL: https://www.usip.org/sites/default/files/SR397-Dynamics-of-Radicalization-and-Violent-Extremism-in-Kosovo.pdf

51. Strategy on the Prevention of Violent Extremism and Radicalisation Leading to Terrorism 2015-2020. Republic of Kosovo. Office of the Prime Minister. Prishtina. http://www.internationalcrimesdatabase.org/foreignfighters?p=2#results

52. Svirsky, M. (2016). German De-Radicalization Programmes Not Working. Clarion Project. URL: https://clarionproject.org/german-de-radicalization-programmes-not-working/. Acccessed: 10.9.2018.

53. Šikman, M. (2018). Return of the Foreign Terrorist Fighters – Criminal Prosecution and Deradicalization. Čaleta, D. (Ed.) and Robinson, A. Corinna (Ed.) Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats. Ljubljana: Ministry of Defence of the Republic of Slovenia, Joint Special Operations University and Institute for Corporative Security Studies, pp.119-136.

54. Taub, Ben. (2018) Iraq`s post-ISIS campaign of revenge. The New Yorker. URL: https://www.newyorker.com/magazine/2018/12/24/iraqs-post-isis-campaign-of-revenge

55. TESAT (2017) European Union Terrorism Situation and Trend Report. Europol. URL: https://www.europol.europa.eu/tesat-report TESAT (2018).

56. Weiss, M., Hassan, H. (2015) ISIS. U srcu vojske terora. Zagreb: Vjesnik d.d.

57. Wilkinson, P. (2002). Terorizam protiv demokracije. Zagreb: Golden Marketing.

3 Russian Cyber Operations: The Relationship between the State and Cybercriminals

Mark Grzegorzewski

1 Introduction

In a world of "Great Power Competition" (GPC), foreign policy analysis tends to focus on state-centric actors. This foreign policy frame of reference is flawed, because GPC analysis focuses on traditional metrics of state power projection, including hard power, such as the quality and quantity of tanks, aircraft carriers, and advanced aircraft. While this certainly is one component in evaluating GPC, it misses many other capabilities of power projection, which include covert operations, influence operations, and cyber activities. While difficult to operationalize due to their often clandestine or covert nature, cyber activities are one of the leading capabilities of states in GPC. In particular, the Russian state specializes in each of these non-traditional capabilities, especially cyberspace activities. Moreover, the Russian state specializes in hybrid warfare, wherein it leverages cybercriminal networks to pursue its interests abroad.

The Russian state is one of the most effective actors in the cyber domain. The Russian state's most potent cyber operators include the Federal Security Service of the Russian Federation (FSB), the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and the Foreign Intelligence Service of the Russian Federation (SVR) (Connell and Vogler, 2017). The FSB collects political intelligence and primarily serves as a domestic security service (i.e. "Cozy Bear"). The GRU is the military intelligence service and collects information on foreign military capabilities, activities, and plans (i.e. "Fancy Bear"). The SVR serves to collect external intelligence on foreign governments. Each of these organizations has wide-ranging cyberspace capabilities that can conduct espionage and/or exploit information systems.

The cyber capabilities of these organizations do not take into account Russia's non-state capabilities, including "patriotic hackers" and Russian cybercriminals who work with the Russian

state (Schwirtz and Goldstein, 2017). How we conceptualize this relationship between the Russian state and these non-state actors impacts how we view Russia in GPC and how we respond to their cyberspace actions. While the relationship between Russian patriotic hackers and the Russian state has been extensively researched (Applegate, 2011; Dinniss, 2013; Summers, 2017), the relationship between the Russian state and Russia cybercriminals is less well understood. If we understand better what the relationship between Russian cybercriminals and the Russian state is, as well as how Russia implicitly steers criminal groups to further their foreign policy interests, it will alter the way in which the United States responds to Russian cyberspace actions. The aim of this paper is to illuminate the false distinction between national security and crime, with a focus on Russia (Broadhurst et al., 2014).

In what follows, I will first lay out the state of the literature in Dark International Relations (IR), a burgeoning field, and the main jumping-off point for this paper, the cyber mercenary thesis. I then move on to how the Russian state has created an implicit avenue in which it does not have to direct its cybercriminals to achieve the state's ends. In the third part of the paper, I show the connection between the state and cybercriminals as part of a fourth cyber mercenary typology. I conclude with some observations about the false distinction between crime and national security.

2 The State of the Literature

The relationship between the Russian state and Russian cyber criminals falls under "Dark IR." This term, coined by Paul Kan, addresses the gap in the literature wherein criminal states are left out of the dominant IR theories, since they fall between Realism's primary focus on the state and conflict in the international system, and Liberalism's integration of non-state actors and the potential for cooperation. As stressed by Kan, the focus on criminal states also has a place within another major IR program, Constructivism, in that Dark IR explains why some states interact with the illicit world of crime to further their international agendas, and why other states choose to focus on "nice norms such as human rights, environmental protection, climate change, and women's rights" (Kan, 2019). That is to say, there is a normative component to the way in which states are supposed to act in both Realism and Liberalism, and those states that look the other way to criminal enterprise are violating the positive IR norm while concurrently perpetuating a negative IR norm. Of course, there are different degrees to which states embrace criminal enterprise in order to further their agendas.

Michael Miklaucic and Moises Naim follow this theme of negative norms in Dark IR, and note that at one end of the spectrum is "criminal penetration" of the state, where a criminal enterprise is able to place one of their own into the state structure; this individual in that capacity works both for the state and for the criminal enterprise. Further up the chain of criminal penetration is "criminal infiltration", where the criminal enterprise begins to spread throughout the institutions of the state, thereby allowing illicit networks to proliferate. According to Miklaucic and Naim, even worse than criminal infiltration is "criminal capture", where the takeover of the state is so complete that criminal agents are in positions of power that excludes them from prosecution. Finally, worst of all, is the "criminal sovereign", at which point the state uses criminal activity as a matter of policy. It is this last stage that the Russian state finds itself in today. As noted by Mark Galeotti, the Russian government has now become the largest gang in the state (Galeotti, 2017).

Criminal states can also be viewed through the lens of the kleptocratic interdependence thesis as articulated by Kelly Greenhill, which addresses "a set of profit- and power-driven, self-reinforcing domestic and international relationships between criminal groups and government officials". In this relationship, criminals provide support to the elites, who protect the criminals. This long-lasting, mutually supportive relationship in effect blurs the lines between politics and crime (Greenhill, 2009); it becomes parasitic in that the institutions of the state become corrupted by crime.

In contrast, the cyber mercenary thesis, as articulated by Tim Maurer, describes how states use proxy groups, including criminals, to project power. Maurer defines a cyber mercenary as "an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect". He divides this relationship between states and their proxies into three distinct typologies along a spectrum in order to explain the degree of control by states. Maurer concludes that the reason for the cyber state-proxy relationship is due to the state attempting to retain plausible deniability and to avoid engaging in direct conflict (Maurer, 2018).

Maurer's three typologies are delegation, orchestration, and sanctioning; in brief, delegation involves the state strictly authorizing the proxy to act on its behalf, orchestration involves a loose relationship between the state and the proxy to carry out actions where the former encourages the latter to act, and finally, sanctioning is the loosest of the relationships, where the state knows of the activities of the proxy but turns a blind eye to its activities.

3 Russia and Cyber Criminals

Today, Russia cannot measure up militaristically to the United States. By all measures of power, Russia is lacking. Yet, the Russian state still wants to be a major player on the world stage. The great loss of power post-Cold War has caused the Russian state to become a vindictive, revisionist power. Accordingly, in order to reach some sort of parity with the United States, Russia has chosen to strike back against the US asymmetrically. This includes their worldwide disinformation efforts, arming insurgents against Western-friendly governments, and employing cyber means to weaken opponents (Blank 2017). All this is to say, Russia uses the power of disruption to stay in the game.

Russia is one the main centres of cybercrime in the world today (Kadlecová, 2015). In fact, 85% of Europol's cybercrime cases are against Russian-speaking organized cyber groups (Brewster, 2014). Furthermore, the largest known collection of stolen internet credentials occurred within Russia (Perlroth and Gelles, 2014). Russia is a hub of cybercrime due to legal loopholes in Russian law, low legal enforcement of the laws, and the low cost of cyber services (Kadlecová, 2015). In addition, the high number of Russian students that graduate with degrees in computer science, coupled with low employment opportunities, pushes many Russians into the field of cybercrime. When put against the backdrop of a culture that had to survive during Soviet times by any means necessary, Russians have developed a belief that they gain what they obtain, including through cyber theft (McDougal, 2015).

Under international law, if a party is able to prove that the state provided "instruction," "direction," or "control" to a proxy, then the actions of the cybercriminal can be attributed to

the state. However, if the act is only incidentally or peripherally associated with the state, the aggrieved party cannot prove guilt by the state (McDougal, 2015). That is to say, Russian cybercriminals know that any cybercrime committed against an external target will not be punished, but that an act targeted within Russia will bring down the wrath of the state. Through this practice, the Russian state has defined the cyberspace "rules of the road" within the country.

In terms of cybercrime it is not an international problem, it is a Russian problem. Russia looks the other way while cybercriminals financially weaken its external enemies. This employment of Russian cybercriminals is a low-cost alternative to employing state-grown cyber capabilities (Insights, 2019). Moreover, by employing cyber criminals, the state retains an aura of plausible deniability (Greenberg, 2019). The Russian state can claim it has no idea that Russian cyber criminals were attacking a target, since they are not nominally connected to the state but are rather merely non-state criminal actors.

While there are some cases in which the state and criminals do work hand-in-hand to accomplish an objective, there are many more where the state has no direct interaction with the cybercriminal but instead allows them to continue to function. In some cases where Russian criminals have acted within Russian territory against Russian state interests, these individuals have found themselves jailed, or newly employed by the state to carry out cyber operations (Plesser, 2014; Galeotti, 2017). In fact, there appears to be an negative norm between Russian cybercriminals and the Russian state: (1) do not touch anything in Russia; (2) share anything that you find of interest with the state; and (3) participate whenever Russia needs you for patriotic activities (McDougal, 2015). This norm between the state and the cybercriminal enterprise deflects the latter's operations outside the state without ever formally encountering the Russian state. Furthermore, as long as Russians engaging online do not cross the state, the state allows these sites to remain open and to perpetuate cybercrime (Insights, 2019). Further implicating the Russian state, some of the sites that sell malicious cyber capabilities have a disclaimer that the tool should not target the Russian state (TrendMicro, 2018).

4 A Different Type of Symbiosis: Commensalism

My contention with Maurer is not over type, but of degree, when analyzing the relationship between the Russian state and Russian cyber criminals. As I will argue, the current relationship is not of mutual benefit, but is rather a commensalistic relationship, meaning that one side, the Russian state, gains greatly from the relationship, while the other side, the Russian cybercriminal, is not harmed. Accordingly, my aim is to add to the analysis on the relationship between the Russian state and Russia cyber criminals.

As such, I argue that there is a fourth typology to Maurer's thesis, which I label commensalism. In this relationship, the Russian state may not actually be formally directing the Russian cybercriminal to act, yet the cybercriminal is still implicitly advancing the state's goals. This relationship is a type of symbiotic relationship, and means that one side benefits while the other is not affected. In this case, the commensalistic relationship allows the Russian state to use cybercriminals to drain the resources of other international actors, while no harm comes to the cybercriminals themselves. It is an unequal relationship, where the Russian state simply tolerates the cybercriminals and allows them to use their cyberspace infrastructure cost-free,

because it knows the criminals' self-interested actions are helping the state. Therefore, in this relationship, the Russian cybercriminal is acting within the scope set out by the Russian state. This is a scope more clearly articulated by Russian sovereign internet law, since it essentially means the state can choose to know about a cybercriminal action, should it want to. Put another way, it is a perfect case of plausible deniability.

In what follows, I first detail three updated cases that align with Maurer's thesis. I then provide three additional cases where the state did not overlap with the cyber criminals' actions but did nothing while they committed cybercrimes within Russia's borders against external targets. I conclude with a negative case study where the Russian cybercriminal did not abide by the negative norms set out by the state, and suffered the consequences. I place the latter cases, excluding the negative case study, under the typology of commensalism, since there is an implicit understanding between the Russian state and the cybercriminal, thereby making them a cyber mercenary by any other name.

4.1 Delegation: Evil Corp

In a case of life imitating art, there is now a Russian cybercriminal group named after the fictional antagonist from the TV show "Mr Robot." The FBI accused Evil Corp founder Maksim Yakubets of working both to enrich himself and to steal documents for the Russian government. Yakubets is believed to have worked for the FSB since at least 2017, to acquire confidential documents and conduct cyber-enabled operations in the service of the state (Al Jazeera, 2019). In addition, Yakubets father-in-law is a former officer within the FSB, while his wife sits on a charitable foundation that supports FSB veterans (Dobrynin and Krutov, 2019). The US Treasury Department also accused Yakubets of recruiting cybercriminals to work for the Russian state. When Yakubets was not working for the state, he used his cyber network to steal more than $100 million from companies across the world, but not in Russia. Despite the $5 million reward for the capture of Yakubets, the FBI notes that it is doubtful that he will ever see the inside of a US courtroom, due to the reluctance of the Russians to extradite him, or any other cybercriminal (Al Jazeera, 2019).

This dual-hatted sanctioning relationship is common in Russia cybercrime. The state has many individuals on their payroll who also serve as criminal entrepreneurs. Since Yakubets never criminally acted within Russia, he is not a threat to the state. Thus, he is not a criminal in Russia's eyes and will not be extradited to the US. Moreover, it is likely that Yakubets will be able to use his connections within the FSB to further his criminal activities, and all the while the FSB rides his coattails as he enters restricted cyberspace networks.

4.2 Orchestration: Carderplanet

Roman Seleznev, also known by his hacker name "Track2", is the son of Valery Seleznev, a member of the Russia Duma who holds the equivalent rank of minority whip (Wilber, 2014). Along with Roman Vega, Seleznev established "CarderPlanet", which sold illegal goods online, including stolen credit cards, as well as hacking tools and expertise (Glenny, 2012). CarderPlanet operated between 2009-2011 and cost Western financial institutions over $1.2 million. Vega also established the "Boa Factory" which served as a clearing house for various goods which were acquired through cyber theft, including stolen credit cards and passports (Alperovitch, 2009).

Vega's Twitter profile (which he operates from a US prison) has a large bat as his profile image, to indicate his connection to the Spetsnaz. In this case, the Russian state set out a scope for cybercriminals to act within, that is to say a scope where CarderPlanet was tasked by the state and allowed to become increasingly prolific. The state essentially gave cover to CarderPlanet as they drained millions from Western accounts. This is in line with the orchestration typology laid out by Maurer.

4.3 Sanctioning: Russian Business Network (RBN)

For about two years from 2006-2008 (before going underground), the RBN was responsible for almost 60% of all cybercrime. The RBN specialized in selling identities, botnets, malware, denial of service, phishing, and computer extortion, amongst other crimes. Lending credence to the kleptocratic interdependence thesis, the RBN was created by a 24-year-old known as "Flyman" who was the nephew of a powerful Russian politician, granting him an extra level of protection.

Despite having "Russian" in the site's name, the Russian state has consistently denied that the RBN is a Russian cyberspace crime hub. As a representative from Verigisign commented, the Russian police have not concerned with the RBN it is "putting it to the fat Westerners with too much money" (Warren, 2007; Insights, 2019). The Russian Business Network was so well-protected in Russia that when the FBI went to the country to ask the FSB for help in shutting down the RBN, they were told by the FSB that the RBN did not operate in Russia. After checking the public domains of the RBN, the FBI found that after they had asked the FSB for help all the public domains had been moved to new IP addresses (Carr, 2012). The RBN is also suspected of supporting the GRU during Russia's conflicts with Azerbaijan and Georgia in 2008 (RBNExploit, 2008; Korns and Kastenberg, 2009).

The Russian Business Network, simply by its scale, caught the eye of the Russian State. Once on the radar of the state, the Russians willingly turned a blind eye to the actions of the RBN as it was adversely affecting Russia's international competitors. This is evident in the interaction with the FBI and FSB when they came to ask about the RBN. Also in line with the cyber mercenary thesis, the RBN came to the state's support when required in an international entanglement along Russia's borders.

5 Commensalism

Russia takes no interest in cybercrime organizations operating from within its territory as long as they direct their operations externally. In what follows, I detail three cases that are similar to Maurer's typology; however, these cases differ in that the state has not even shown an interest in the activities of these proxies. The Russian state certainly knows now what these cybercriminals are doing, due to a recent new cyberspace law, enacted in February 2018, which protects its online sovereign rights. This law dictates that everyone, including cyber criminals, must use a state sanctioned virtual privacy network (VPN). Using only approved VPNs allows the state to track its citizens' actions online (Kundaliya, 2019). In addition, the new sovereign internet law requires Russian Internet Service Providers to install deep package inspection tools to locate the source of web traffic and to channel all Russian web traffic through state-controlled exchange points, thereby allowing the state to survey its citizens (Ma, 2019; Rashid, 2019).

My contention is that the Russian state does not even need to monitor all the cybercriminals within its territory. Rather, the state has created a negative norm through acts such as the sovereign internet law, having postings on forums not to use capabilities against the state, and non- prosecution of cybercriminals that operate within Russia. This norm means that the state does not need to turn a blind eye, which would indicate they are aware of the cybercrime. Rather, the state allows cybercrime to continue unabated outside its territory without any government oversight, as it is relatively certain, due to the strength of the norm, that no cybercriminal would be foolish enough to operate against the state.

In a parallel, it is similar to the panopticon, in that the state does not need to actually "man the rotunda" since cybercriminals within Russia are certain that they are being watched at all times. While many of their activities within Russia are most likely monitored, the state does not have the resources to watch all criminal actions being undertaken online. For this reason the state needed to create this powerful negative norm in order to shepherd most of the cybercriminals in the same direction. That said, because of the new sovereign internet law, the state can still check on activities if it thinks someone has strayed outside the norm; the action reinforces the existing norm.

5.1 Commensalism: Infraud

Sergey Medvedev, a Russian national, and Svyatoslav Bondarenko, a Ukrainian national, started "Infraud," which is short for "In Fraud We Trust", in 2010 (Department of Justice, 2018). One of the main precepts of Infraud was that it was "against the rules to buy or sell stolen access devices and other contraband belonging to victims within Russia" (O'Neill, 2018). Using their online forum, Infraud members were able to "purchase, sell, and disseminate stolen identities, compromised debit and credit cards, and financial and banking information" (Radio Free Europe Radio Liberty, 2018). Infraud's members totalled nearly 11,000 people who "targeted more than 4.3 million credit cards, debit cards, and bank accounts around the world" (Radio Free Europe Radio Liberty, 2018). The Infraud scheme "inflicted approximately $2.2 billion in intended losses" (Department of Justice, 2018) and "netted approximately $530 million in illicit profits from financial institutions and individual consumers throughout the world." While 13 members of Infraud were arrested in a multinational takedown in countries such as Australia, France, Italy, Kosovo, Serbia, the United Kingdom and the United States, the Russian government did not provide any support to the US Justice Department in pursuing criminal charges against Russian citizens (Krebs on Security, 2018).

5.2 Commensalism: FIN6

In another instance of Russia taking no interest in a cybercrime operating from within its territory, FIN6 is a group believed to be operating out of Russia (Cimpanu, 2019). The group originally started out with simple payment card theft and has now moved on to selling ransomware (Fire Eye, 2016). FIN6 is believed to have collected about 20 million payment cards worth $400 million from point of sale systems in both the United States and Europe (Osborne, 2018; Ferguson, 2019). FIN6 is also believed to have employed ransomware against Chicago's Tribune Publishing and the Norwegian firm Norsk Hydro, which cost the latter at least $40,000 (Ferguson, 2019).

5.3 Commensalism: GozNym

A final case of Russia allowing cybercrime to operate freely within its territory is GozNym. The malware developed by GozNym (which itself is a Trojan hybrid spawned from Nymaim and Gozi ISFB malware) attacked and stole around $4 million dollars (Stupp, 2019) from more than 24 US and Canadian banks (Kessem and Keshet, 2016). This malware infected 41,000 computers and captured their login credentials to fraudulently access banking accounts. GozNym was installed through a phishing campaign in which thousands of legitimate looking emails with malicious attachments were sent to banks, and once the user clicked on the attachment the malware was able to access the account (SentinelOne, 2019). The Russian malware developer, Vladimir Gorin, and four other Russians charged in the case remain at large due to Russia being unwilling to extradite them to the United States. However, authorities in Georgia, Ukraine and Moldova are working with the United States to bring charges against their nationals involved in the GozNym cybercrime group (Krebs on Security, 2019).

5.4 Failure to Comply with Negative Norms: Maza-In

What happens when a Russian cybercriminal targets financial institutions around the world, including Russia, and when apprehended refuses to work for the Russian state? These individuals flout the negative norm propagated by the state and end up in a Russian prison. In one case, the Russian hacker known as "Maza-In" was apprehended in March 2019 (Insights, 2019) and is serving a 5-year prison sentence for targeting Russians (Shvornev, 2019); one assumes by his heavy sentence that he was also penalized for refusing to work for the state. This assumption is based upon the fact that the crime he was charged with, the 273rd article of the Criminal Code of the Russian Federation, the creation, use and distribution of computer malware, typically carries with it a 3-year sentence (Weekly Geekly, 2019). Moreover, Russian cybercriminals are rarely charged with this crime nor given the recommended sentence (McDougal, 2015). Maza-In, whose identity online is actively debated (Shvornev, 2019), created the Anubis Android banking malware which targeted 188 legitimate banking and financial mobile applications (Osborne, 2019).

5.5 Commensalism as Part of the Cyber Mercenary Thesis

Maurer does an exceptional job in detailing his cyber mercenary typologies: delegation, orchestration, and sanctioning. However, he is missing a typology: commensalism. According to Maurer, his work is an attempt to detail the relationships between cyberspace actors and states. As mentioned above, he defines this relationship as "an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect." In laying out his typologies, he neglects to mention one relationship: the unstated relationship between states and cybercriminals in which the latter knows the rules of the road and does not formally interact with the state.

As detailed in the three cases above, a cybercrime is not a cybercrime in Russia if it is committed outside the Russian state against external enemies. Further enabling these Russian cybercriminals, the Russians do not have an extradition treaty with the United States and are less than forthcoming when approached by the FBI or the Secret Service to investigate cybercrime. These circumstances create conditions where the Russian state does not have ties to these cybercriminals, but rather allows them to conduct their activities untroubled by the Russian state. That is to not to say that these groups may not one day move into a different

typology and have a closer relationship with the state. It is to say that at this time the cybercriminals know that the state has no interest in prosecuting them as long as their activities harm external enemies.

Moreover, by channelling Russian cybercriminals into acts outside the state and against Russian foes, the Russian state can employ the ultimate version of plausible deniability. This benefit works both ways in that the cybercriminal, if caught, has no idea of any larger plan by the state; if the cybercriminal were to be apprehended, he could not inform on the state since he is not working for it. Rather, the cybercriminals are working towards their own self-interest, which just happens to align with the state's interest. Conversely, the state can claim that it had no interaction with the cybercriminal and therefore the act was not committed on behalf of the state.

In addition, by relying on the negative norm and not directly employing cyber actors, the Russian state is granted flexibility, all the while keeping costs low. In fact, the techniques and tools that a cybercriminal uses may not be all that different from the methods used by the state. In such a case, using a cybercriminal may be just as good as using a Russian state hacker, but at a fraction of the cost. This is due to the competitive market for cybercrime in Russia, which keeps prices down. When compared to keeping a permanent government employee on the books, including the training and upkeep of their skillset, it is much cheaper to allow cybercriminals to carry out their operations, especially if you do not have to pay them to weaken your enemies.

Finally, in the West cybercrime is artificially separated from warfare, meaning Russian actions never rise to the level of military operations against an adversary. Therefore, the Russian state can continue to escalate its operations against the West without fear of military reprisal. Using cybercriminals in this hybrid approach to warfare allows Russia to operate in the grey zone between peace and war – all the while, over time, weakening the West.

6 Conclusion

This study's theoretical argument, which extends Maurer's (2018) theory of cyber mercenaries, begins with the assumption that it is valuable for states, in this case Russia, to employ cyberspace proxies on behalf of the state in order to retain plausible deniability. Operating within Dark IR, Russia is able to conduct operations that are not typically addressed within the international system, as this system is typically the domain of states. By implicitly employing cybercriminals and creating a negative norm in which they can prosper, states cannot bring formal charges against the Russian state nor claim that Russia's actions rise to the level of war.

By adding a new typology to Maurer's cyber mercenary thesis, scholars and practitioners alike can re-frame what Russia is doing in the international system today. This re-framing should cause states, in particular the West, to look into the shadows of where the Russian state is not formally operating. This is the space where Russian cybercriminals are conducting operations retribution-free. By calling out this negative norm, the West can begin to re-conceptualize the false distinction between crime and national security. The implications of this re-framing should more broadly shape the proper way to address cyber criminals and the states that do not stop them. Ultimately, it should cause states to stop operating by the old rules of war and instead look to how states are supplanting conventional warfare with hybrid

warfare, including cybercrime (McFate, 2019). If the West does not realize that the ground is shifting beneath them in the international system and that revisionist actors are employing cybercrime as a hybrid capability, then the US will continue to miss out on a whole spectrum of warfare within GPC.

7 References

1. Al Jazeera (2019). Russian 'Evil Corp' hackers charged by US in $100m cyber theft. *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2019/12/russian-evil-corp-hackers-charged-100m-cyber-theft-191206054758063.html.
2. Alperovitch, D. (2009). Fighting Russian cybercrime mobsters: report from the trenches. Presented at Black Hat USA 2009. Retrieved from: http://www.blackhat.com/presentations/bh-usa09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf
3. Applegate, S. D. (2011). Cybermilitias and political hackers: Use of irregular forces in cyberwarfare. *IEEE Security & Privacy*, 5, 16-22.
4. Blank, S. (2017). Cyber war and information war a la russe. *Understanding Cyber Conflict: Fourteen Analogies*, 1-18.
5. Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. (2014). Organizations and Cybercrime: An Analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*. 8. 1-20.
6. Brewster, T. (2014). Trouble with Russia, trouble with the law: inside Europe's digital crime unit. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/apr/15/european-cyber-crimeunit-russia.
7. Carr, J. (2012). *Inside cyber space: mapping the cyber underworld*. 2nd ed. Sebastopol: O'Reilly.
8. Cimpanu, C. (2019). Cybercrime group FIN6 evolves from POS malware to ransomware. *ZDNet*. Retrieved from https://www.zdnet.com/article/cybercrime-group-fin6-evolves-from-pos-malware-to-ransomware/.
9. Connell, M. and Vogler, S. (2017). Russia's Approach to Cyber Warfare. *Center for Naval Analyses Occasional Paper*. Retrieved from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.
10. Department of Justice (2018). Thirty-Six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes. Office of Public Affairs. Retrieved from https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible.
11. Dinniss, H. (2013). Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War. In *International Humanitarian Law and the Changing Technology of War* (pp 251-278). Brill Nijhoff.
12. Dobrynin, S. and Krutov, M. (2019). In Lavish Wedding Photos, Clues To An Alleged Russian Cyberthief's FSB Family Ties. *Radio Free Europe Radio Liberty.* Retrieved from *https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.html.*
13. Ferguson, S. (2019). Report: FIN6 Shifts From Payment Card Theft to Ransomware. *Bank Info Security*. Retrieved from https://www.bankinfosecurity.com/report-fin6-shifts-from-payment-card-theft-to-ransomware-a-12358.

14. Fire Eye (2016). Follow The Money: Dissecting The Operations Of The Cyber Crime Group Fin6. *Fire Eye Special Report*. Retrieved from https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf.

15. Galeotti, M. (2017). Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe. *London: European Council on Foreign Relations*.

16. Glenny, M. (2012). *Dark Market*. London: Vintage Books.

17. Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

18. Greenhill, K. (2009). Kleptocratic Interdependence: Trafficking, Corruption, and the Marriage of Politics and Illicit Profits. In APSA 2009 Toronto Meeting Paper.

19. Insights (2019). Russia's Most Dangerous Cyber Threat Groups. *Insights*. Retrieved from https://wow.intsights.com/rs/071-ZWD-900/images/RussianAPTs.pdf.

20. Insights (2019). The Dark Side of Russia. *Insights*. Retrieved from https://wow.intsights.com/rs/071-ZWD-900/images/DarkSideofRussia.pdf.

21. Kadlecová, L. (2015). Russian-speaking cyber crime: reasons behind its success. *Eur Rev Organised Crime*, 2(2), 104-121.

22. Kan, P. (2019). Dark International Relations: When Crime Is The "Dime." *War Room*. Retrieved from https://warroom.armywarcollege.edu/articles/dark-international-relations-when-crime-is-the-dime/.

23. Kessem, L. and Keshet, L. (2016). Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim. *Security Intelligence*. Retrieved from https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/.

24. Korns, S., and Kastenberg, J. (2009). *Georgia's Cyber Left Hook*. Army War College Carlisle Barracks Pa Strategic Studies Institute.

25. Krebs on Security (2018). US Arrests 13, Charges 36 in 'Infraud' Cybercrime Forum Bust. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2018/02/u-s-arrests-13-charges-36-in-infraud-cybercrime-forum-bust/#more-42484.

26. Krebs on Security (2019). Feds Target $100M 'GozNym' Cybercrime Network. *Krebs on Security*. Retrieved from https://krebsonsecurity.com/2019/05/feds-target-100m-goznym-cybercrime-network/.

27. Kundaliya, D. (2019) Russia's new cyber laws will fuel online crime, claims report. *Computing. Retrieved from https://www.computing.co.uk/news/3080270/russia-cyber-crime.*

28. Ma, A. (2019). Russia officially introduced a 'sovereign internet' law to let Putin cut off the entire country from the rest of the web. *Business Insider*. Retrieved from https://www.businessinsider.com/russia-sovereign-internet-law-cut-web-access-censorship-2019-11.

29. Maurer, T. (2018). *Cyber Mercenaries*. Cambridge University Press.

30. McFate, S. (2019). *The New Rules Of War: Victory In The Age Of Durable Disorder*. William Morrow.

31. McDougal, T. (2015). Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker *Culture. Int'l L. & Mgmt. Rev.*, 11, 55.

32. Miklaucic, M., & Naím, M. (2013). The Criminal State. *Convergence: Illicit networks and national security in the age of globalization*, 149-170.

33. O'Neill, P. (2018). DOJ indicts leaders of cybercrime ring that allegedly stole $530 million. *Cyberscoop*. Retrieved from https://www.cyberscoop.com/infraud-doj-arrests-svyatoslav-bondarenko-sergey-medvedev/.

34. Osborne, C. (2018). FIN6 returns to attack retailer point of sale systems in US, Europe. *ZDNet*. Retrieved from https://www.zdnet.com/article/fin6-returns-to-attack-retailers-in-us-europe/.

35. Osborne, C. (2019). Anubis Android banking malware returns with extensive financial app hit list. *ZDNet*. Retrieved from https://www.zdnet.com/article/anubis-android-banking-malware-returns-with-a-bang/.

36. Perlroth, N. and Gelles, D. (2014). Russian hackers amass over a billion internet passwords. *New York Times*. Retrieved from http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amassmore-than-a-billion-stolen-internet-credentials.html?_r=1.

37. Plesser, B. (2014). Skilled, cheap Russian hackers power American cybercrime. *NBC News*. Retrieved from http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-poweramerican-cybercrime-n22371.

38. Radio Free Europe Radio Liberty (2018). US Charges Dozens In Massive Cyberfraud Ring. *Radio Free Europe Radio Liberty.* Retrieved from https://www.rferl.org/a/united-states-cyberidentity-fraud-scheme-dozens-charged/29025980.html.

39. Rashid, F. (2019). A Sovereign Internet Will Not Combat Cybercrime. *Decipher*. Retrieved from https://duo.com/decipher/a-sovereign-internet-will-not-combat-cybercrime.

40. RBNExploit (2008). RBN (Russian Business Network) now nationalized, invades Georgia cyber space. RBNExploit. Retrieved from http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html.

41. Schwirtz, M. and Goldstein, J. (2017). Russian Espionage Piggybacks on a Cybercriminal's Hacking. *New York Times*. Retrieved from https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

42. SentinelOne (2019). GozNym Banking Malware: Gang Busted, But Is That The End? *SentinelOne*. Retrieved from https://www.sentinelone.com/blog/goznym-banking-malware-gang-busted/.

43. Shvornev, A. (2019). Famous Hacker Maza-In will be tried in Stavropol. *CBOE*. Retrieved from https://stv24.tv/novosti/izvestnogo-hakera-maza-in-budut-sudit-v-stavropole.

44. Stupp, C. (2019). International Hacker Group Charged After Stealing Millions. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/international-hacker-group-charged-after-stealing-millions-11558045696.

45. Summers, J. (2017). Countering Disinformation: Russia's Infowar in Ukraine. The Henry M. Jackson School of International Studies, University of Washington.

46. TrendMicro (2018). Russian Underground 2.0. *TrendLabs*. Retrieved from https://documents.trendmicro.com/assets/wp/wp-russian-underground-2.0.pdf.

47. Warren, P. (2007). Hunt for Russia's web criminals. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2007/nov/15/news.crime.

48. Weekly Geekly (2019). Trojan creator Anubis arrested. *Weekly Geekly*. Retrieved from https://weekly-geekly.github.io/articles/442830/index.html

49. Wilber, D. (2014). Russian Charged by US as Hacker Is Duma Member's Son. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2014-07-08/russian-charged-by-u-s-as-hacker-is-duma-member-s-son.

4 Radicalization as a Cause of Terrorism – The Case of Bosnia and Herzegovina

Mile Šikman

1 Introduction

The term radicalization has a broader practical application than a theoretical determination. This is the main reason why this phenomenon is very often understood broadly and vaguely. Such an approach may result in negative effects, especially when it is associated with a socially negative phenomenon such as terrorism[1]. For this reason, it is necessary to offer a clear theoretical concept of radicalization, and subsequently associate it with the concept of terrorism. Thus the criteria for considering a particular process to be socially unacceptable would be established, while at same time avoiding the dangers of misunderstanding certain social processes. In the context of criminal law, this is also necessary because codified behaviours must be prescribed on which coercive measures may be imposed, at the same time guaranteeing human rights and freedoms. Additionally, the issue of radicalization is important in a globalized world where people from around the world are connected and share ideas (particularly via social media and the internet), because the increased connectivity makes it more likely that an individual will be exposed to extremist ideology (by chance or choice) at some point, and also facilitates the exchange of information, propaganda and socialization with other extremists (Hendrickson, 2014, p 2).

Although the initial forms of terrorism (e.g. left- or right-wing terrorism) could have been regarded as radical[2], this phenomenon is generally associated with the global jihadist move-

[1] According to the European Parliament Report (2015), terrorism and religious radicalization are often perceived through the prism of stereotypes, resulting in hate crimes and hate speech driven by racism, xenophobia or intolerance toward different opinions, beliefs or religions. In this respect, it is important to emphasize "that it is the perverse misuse of religion, and not religion per se, that is one of the causes of radicalisation" and "radicalisation is not to be associated with any one ideology or faith but may occur within any of them" (European Parliament, 2015).

[2] Because, according to Simeunović (2009), terrorism, like any other political violence: "can be related to ideology in at least three ways: first, in the sense of the system of value orientations that encourages terrorist activity; secondly, ideology can act as a guide when choosing goals, methods, and types of terrorist activity; and thirdly, ideology justifies what has been done – the interpretive function of ideology" (Simenunović, 2009, p 123).

ment[3] and terrorism which has been manifesting since the 1990s. Specifically, a radical ideology emerged during this period, based on the recruitment of individuals around the world to fight against the proclaimed enemy, be it home or abroad, to achieve the set goals[4] (cf. Hegghammer, 2011, p 73; Kohlmann, 2004). Al Qaeda was the first global terrorist network under whose umbrella radicalized individuals began to gather and commit terrorist acts around the world[5]. Subsequently, this problem escalated when the Islamic State was established in the area of Syria and Iraq, with more than 40,000 people from over 120 countries[6] joining the Islamic State between 2012 and 2017. Even though the method and goal have remained the same (the recruitment of individuals around the world, the formation of a caliphate), terrorism now manifests itself in a much deadlier, more dangerous and brutal way[7]. Finally, according to the latest data by the Institute for Economics and Peace (2019), there has been an increase in terrorist attacks in Afghanistan, suggesting that the Taliban became the deadliest terrorist group in the world during 2018 (Institute for Economics & Peace [IEP], 2019, p 2). Thus, we currently have a paradoxical situation – although the Islamic State's caliphate has collapsed in Iraq and Syria, and the influence of al Qaeda has been completely weakened, there may now be four times as many jihadists as there were in 2001[8] (Clarke, 2018). This suggests that "the global jihadist movement is alive and well, even if it is currently more fractured and atomized than at any point in recent memory" (Ibid., 2018). As a result, the concept of radicalization as a cause of terrorism is widely used to refer to the process of individuals joining extreme and violent movements, with an emphasis on the recruitment and mobilization to the cause of global jihad (Meleagrou-Hitchens and Kaderbhai, 2017 p 13).

---

3 Daniel Byman has written a book on the global jihadist movement entitled *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know*, which was published in 2015 by Oxford University Press (Byman, 2015).

4 According to Jason Burke (2009): "In 1987, when Abdullah Azzam, the leading ideologue for modern Sunni Muslim radical activists, called for al-qaeda al-sulbah (a vanguard of the strong), he envisaged men who, acting independently, would set an example for the rest of the Islamic world and thus galvanize the *umma* (global community of believers) against its oppressors" (Burke, 2009). This is actually the essence of the global jihadist movement ideology and the main reason why it has existed for over 30 years.

5 Foreign terrorist fighters are known to have been in Afghanistan during the Soviet occupation. Thereafter, they participated in conflicts in BiH (1992-1995), Somalia (1993-2014), Chechnya (1994-2009), Afghanistan (2001-2014), and Iraq (2003-2012) (Schmid, 2015, p 3). At the same time, al-Qaeda members carried out individual terrorist attacks, such as a suicide attack against the US Embassy in Kenya and Tanzania in 1998 (more than 200 casualties), the terrorist attack on the United States in 2001 (2977 casualties), the 2002 Bali terrorist attack (202 casualties), the 2004 Madrid terrorist attack (192 casualties), the 2005 London terrorist attack (52 casualties), the 2015 Paris terrorist attacks (130 casualties), the Nice terrorist attack (86 victims), and so on (see more: SINCE 9/11, n.d.).

6 According to the United Nations reports, the Islamic State, as part of its overarching aim to build a global Islamic caliphate (ISIL), has announced the establishment of a number of provinces outside Iraq and the Syrian Arab Republic (in the Middle East: Libya, Yemen, Egypt-Sinai and Saudi Arabia and beyond: North Caucasus, Algeria, Nigeria and on the Afghanistan/Pakistan border), while more than 50 terrorist groups around the world have pledged allegiance to ISIL (United Nations Office On Drugs And Crime [UNODC], 2018, p 5).

7 Additionally, the Islamic State has demonstrated capabilities that al-Qaeda never possessed: forming state governments in large areas inhabited by millions of people (Bunker and Dilegge, 2016).

8 The total number of jihadists is currently estimated at 230,000 militants spread across approximately 70 countries, with the lion's share currently located in Syria, Afghanistan, and Pakistan (Clarke, 2018). The number of them in Europe is not negligible; for example, according to estimates by the European Commission, in France, the United Kingdom and Germany alone, there are more than 51,000 radicalized individuals who pose a potential security threat (European Commission, 2018, p 1).

The literature on radicalization and terrorism is quite extensive and diverse[9]. It ranges from viewpoints that radicalization is a process which has a direct causal relation with terrorism (Laqueur, 1999; Hegghammer, 2011; Kohlmann, 2004; Burke, 2009), through viewpoints that the concept of radicalization has been misused in order to draw attention away from the real causes of terrorism, such as poverty and Western foreign policies (Kundnani, 2012; Silva, 2018), to viewpoints that the concept of radicalization should be replaced with another concept, for example, "fanaticism" as an introduction to terrorism (Schuurman, Taylor, 2018: 14). It could therefore be said that the concept of radicalization follows the fate of terrorism with regard to the conceptual definition (Lalić and Šikman, 2018). Unquestionably, radicalization always manifests itself at the level of attitudes[10], and it does not necessarily have to result in violence, whereas terrorism always results in terrorist behaviour (Marret et al., 2013, p 125). It is for this reason that these different viewpoints must be taken into consideration when considering such a complex issue as the impact of radicalization on terrorism.

The aim of this paper is to examine the theoretical concept of radicalization and to determine the extent to which this factor has contributed to the manifestation of specific forms of terrorism in BiH. The terrorist attacks carried out in BiH, and the BiH citizens who leave for Syria and Iraq to become foreign terrorist fighters are examined. Thus, this paper continues to deal with these issues based on previous research results (see more: Šikman, 2018; Šikman, 2016).

2 The Theoretical Concept of Radicalization

In the most general sense, *Leksikonu stranih reči i izraza*[11] (2002) defines the term *radicalism* (Lat. radicalis) as "rootedness, thoroughness, complete consistency in advocating understanding or the implementation of a programme", while the term *radical* (Lat. radicale) is defined as "radical, complete, fundamental, deep-rooted" (Vujaklija, 2002, p 772). Similarly, *radicalization* is defined in the Oxford Dictionary as "'the action or process of making somebody more extreme or radical in their opinions on political or social issues" (Oxford University Press, n.d.). However, even though it is generally used in a negative sense when describing the process leading to terrorism, the concept of radicalization may also be used in a positive sense.

In this sense, it corresponds to the term *extremism* (Lat. extremus) used to denote "immoderacy, intransigence, irreconcilability (regarding an attitude or viewpoint)" (Vujaklija, 2002, p 268). Although the term extremism is encountered in culture, sports, art, and religion, its destructiveness is most pronounced in the area of politics (Đorić, 2012, p 47). *Extremism* is often described as the end result of the process of radicalization, whereas violent extremism is described as the acceptance of, and involvement in, violent activity as a result of radical or extremist views (Hendrickson, 2014, p 2; Bjelopera, 2013, pp 11-12); hence the connec-

[9] The best review of the selected literature on radicalization and deradicalization in the context of terrorism was provided by Eric Price and Alex P. Schmid in the journal *Perspectives on Terrorism* Vol. 4, No. 2 (May 2010) (see: Price, Schmid, 2010), while in their paper entitled "The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization into Violent Extremism", Matteo Vergani, Muhammad Iqbal, Ekin Ilbahar and Greg Barton presented the findings of the first systematic scoping review of scientific literature on radicalization into violent extremism, obtained between 2001 and 2015 (Vergani et al., 2018).

[10] Scholars such as Peter Neumann (2013) emphasize that: "'the principal conceptual fault-line is between notions of radicalization that emphasize extremist beliefs ('cognitive radicalization') and those that focus on extremist behaviour ('behavioural radicalization')" (Neumann, 2013: 873).

[11] Lexicon of Foreign Words and Phrases.

tion between radicalization, extremism and terrorism, as a distinct form of political violence. The term "connection" is used because it clearly distinguishes these phenomena (radicalism, extremism, terrorism), but at the same time a certain causality may be found. Finally, the concepts of fundamentalism and fanaticism are also mentioned within the conceptual-categorical apparatus closely related to radicalization as a cause of terrorism. *Fundamentalism* (Lat. fundamentum) is predominantly related to religion and signifies a tendency to return to the fundamental postulates of that religion within certain religious teachings (Đorić, 2012, p 50). Thus, fundamentalism explains the phenomenon of violence caused by religious teachings, with the addition of the term religious fanaticism[12]. *Fanaticism* (Lat. fanum) is also one of the terms related to religion, which is used to explain the behaviours leading to terrorism (see: Laqueur, 1999), particularly some of its forms such as suicide terrorism. Specifically, fanaticism provides a behavioural perspective on whether and when extremist beliefs can lead to terrorist violence, a key element in distinguishing it from radicalization (Schuurman and Taylor, 2018, p 13). Thus, radicalization is a term which is not synonymous with related concepts, because it differs from them in certain elements. These terms should not be confused because religion-based terrorism (as a form of extremism) or religious fanaticism is not the same as the process of radicalization leading to terrorism. Therefore, Randy Borum rightly argues that radicalization, or more precisely, involvement in terrorism, can best be seen as a set of different processes (Borum, 2012). This is also the first issue that needs to be clarified with regard to radicalization as a cause of terrorism.

The academic debates on this notion, which are, as already stated, quite divergent[13], have influenced the institutional framework of radicalization as a cause of terrorism in many respects. In defining the concept of radicalization, the United Nations generally refers to academic opinions on this issue[14]. Additionally, the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2016a), paragraph 14, states that "a further conceptual challenge relates to our understanding of the "radicalization process" through which individuals adopt violent extremist ideologies that may lead them to commit acts of terrorism, or that make them vulnerable to recruitment by terrorist organizations" (United Nations [UN], 2016a: 6). A more detailed approach to the conceptualization of radicalization was given by UNDP (2015), stating that the participants at the 2015 Nairobi Ministerial Conference arrived at an agreed view, which reads as follows: "Radicalization is a process marked by departure from generally accepted social norms and values; the objective of those using radicalization as a tool is to pressure others to subscribe to the worldview itself. The methods used to convert others to the same worldview may take a coercive form, including outright violence. Radicalization is a phenomenon characterized by aggressive and exclusive imposition of one's identity on others, consequently constraining or denying space for the expression of other identities. The uncompromising imposition of one belief system onto another through violent means characterizes processes of radicalization that lead to violent extremism. This form of absolutism requires compliance (with

[12] Thus, in addition to religious fundamentalism, violent-terrorist connotations are emphasized to create a social opinion that religious communities play a major role in these acts and should be viewed and condemned as such. This is why we accept some scholarly opinions that the terms "religious" and "fanaticism" can in no way be placed under the same umbrella (Nimac, Ćurković-Nimac, 2014: 126).

[13] Many academic definitions of the term radicalization can be found in the literature. One definition was proposed by Randy Borum in his paper entitled "Radicalization into Violent Extremism I: A Review of Social Science Theories", including certain criminological theories that may be helpful in studying this research problem (Borum, 2012b).

[14] For example, see Report on Best Practices and Lessons Learned on how Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism (2016b), Chapter III: "Domestic Law and Policy Developments in the Area of Preventing And Countering Violent Extremism" (UN, 2016b: pp 7-10).

no exception). Radicalization can manifest itself in the form of physical violence, in systems (including laws, regulations, etc.) and the broader denial of rights. It is largely context-specific and, therefore, subject to local driving factors which contributes to the challenge of establishing a common definition" (United Nations Development Programme [UNDP], 2015: 3). The European Union determines radicalization as "a phased and complex process in which an individual or a group embraces a radical ideology or belief that accepts, uses or condones violence, including acts of terrorism within the meaning of the Directive on combating terrorism, to reach a specific political or ideological purpose" (European Commission, n.d.). The Council of Europe (2016) Guidelines for Prison and Probation Services Regarding Radicalization and Violent Extremism define violent extremism "as behaviour promoting, supporting or committing acts which may lead to terrorism and which are aimed at defending an ideology advocating racial, national, ethnic or religious supremacy. This may include the violent opposition to core democratic principles or values. Radicalization to violence is the dynamic process whereby an individual increasingly accepts and supports violent extremism. Indicators of violent extremism exist. These are evidence-based behaviours that reveal an increasing commitment to an ideology that supports the use of violence, the increasing intention to act in a violent manner to achieve ideological goals and/or actual participation in unlawful violent action in support of political, religious, social or other ideological objectives'' (Council of Europe, 2016, p 9). Finally, it is worth mentioning the Organization for Security and Co-operation in Europe, which has embraced the concept of terrorist radicalization to mean "a process whereby an individual comes to accept terrorist violence as a possible, perhaps even legitimate, course of action" (Organization for Security and Co-operation in Europe [OSCE], 2014, p 21).

In order to answer the question of radicalization as a cause of terrorism, taking into account the above points, we may conclude that there are three common denominators related to the concept of radicalization. First, we agree that radicalization is an individual and systemic, social-psychological process consisting of adopting particular attitudes and beliefs based on extremist views. As such, this process has its own timeline: the moment when it occurs, the time of manifestation and the phase when it ends (cf., Borum, 2012c, p 58). Terrorist radicalization is a dynamic process: it may be accelerated, possibly slowed down and in some cases reversed (OSCE, 2014, p 37). However, this is not a linear process; the transition from one stage to the next is individual and depends on a number of circumstances. In this case, the focus is on those conceptualizations of radicalization that see it as a cognitive process of increasing adherence to radical views which is then implicitly or explicitly tied to involvement in terrorism (Schuurman and Taylor, 2018, p 13). Specifically, many individuals may have radical ideas, but the vast majority of them never act on them (Moskalenko and McCauley, 2009, p 257; Borum, 2012a, p 2). The transition from radical to terrorist is often a matter of a number of circumstances, which is why, according to Brian Jenkins, there is no easily identifiable terrorist-prone personality, nor is there a single path to radicalization (Jenkins, 2010, p 7). The key difference is the adoption of views that violence is a justifiable way of achieving goals. Following the model used by Sophia Moskalenko and Clark McCauley, we can draw a distinction between an individual's willingness to engage in legal and non-violent political action (activism), and an individual's willingness to engage in illegal and violent political action (radicalism)[15] (Moskalenko and McCauley, 2009). In this sense, we are discussing ter-

[15] Sophia Moskalenko and Clark McCauley published a paper in 2009 entitled *Measuring Political Mobilization: The Distinction Between Activism and Radicalism*, which addressed willingness to participate in legal and non-violent political actions in relation to willingness to participate in illegal or violent political actions. They reached the conclusion that a smaller number of radical activists have the intention or willingness to pursue their goals by violent means (Moskalenko and McCauley, 2009, p 257).

rorist radicalization, which differs from other forms of radicalization (including those with a positive meaning).

Secondly, radicalization must be aimed at pursuing the goals of a terrorist organization, including terrorist-related behaviours (recruitment for terrorism purposes, terrorist training, and the like). Thus, the process of radicalization does not only refer to the adoption of views and beliefs that justify violence, but also to a process which imposes and shapes such views (Borum, 2012a, p 2). It is always an interactive process (even with the minimum degree of interaction) between individual and external influences, including those inciting terrorism and those seeking to recruit others for terrorism. The terms "self-directed" or "self-initiated" radicalization are often used when there is a minimal degree of interaction with people actively seeking to radicalize them (OSCE, 2014, p 38). Vergani et al. point out the need to focus more on the interaction between push, pull, and personal factors, both cognitive and behavioural radicalization and specific conditions that develop the occurrence of different types of these factors in certain contexts (Vergani, Iqbal, Ilbahar, & Barton, 2018).

Thirdly, in accordance with the multifactorial approach to explaining crime, including terrorism, other factors (external and internal) leading to behaviour referred to as terrorism should be considered. To accept radicalization as the only cause of terrorism, which is sometimes referred to as "mainstream" radicalization, is not only wrong, but also overstates the explanatory potential of this phenomenon while leaving other causes underemphasized (Schuurman and Taylor, 2018, p 13). Additionally, the process of radicalization itself is multi-fold; it is triggered and sustained by more than one cause (Borum, 2012c, p 57). Radicalization involves both internal and external factors, and the causes of radicalization can be equally socio-economic, ideological, personal or psychological[16], as well as a number of other components, including, for example, socialization with the group (Hendrickson, 2014, p 2). These triggers are complex, multi-fold, interconnected, and closely linked to structural elements of the environment, which may favour radicalization and eventual violent extremism (UNDP, 2016). Therefore, radicalization should be understood as a complex phenomenon including individual, group, and societal level dynamics (Ozer, Bertelsen, 2018, p 654), depending on the circumstances surrounding each individual case.

3 Radicalization in Bosnia and Herzegovina

Radicalization in BiH began in the early 1990s, with the outbreak of the 1992 conflict, and has continued through at least three stages (see more: Šikman, 2018, p 121). The first was marked by the arrival of foreign terrorist fighters from Afghanistan and other countries (Egypt, Syria, Yemen, and so on) who, driven by the idea of global jihad, fought in the 1992-1995 war in BiH[17] while actively spreading the radical fundamentalist ideology known as the global jihadist movement[18]. These were the first instances of radicalization through this ideology in

[16] According to Keiran Hardy (2018), the predominant causes of radicalization, though not pure types (e.g. overlapping political and ideological causes) can be divided into ideological (e.g. demonizing enemies, promising heroic merit), psychological (the lack of self-esteem or sense of identity), social (group dynamics), political, economic and technological (spreading terrorist propaganda via the internet) (Hardy, 2018, p 82-90).

[17] During 1992, they acted independently, and from mid-1993 as the squad "El Mujahid" as part of the 3rd Corps of the BiH Army, headquartered in Zenica (cf. Lučić, 2001, p 127; Šikman, 2018, p 122).

[18] This was done within training which also included the religious education of local people who joined them. Additionally, as Edina Becirevic states, "the Salafi ideology that arrived in Bosnia during the war was more rigid than the version that spread in Western European countries, and even more rigid than the version preached in Saudi Arabia, the home of Salafism" (Bećirević, 2016, p 36 as cited in Šikman, 2018, p 123).

Europe (Kohlmann, 2004), which, among other things, manifested the aggressive imposition of their views and behaviour publicly, as well as intolerance towards members belonging to the same religion (Lebl, 2014, pp 4, 13). The second stage (1995-2012) included the establishment and development of radicalization among the local population, and the formation of the first Salafi communities in isolated and remote villages, to which BiH citizens gradually began to arrive[19]. Finally, the third stage (2012 to date) was characterized by BiH citizens leaving for Syria and Iraq to join the ISIL and participate in terrorist activities (Šikman, 2018, pp 121-125).

Each of these stages is characterized by a pronounced process of radicalization, based on the concept described in the previous section. In terms of the manifestation of radical views (behavioural component) and the commission of specific terrorist acts, radicalization was first manifested at the attitudinal level (cognitive component) and then at the behavioural level. Each of these cases was caused by a different set of circumstances and the offenders' personal characteristics in specific cases.

The following section gives a brief overview of the offenders of terrorism offences, with reference to the degree of their radicalization (cf. Šikman, 2018; Šikman, 2016). Due to the limited space, other characteristics, such as the age of the offender, family and personal circumstances, or social status will not be addressed. In order to gain a deeper insight into the problem of radicalization, it would certainly be necessary to consider these factors as well, so the research results may be regarded as only partial.

3.1 The Offenders of Terrorism Offences in Bosnia and Herzegovina

Although foreign fighters – mujahideen – were involved in numerous incidents following the Bosnian war, the first terrorist attack was carried out in Mostar in 1997, when a car bomb was activated in the city district[20]. Three foreign nationals (from Saudi Arabia, Bahrain and Yemen), who came to BiH led by the global jihad ideology and were directly linked to al-Qaeda, were charged with this terrorist attack. Although charged with terrorism, they were actually convicted of the offence of endangering the public on the basis of a reduced charge (Lucic, 2001, p 133), which does not detract from the fact that they acted as radicalized individuals in order to achieve the global goals of the jihadist movement. This is further supported by the fact that, following this attack, the first defendant managed to escape from BiH[21]. However, he was arrested in Pakistan in 2001 and extradited to the United States and was detained at the military base in Guantánamo Bay. The second defendant stated that he, being a member of al-Qaeda, completed military training in Afghanistan and arrived in BiH in 1992 as a fighter in the El Mujahid Detachment, subsequently promoted to company commander (Glavonjic, 2009). The third defendant was wanted by the Italian judiciary for the offence of terrorism, but the domestic courts rejected his extradition and he was subsequently released (Lucic, 2001, p 132).

One of the terrorism proceedings was conducted in 2001 at the Supreme Court of the Federation of Bosnia and Herzegovina (FBiH), in the case of the "Algerian Group" made up of six

[19] The BiH government authorities identified their activities as a method of spreading radical religious ideology and recruiting new supporters, therefore characterizing them as the epicentre of extremism and radicalism (Ministarstvo bezbjednosti Bosne i Hercegovine [MB BiH], 2017, p 30).

[20] In this terrorist attack, 50 people were injured and substantial material damage was caused (a large number of parked vehicles were damaged, including the surrounding housing units).

[21] On 7 August 2007, on the order of the Municipal Court in Žepče, an international arrest warrant was issued for the commission of terrorism offence, Article 146, Paragraph 1 of the former FBiH Criminal Code (see: Federalna uprava policije, n.d.)

Algerian nationals[22]. Acting as an organized terrorist group and in coordination with an al-Qaeda terrorist network officer, they were accused of jointly attempting to carry out a terrorist attack against the facilities and staff of the US Embassy in Sarajevo (Hecimovic, 2001). Since the FBiH Supreme Court did not have sufficient evidence to conduct criminal proceedings against them, they were handed over to the US Government which transferred them to Guantánamo Bay in January 2002, where they were held as enemy combatants[23]. On being released from prison, they were returned to BiH (Šikman, 2018).

The next incident occurred in 2002, in the village of Kostajnica near Konjic, when a member of the Salafi community, motivated by ideological and religious fanaticism, committed a triple homicide and attempted a fourth. Although he was charged with the offence of aggravated murder, rather than the offence of terrorism, the more serious charge was applied because the offence was committed for ideological and religious reasons[24]. As a result, the defendant was sentenced to 35 years' imprisonment by the Mostar County Court.

Subsequently, in 2005, two defendants arrived in Sarajevo from Sweden and Denmark, with the intention of carrying out a terrorist act in BiH or another European country to force the BiH authorities or the other country's government to withdraw their forces from Iraq and Afghanistan. Thereafter, they contacted a third defendant who had procured explosive substances (about 20 kilograms) which they used to prepare a so-called "suicide belt" (ready to be activated). They videotaped all this and recorded an audio message announcing the attacks[25]. This suicide terrorist attack was prevented, and in 2007, the defendants were convicted of the offence of terrorism before the Court of BiH (see more: Šikman, 2016, p 169). As noted in the court judgment, the defendants were also in contact with radicalized individuals who had criminal proceedings for terrorism pending against them in their home countries. The defendants maintained contact with these individuals via the internet from BiH, and their intent to commit a terrorist act was clear (Court of Bosnia and Herzegovina [Court of BiH], 2007, p 49). Their loyalty to radicalism is evidenced by the fact that the first defendant, after serving his prison sentence, attempted to join the Islamic State in Syria and Iraq, while the third defendant succeeded and became a member of the Al-Nusra terrorist organization[26].

---

22 These people arrived in BiH in the period between 1992 and 1997 and they had BiH citizenship. One of them was a member of the El Mujahid Detachment, while the rest came to BiH after finishing their job, as "Islamic missionaries" (Hećimović, 2001).

23 The importance of this anti-terrorist action is demonstrated by the fact that the US President, in his speech to sessions of Congress, praised the cooperation of the BiH authorities in the fight against terrorism and invited other countries to follow this example (Azinovic, 2004, p 91).

24 In the documentary "Blood Delicts" shown on Federal Television, the defendant stated the following: "They ruined our Bajram, I know how I felt at the time, so I decided to ruin their Christmas Eve", on the basis of which it was concluded that this crime was motivated by national and religious hatred, which adds substantial weight to this crime (Federalna televizija, 2019).

25 According to the judgment of the Court of Bosnia and Herzegovina, the audio recording contained the following message: "Allahu Ekber. This is where the brothers are preparing for the attacks. They show us things they are going to use to attack. These brothers are ready to attack and, inshallah, they will attack Al-Qufar who kill our Muslim brothers in Iraq, Afghanistan, Shishan, and other countries. These weapons will be used against Europe, against those whose forces are in Iraq and Afghanistan. These two brothers have sold their lives to please Allah, to help their brothers and sisters. They are Muslims. Their hours are approaching. They're ready to attack, so don't think we have forgotten you. We are here and we plan and have everything ready. This is the message for you" (Sud BiH, 2007, p 3).

26 He was one of the first BiH citizens to go to Syria and Iraq to join terrorist organizations. According to the documentary "Terrorist" produced by the Centre for Investigative Reporting, he died fighting for this terrorist organization, while according to the Prosecutor's Office of BiH, he was a commander of the "Jaysh Muhammad Qa'atiba" military unit made up of Bosniaks from the Balkans (Centar za istraživačko novinarstvo, 2019).

Then in 2009, three individuals were accused of plotting terrorist attacks in BiH. As members of the Salafi community, they formed a terrorist group and underwent training in handling and using firearms and explosives; they possessed and prepared components for the production of explosive devices; they owned videotapes showing the magnitude of terrorist attacks around the world; and undertook other actions aimed at committing a terrorist act in BiH between 2007 and 2009. It should be emphasized that while carrying out these activities they acted from the standpoint of ethnic and religious extremism and radicalism, advocating that a Sharia state should be established in BiH[27]. In 2011, the same individuals were convicted of the criminal offence of terrorism at the Court of BiH (Sud BiH, 2011). Additionally, they recruited other people to "fight against the dissenters", propagating that "unbelievers should be killed", while at the meetings, they explained what jihad meant and what their goals were. During searches, the defendants were found in possession of video recordings of combat operations at different locations, files containing propaganda material promoting and justifying the mujahideen's fighting, and promotional video recordings of al-Qaeda's actions (Sud BiH, 2011, p 23).

In 2010, a terrorist attack was carried out near the Bugujno police station. The defendants planted and activated an improvised explosive device close to the Bugojno Police Station building in the early morning hours, which killed a police officer, injured several others, and inflicted damage on the facilities. This case is closely related to a planned terrorist attack, since the defendant participated in meetings discussing Sharia and jihad and the establishment of a Sharia state in BiH[28] (Sud BiH, 2013, p 103). It should be emphasized that in this case the Court found particularly aggravating circumstances on the part of the defendant, which can be regarded as the consequences of his radicalization. Thus, he demonstrated his long-term determination to commit such a serious crime, with the aim of causing graver consequences (by choosing to carry out the attack when a larger number of police officers were present at the police station). Furthermore, the Court found the defendant's behaviour after the offence had been committed (e.g. a threat that the next time there would 9 tons of explosives rather than 15 kilos) and his behaviour toward the injured parties to be further aggravating circumstances, on the basis of which the Court additionally concluded that the defendant was unscrupulous and cruel, who showed no remorse for this tragic act during the course of a three-year trial, and who failed to offer his condolences to the injured parties for the grave and tragic consequences of his act (Sud BiH, 2013, pp 126-127).

In 2011, a terrorist attack was carried out in front of the US Embassy building in Sarajevo by a defendant who was moving in the immediate vicinity of the Embassy building and firing at it with an automatic rifle, subsequently injuring a police officer and inflicting material damage to the Embassy building (see more: Šikman, 2016, p 169). The aim of this terrorist attack was to extort a concession by demanding that NATO forces leave Afghanistan. The defendants were members of the Salafi community in BiH and it was this terrorist act that expressed their dissatisfaction and an attempt to forcibly achieve their goals. They continued to express

[27] The witness in the criminal proceedings against the defendants explained that the purpose of these actions would be "to unite jamaats, to make everything as Allah commands" and "the Mujahideen to fight in the way of Allah"; the aim was "to establish the law of Allah in BiH, that is, the fight to the death until the Sharia State is established" (Sud BiH, 2011, p 60).

[28] This is supported by the statements of witnesses (who practised faith in the same way as the defendant): "That he no longer has to wait, his time is passing and that he is old, that if he waits any longer, he will not be able to do anything for Islam, that something will happen in Bugojno, a punishment from Allah, that this people is pagan and he had repeated that he was going to blow up the police station" (Sud BiH, 2013, p 82).

their views during the course of the trial (e.g. contempt of court[29] or commitment to jihadist ideology[30]), which remained particularly striking during the closing argument of the first defendant[31]. The second defendant was acquitted; he subsequently joined the Islamic State in Iraq and died during a 2014 suicide bombing. The third defendant was also acquitted of the charges and joined a terrorist group in Syria (Šikman, 2018).

In 2015, criminal proceedings were conducted against a defendant charged with the offence of incitement to terrorism. In this case, as stated in the judgment, the defendant was a member of the Salafi community in BiH, which was organized outside the official institutions of the Islamic Community of BiH. During 2013 and 2014, as a religious authority in the Salafi community, he premeditatedly carried out these actions in several BiH cities (Velika Kladuša, Cazin, Bužim, and Gornja Maoča) in order to propagate and spread Islamic radicalism (Sud BiH, 2015, p 2)[32]. Following such a public incitement, the Court found that a large number of the members of the Salafi community in BiH – BiH citizens – left BiH and joined the Islamic State terrorist organizations in Syria and Iraq. While participating in the terrorist activities in Syria and Iraq, they carried out actions with elements of terrorism offences; a number of them died, while others continued to participate in the activities of the terrorist organization they had joined (Sud BiH, 2015, p 4).

In 2015, two terrorist acts were committed: one against Zvornik Police Station, during which one police officer was killed; and the other on personnel of the BiH Armed Forces in Sarajevo, during which two members were killed. In both cases, the offenders of these terrorist acts died (in the first case, the offender was fatally shot during a confrontation with police, while in the second case, the offender committed suicide). Both offenders were members of, or closely related to, the Salafi communities (Šikman, 2016, p 170; Šikman, 2018, p 124).

From mid-June 2017 to 10 April 2018, two defendants planned and prepared the procurement of weapons (a M84 machine gun, hand grenades, ammunition and shells) to carry out terrorist attacks in BiH (against the building of the BiH State Investigation and Protection Agency in Sarajevo, and the building of the Ministry of the Interior of the Tuzla Canton). To this end, the first defendant had repeatedly come into contact with members of the radical Salafi movement in BiH, including the second defendant. After obtaining the weapons to carry out the planned terrorist act, he recorded a video jihad death note and demanded that it be released to the media after the commission of the act (Sud BiH, 2019).

[29] At the beginning of the trial, the defendants refused to stand up, which is a statutory obligation, and they wore caps on their heads, which the Court could associate with clothing details marking religious affiliation. The defendants stated that they honoured only the court of Allah and did not wish to participate in the rituals acknowledging the earthly court of law, confirming that they did not intend to stand up and show respect to a court they did not acknowledge (Sud BiH, 2012, p 24).

[30] In the course of the criminal proceedings, the first defendant demonstrated commitment to the idea, stating the following: "a Muslim fights in the way of Allah, and a non-believer in the way of Shaitan. I am Allah's protégé, you are Shaitan's protégés because you are not Muslims" (Sud BiH, 2012, p 27).

[31] In his closing argument at the trial, the first defendant spoke in a calm voice, in terms of firm beliefs, rather than threat: "Do you really think that you will, if you sentence me to a milder or harsher sentence, this will stop no one. He is prepared to die, he leaves his family, he leaves everything ... do not put everything on my shoulders to stop it, it won't help anyone" (Media Gerila, 2013: 2.36-2.53).

[32] Specifically, the defendant gave speeches at gatherings attended by members of the Salafi community, which were posted on YouTube, and sent public messages aimed at inciting the members of the Salafi communities to join the ISIL organized terrorist group and, as the members of that group, participate in its activities by sending them public messages quoted in the court judgment (Sud BiH, 2015, p 3).

Additionally, through the process of radicalization, a number of BiH citizens have gone to Syria and Iraq since 2012 to join the Islamic State and other terrorist groups. All of them have been indoctrinated with Salafi ideas, either by radical self-proclaimed leaders or via the internet; they advocated the ideas of religious radicalism in para-jamaats and as such went to Syria and Iraq (Shikman, 2018). Some of them took their wives and children to Iraq and Syria and some died in combat, while a number of them returned to BiH. Some of these were charged with terrorism-related offences (the offences of organizing a terrorist group and joining foreign paramilitary and parapolice forces) and tried in BiH (see more: Šikman, 2018). However, this did not diminish the degree of their radicalization, because not only did they disobey government authorities, including the court adjudicating the case, but some of them continued to express radical views, either by radicalizing other prisoners or even by attempting to return to Syria and Iraq (Šikman, 2018, p 132).

The common thread in all the cases of terrorism in BiH is the adherence to the rigid ideology of the global jihadist movement. This thesis is confirmed by the data that individuals who were active members of the Salafi communities in BiH were involved in all terrorist attacks carried out in BiH, expressing views typical of such an ideology (cf. Bećirević, 2016, p 18).

4 Conclusion

Although the concept of radicalization is not theoretically grounded, it may serve to understand the process leading to terrorism. There is a consensus that radicalization as such has two basic dimensions: the first is expressed at the attitudinal level and the second at the level of behaviour. Clearly, the cognitive dimension of radicalization encompasses a broad range of individuals, and many of them will probably never be involved in a terrorist act. However, caution should be exercised, since terrorism today also encompasses public views inciting others to engage in terrorist activities. On the other hand, the behavioural dimension of radicalization means a specific behaviour caused by extremist views. It usually involves the manifestation of violent actions to achieve their goals as a result of the extremist ideas adopted. However, as Marco Nilsson (2018) points out, the causal path may also run the other way, with radical behaviour leading to increasingly radical beliefs: "This exemplifies the complexity of jihadiship as a process whereby ideas merge and problems seeking solutions arise in encounters with new circumstances" (Nilsson, 2018, p 8). This concept also includes the influence of other factors (individual and external) that lead to terrorism in their interaction. If we view radicalization in this way, we can explain some of the behaviours concerning radicalization and terrorism which have manifested themselves in BiH over the past 30 years.

In this respect, it is evident that the process of radicalization in BiH began to manifest itself in the early 1990s with the arrival of foreign nationals to participate in the global jihadist movement. These individuals internalized both the cognitive and behavioural dimensions of radicalization as they actively participated in spreading extremist beliefs, on the one hand, and in using violence as a method of achieving goals on the other. The rigidity of this ideology is supported by the fact that violence was not only aimed at enemies, but also at fellow-nationals who refused to accept the proclaimed views. Radicalization gradually spread and was accepted by a small portion of the local population, who gradually adopted the established patterns of belief and behaviour. This led to the formation of separate communities, organized according to strictly defined lifestyles and activities (the Salafi communities). These communes were

the nucleus of terrorist activity in BiH. This is confirmed by the fact that all terrorist attacks carried out in BiH were perpetrated by members of these communities. Therefore, many international authorities, local authorities in BiH, and court judgments pointed to the danger of these radicalized communities. Moreover, not only has the problem not been resolved, but it has escalated since 2012, resulting in a large number of BiH citizens travelling to Syria and Iraq to join the Islamic State terrorist organization.

Thus, the aforementioned concept of radicalization in BiH is at its peak – the gradual and long-term process of adopting extremist views and beliefs (cognitive radicalization), and the manifestation of specific behaviours, including those which are violent in nature (behavioural radicalization). Additionally, it is manifested through reverse radicalization in such a way that radical behaviour led to the adoption of radical beliefs. The best examples of this are the isolated Salafi communities, which, through the process of "socialization" of new members, created and strengthened their belief in the correctness of their activities. Some of them went a step further and carried out terrorist attacks or joined the Islamic State, thus contributing to the achievement of their set goals.

5 References

1. Azinović, V. (2007). *Al Kai'da u Bosni i Hercegovini: mit ili stvarnost*. Sarajevo: Radio Slobodna Europa.
2. Bećirević, E. (2016). *Salafism vs. Moderate Islam: a Rhetorical Fight for the Hearts and Minds of Bosnian Muslims.* Sarajevo: Atlanska inicijativa. Retrieved January 28, 2018, from http://www.atlantskainicijativa.org/bos/images/2015/dokumenti_i_publikacije/Salafism_vs._moderate_islam-web.pdf
3. Bjelopera, J. (2013). *American Jihadist Terrorism: Combating a Complex Threat*, Congressional Research Service. Retrieved February 19, 2020, from https://fas.org/sgp/crs/terror/R41416.pdf
4. Borum, R. (2012a). Rethinking Radicalization. *Journal of Strategic Security* 4(4), 1-6.
5. Borum, R. (2012b). Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security* 4(4), 7-36. DOI: http://dx.doi.org/10.5038/1944-0472.4.4.1
6. Borum, R. (2012c). Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research. *Journal of Strategic Security* 4(4), 37-62. DOI: http://dx.doi.org/10.5038/1944-0472.4.4.2
7. Burke, J. (October 27, 2009). Think Again: Al Qaeda. *Foreign Policy*, Retrieved February 14, 2020, from https://foreignpolicy.com/2009/10/27/think-again-al-qaeda-4/
8. Bunker, D., Dilegge, R. (2016). *Global Radical Islamist Insurgency: Al Qaeda And Islamic State Networks Focus: A Small Wars Journal Anthology*. Retrieved February 14, 2020, from https://books.google.ba/books?id=3HCdCwAAQBAJ&pg=PT652&dq=Al-Qaeda:+The+True+Story+of+Radical+Islam&hl=sr-Latn&sa=X&ved=0ahUKEwjrp7P--9DnAhWOMewKHf7jBdAQ6AEISzAE#v=onepage&q=Al-Qaeda%3A%20The%20True%20Story%20of%20Radical%20Islam&f=false
9. Byman, D. (2015). *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know.* New York, NY: Oxford University Press.
10. Centar za istraživačko novinarstvo (Novembar 19, 2019). *Terorista*. Retrieved February 14, 2020, from https://www.youtube.com/watch?v=5JZBVuu_kug

11. Clarke, C. (December 11, 2018). The Future of the Global Jihadist Movement After the Collapse of the Caliphate. *The RAND Blog*. Retrieved February 14, 2020, from https://www.rand.org/blog/2018/12/the-future-of-the-global-jihadist-movement-after-the.html

12. Council of Europe (2016). *Council of Europe Handbook for Prison and Probation Services Regarding Radicalisation and Violent Extremism*. Retrieved February 14, 2020, from https://rm.coe.int/16806f9aa9

13. Đorić, M. (2012). Teorijsko određenje ekstremizma, *Kultura polisa*, 9(17), 45-62.

14. European Commission (2018). *High-Level Commission Expert Group on Radicalisation (HLCEG-R)*. Retrieved February 14, 2020, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180613_final-report-radicalisation.pdf

15. European Commission (n.d.). *Prevention of radicalization*. Retrieved February 14, 2020, from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/radicalisation_en

16. European Parliament (2015). *Report on the prevention of radicalisation and recruitment of European citizens by terrorist organisations*, (2015/2063(INI)). Retrieved February 14, 2020, from http://www.europarl.europa.eu/doceo/document/A-8-2015-0316_EN.html

17. Federalna televizija (November 1, 2019). *Krvni delikti*, 01.10.2019. Retrieved February 14, 2020, from http://www.federalna.ba/bhs/vijest/289514/01102019

18. Federlana uprava policije (n.d.). *Ahmed Zuhair – Zbog terorizma*. Retrieved February 14, 2020, from http://www.fup.gov.ba/?p=843

19. Glavonjić, Z. (January 14, 2009). Ali Hamad potencijalni svedok srpskog tužilaštva, *Radio Slobodna Evropa.* Retrieved February 14, 2020, from https://www.slobodnaevropa.org/a/1370074.html

20. Hardy, K. (2018). Comparing Theories of Radicalisation with Countering Violent Extremism Policy. *Journal for Deradicalization,* 15, 76-110. Retrieved February 14, 2020, from http://journals.sfu.ca/jd/index.php/jd/article/view/150/119

21. Hećimović, E. (December 21, 2001). Al Ka'ida u humanitarnoj pomoći, *Dani br. 237*. Retrieved February 14, 2020, from https://www.bhdani.ba/portal/arhiva-67-281/237/t23702.shtml

22. Hegghammer, T. (2011). The Rise of Muslim Foreign Fighters. Islam and the Globalization of Jihad, *International Security,* 35 (3), 53-91.

23. Hendrickson, J. (2014). Counter-Radicalization: Combating Terrorism at the Core: A Study of the Motivations and Inspirational Leaders Behind Radicalization to Violent Extremism and the Programs Designed to Combat Them. *Master Thesis*, Johns Hopkins University. Retrieved February 14, 2020, from https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/38096/HENDRICKSON-THESIS-2014.pdf

24. Institute for Economics & Peace (2019). *Global Terrorism Index 2019: Measuring the Impact of Terrorism*. Retrieved February 21, 2020, from https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2019web.pdf

25. Jenkins, B. (2010). *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001*. Santa Monica, CA: The RAND Corporation.

26. Kohlmann, E. (2004). *Al-Qaida's Jihad in Europe: The Afghan-Bosnian Network*. New York: Berg Publishers

27. Kundnani, A. (2012). Radicalization: The Journey of a Concept, *Race and Class,* 54 (2), 3-25.

28. Lalić, V., Šikman, M. (2018). Teorijski i praktični aspekti koncepta radikalizacije koja vodi terorizmu. In: Ćeranić, P. (Ed), *Regionalna saradnja u suzbijanju prekograničnog kriminala: savremeni izazovi terorizma i migrantska kriza* (pp 47-66). Banja Luka: Fakultet bezbjednosnih nauka Univerziteta u Banjoj Luci.

29. Laqueur, W. (1999). *The New Terrorism: Fanaticism and the Arms of Mass Destruction,* New York: Oxford University Press.

30. Lebl, L. (2014). *Islamism and Security in Bosnia-Herzegovina*. Retrieved February 18, 2020, from https://www.globalsecurity.org/military/library/report/2014/ssi_lebl_140523.pdf

31. Lučić, I. (2001). Bosnia and Herzegovina and Terrorism. *National Security and the Future,* 2 (3-4), 111-142

32. Marret, J. L., Feddes, A., Mann, L. Doosje B., Griffioen-Young, H. (2013). An overview of the SAFIRE Project: A Scientific Approach to Finding Indicators of and Responses to Radicalisation. *Journal EXIT - Deutschland: Zeitschrift für Deradikalisierung und demokratische Kultur*, 1 (2), 123-148.

33. Media Gerila (Febrary 18, 2013). *ZAVRŠNE RIJEČI_JAŠAREVIĆ I OSTALI_ obraćanje optuženog Jašarevica.flv.* Retrieved February 16, 2018, from https://www.youtube.com/watch?v=-vMENz-0zeU&t=279s

34. Meleagrou-Hitchens, A., Kaderbhai, N. (2017). *Research Perspectives On Online Radicalisation A Literature Review, 2006-2016*. Retrieved February 18, 2020, from https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf

35. Ministarstvo bezbjednosti BiH (2017). Informacija o stanju sigurnosti u Bosni i Hercegovini u 2016. godini. Retrieved February 16, 2018, from http://www.msb.gov.ba/PDF/info2017.pdf

36. Moskalenko, S., McCauley, C. (2009). Measuring Political Mobilization: The Distinction Between Activism and Radicalism, *Terrorism and Political Violence,* 21 (2), 239-260, DOI: 10.1080/09546550902765508

37. Neumann, P. (2013). The trouble with radicalization. *International Affairs*,89 (4), 873-893

38. Nilsson, M. (2018). Jihadiship: From Radical Behavior to Radical Beliefs, *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2018.1538092 Retrieved February 18, 2020, from https://www.tandfonline.com/doi/full/10.1080/1057610X.2018.1538092

39. Nimac, D., Ćurković-Nimac, J. (2014). Religija kao socijalni kapital u kontekstu sigurnosne politike suvremenoga europskog društva, *Bogoslovska smotra*, 84 (1), 111-136.

40. Organization for Security and Co-operation in Europe (2014). *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*. Retrieved February 18, 2020, from https://www.osce.org/atu/111438?download=true

41. Oxford University Press (n.d.). *Oxford Advanced Learner's Dictionary*. Retrieved February 18, 2020, from https://www.oxfordlearnersdictionaries.com/definition/english/radicalization

42. Ozer, S. & Bertelsen, P. (2018). Capturing violent radicalization: developing and validating scales measuring central aspects of radicalization. *Scandinavian Journal of Psychology*, 59, 653-660. doi: https://doi.org/10.1111/sjop.12484

43. Price, E., Schmid, A. (2010). Selected Literature on Radicalization and De-radicalization from Terrorism: Monographs, Edited Volumes, Grey Literature and Prime Articles published since 1970. *Perspectives on Terrorism,* 4 (2), 58-76

44. Schmid, A. (2015). *Foreign (Terrorist) Fighter Estimates: Conceptual and Data Issues*. Retrieved January 25, 2018, from https://icct.nl/wp-content/uploads/2015/10/ICCT-Schmid-Foreign-Terrorist-Fighter-Estimates-Conceptual-and-Data-Issues-October20152.pdf

45. Schuurman, B., Taylor, M. (2018). Reconsidering Radicalization: Fanaticism and the Link Between Ideas and Violence, *Perspectives on Terrorism,* 12 (1), 3-22.

46. Silva, Derek M.D. (2018). "Radicalisation: The Journey of a Concept"revisited. *Race & Class,* 59 (4), 34-53

47. Simeunović, D. (2009). *Terorizam*. Beograd: Pravni fakultet Univerziteta u Beogradu.

48. SINCE 9/11 (n.d.). *Terrorism Timeline*. Retrieved February 18, 2020, from https://since911.com/explore-911/terrorism-timeline#jump_time_item_411

49. Sud Bosne i Hercegovine (2019). Presuda S1 2 K 025597 18 K od 4.7.2019. Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/3877/show

50. Sud Bosne i Hercegovine (2015). *Presuda S1 2 K 017968 15 K od 05.11.2015*. Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/3379/show

51. Sud Bosne i Hercegovine (2013). *Presuda S1 2 K 002596 11 K (veza X-K-10/995) od 20.12.2013*. Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/2744/show

52. Sud Bosne i Hercegovine (2012). *Presuda S1 2 K 007723 12 Kod 06.12.2012*. Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/3158/show

53. Sud Bosne i Hercegovine (2011). *Presuda S1 2 K 003342 10 K (veza broj:X-K-09/670-1) od 10.11.2011.* Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/2644/show

54. Sud Bosne i Hercegovine (2007). *Presuda X-K-06/190 od 10.01.2007.* Retrieved February 28, 2020, from http://www.sudbih.gov.ba/predmet/2431/show

55. Šikman, M. (2018). Return of the Foreign Terrorist Fighters – Criminal Persecution and Deradicalization. In: Čaleta, D., Robinson, C. (Eds.). *Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats* (pp 109-136). Ljubljana: Ministry of Defence of Slovenia, Joint Special Operations University from Tampa, USA, and Institute for Corporative Security Studies.

56. Šikman, M. (2016). Foreign Terrorist Fighters – Different Points of View. In: Čaleta, D., Shemella, P. (Eds.). *Comprehensive Approach to Counter Radicalism and Extremism – Future Challenges for Counter Terrorism Process* (pp 161-176). Ljubljana: Institute for Corporative Studies.

57. United Nations Office On Drugs And Crime (2018). *Investigation, Prosecution and Adjudication of Foreign Terrorist Fighter Cases for South and South-East Asia*. Retrieved February 18, 2020, from https://www.unodc.org/documents/terrorism/Publications/FTF%20SSEA/Foreign_Terrorist_Fighters_Asia_Ebook.pdf

58. United Nations, General Assembly (2016a). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/31/65.* Retrieved February 21, 2020, from https://undocs.org/A/HRC/31/65

59. United Nations, General Assembly (2016b). *Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism. Report of the United Nations High Commissioner for Human Rights. A/HRC/33/29*. Retrieved February 21, 2020, from https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/162/55/PDF/G1616255.pdf?OpenElement

60. United Nations Development Programme (2016). *Preventing Violent Extremism Through Promoting Inclusive Development, Tolerance And Respect For Diversity. United Nations Development Programme: A Development Response to Addressing Radicalization and Violent Extremism.* Retrieved February 21, 2020, from https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/conflict-prevention/discussion-paper---preventing-violent-extremism-through-inclusiv.html

61. United Nations Development Programme (2015). *Framing the Development Solutions to Radicalization in Africa.* Retrieved February 21, 2020, from https://www.undp.org/content/dam/rba/docs/Radicalization%20in%20Africa%20-%20summary%20consultation%20report%20-%20Draft%20Final%20Oct.pdf

62. Vergani, M., Iqbal, M., Ilbahar, E., Barton, G. (2018). The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization into Violent Extremism, *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2018.1505686 Retrieved February 21, 2020, from https://www.tandfonline.com/doi/citedby/10.1080/1057610X.2018.1505686?scroll=top&needAccess=true

63. Vujaklija, M. (2002). *Leksikon stranih reči i izraza*. Beograd: Prosveta

5 Addressing Challenges from Cyber Terrorism in Kosovo

Kadri Arifi

1 Introduction

The Republic of Kosovo, as well as the countries of the region and beyond, has faced and is still facing the consequences of violent extremism and terrorism as a result of the spread of extremist ideologies that have affected some of the citizens of the Republic of Kosovo. In spite of practising traditional and moderate Islam in Kosovo, and the resistance of society against these ideologies, vulnerable parts of society, being exposed to them, embraced the idea of political Islam and gradually turned to extremists and began to radicalize their attitudes and actions. This began with intolerant inter-religious discourse, problems within families, incidents at mosques, isolated attacks on moderate imams, hate speech, attempts to influence and control the Muslim community in Kosovo, and efforts for political empowerment and involvement of citizens of the Republic of Kosovo in acts of violence and terrorism at home and abroad. The efforts of Kosovo institutions in the fight against extremism and terrorism have significantly and consistently increased. The Republic of Kosovo, as part of the international coalition against ISIS, has successfully implemented all the responsibilities and obligations arising from membership of this coalition, becoming a very important partner in the global fight against terrorism.

As a result of the measures undertaken by Kosovo's institutions, both in terms of prevention and prosecution, the threats of violent extremism and terrorism have been significantly minimized. "Law enforcement authorities demonstrated adequate capacity to detect and prevent several terrorist plots in Kosovo and abroad. The Kosovo Police Counterterrorism Directorate (KPCT), which is responsible for counterterrorism investigations, increased their investigative capacities by increasing personnel and developing a cyber-counterterrorism unit" (US Department of State, 2019: p 97). However, the phenomenon of extremism and radicalism remains an ongoing challenge for Kosovo's institutions. A number of Kosovo citizens still remain in the zones of conflict in Syria and Iraq, while others have returned through an operation organized by the security institutions. Returned foreign fighters and their family members

have been subject to investigative procedures and prosecuted. In addition to sentencing, at the same time efforts have been made by Kosovo institutions to deradicalize them, including those serving sentences in Kosovo prisons, through various programmes. A complex and long-term project for the rehabilitation and reintegration of people indoctrinated by extreme ideology is in process. The results remain to be seen.

What the author observes is that, even in Kosovo, cyberspace is considered to be a suitable environment for extremists and perpetrators to commit various criminal offences using sophisticated computer tools and software. The main purpose or motive of the perpetrators remains material gain, but there are also other reasons, such as revenge, sabotage, espionage, extremist intentions, and so on. The trend of spread of extreme ideology and Islamic radicalism through the internet is challenging. "Terrorists employ the internet in a variety of ways—both visibly and covertly. While much of the communication, training, planning, and execution of their designs are conducted behind the cloak of invisibility, terrorists also employ the internet as a tool for propagandizing their ideology" (Britz, 2014: p 154). No case of cyber terrorism on a large scale that would endanger the country's critical infrastructure has so far been reported in Kosovo, but whatever the case, the threats from cyber terrorism should never be neglected. "Over time, hackers have proven to cyber security experts that they can be persistent, more creative, and increasingly sophisticated with their attacks. They have learned how to adapt to changes in the IT landscape so that they can always be effective when they launch attacks" (Diogenes and Ozkaya, 2018: p 91). Extremists and radical Islamic groups continue to increase the use of cyberspace to propagate and spread the ideology, promote their activities, recruit new members, facilitate terrorist financing, and take other action in support of terrorism. This is an increasing risk to national security. Protecting critical infrastructure, national assets and cyberspace remains vital, therefore, and should be a priority for Kosovo's security institutions. Addressing the challenges and developing a comprehensive response in combating cyber terrorism is essential.

2 Terrorism as a Continuing Challenge for Kosovo

The start of conflicts in the Middle East, particularly that in Syria and Iraq, activated extremist individuals and groups from Kosovo and the region, who began to recruit and facilitate the deployment of Kosovo fighters to the conflict zones to take part in the fighting, according to their perception of the "holy war" and the "creation of an Islamic state". Initially, the propaganda of terrorist groups was focused through various meetings and religious tribunes with the participation of some radical imams not only from Kosovo, but also from countries in the region, as well as in mosques outside of the Kosovo Islamic Community administration where the role of the religious leaders was performed by self-declared imams with radical convictions. As a result, a large number of young people from Kosovo joined terrorist groups in Syria and Iraq. Consequently, Kosovo continues to face threats and challenges in combating and preventing violent extremism and terrorism.

Completing the legal infrastructure and creating state mechanisms to combat extremism and terrorism, while strengthening security institutions and raising public awareness of the consequences of violent extremism and radicalism has resulted in a reduction in extreme activities. "The response of the institutions of Kosovo brought obvious results in combating the violent extremism and radicalism, especially in advancing the legal infrastructure, creation and func-

tionalization of Institutional mechanisms, the approval of strategic documents, strengthening of operational capacities of security institutions and increasing the international cooperation. Kosovo is a member of the Global Coalition to Defeat ISIS and has taken steps to support the various lines of effort within the limits of its capabilities. It has primarily focused on stemming the flow of foreign terrorist fighters and tracking and restricting financing for terrorist groups" (US Department of State, 2017: p 135).

Law enforcement agencies play a key role in preventing terrorism and extremism. "Kosovo has further stepped up its efforts to fight terrorism, including measures to prevent violent extremism. Since 2016, there have been no new reported cases of Kosovo citizens travelling to the conflicts in Syria/Iraq as foreign terrorist fighters. Since 2012 until today, an estimated 355 Kosovo citizens (256 men, 52 women and 47 children) left for conflict zones in the Middle East, mostly as foreign terrorist fighters. 71 children were born in the conflict zone. 242 Kosovo citizens have returned (124 men, 38 women, 80 children), 96 died (91 killed, 5 died of other natural causes), and 97 remain in the theatre (47 men, 8 women, 42 children). Out of the 242 returnees, 110 of them (4 men, 32 women and 74 children) were returned from the conflict zone in an operation organized by the government in April 2019" (European Commission, 2019: p 38). The police combated this phenomenon in a strategic way, beginning with cooperation at the local level, through Municipal Councils of Community Safety (MCCS) and Local Councils of Community Safety (LCCS), and by playing a vital role in implementing the Strategy on the Prevention of Violent Extremism and Radicalism leading to terrorism for the period 2015-2020. Furthermore, the police played a vital role in the implementation of the National Strategy of the Republic of Kosovo on Preventing and Combating the Informal Economy, Money Laundering, Financing Terrorism and Financial Crimes 2014-2019. "Among the main engagements and activities of the Directorate against Terrorism during 2019 has been the process of return of 110 citizens of the Republic of Kosovo from the area of conflict. An individual risk assessment was conducted for each individual who was in the conflict area, then a list of data of the citizens of the Republic of Kosovo in the conflict area was compiled, and an analytical document explaining the positive and negative aspects, including challenges and threats in the event of the return or non-return of the citizens of the Republic of Kosovo from the conflict area was drafted" (Kosovo Police, 2019: p 13).

However, propaganda and the spread of extremist ideology have undergone changes, focusing almost entirely on the use of the internet and social media. "In the past decade, the internet has been employed in a variety of ways by terrorist organizations. Such use includes, but is not limited to, the following: propaganda, information dissemination, recruiting and fundraising; training; communication; research and planning; criminal activities and money laundering; attack mechanism" (Britz, 2014: p 153). Many of the narratives and much of the propaganda used by terrorist groups in order to achieve their goals, including threats and calls for attacks by leaders of these terrorist organizations, are also translated into Albanian and are easily accessible.

In Kosovo, as in other countries in the region, there have been no large-scale terrorist acts. "Western Balkan countries reported that radicalized communities, some comprising returnees from the conflict zones in Iraq and Syria, existed in their territories and were engaged in recruitment and propaganda activities, but terrorist activities were rarely observed" (Europol, 2019: p 44). Nevertheless, "there are still large gaps in our understanding about how the Syrian conflict will incubate new phases in the development of Salafi-Jihadism. As more docu-

ments and theories emerge, our understanding will grow, particularly as they relate to Islamic State" (Maher, 2016: p 211). Given the relatively large number of returned foreign fighters, those who are still in the conflict zone and could potentially return to Kosovo, the number of foreign fighters convicted and imprisoned, and the continuing spread of extremist propaganda and ideology, extremism and terrorism remain a constant challenge for Kosovo.

3 The Phenomenon of Cyber Terrorism in Kosovo

Along with the challenges of combating the organized crimes of trafficking with drugs, human beings and weapons, money laundering, other forms of organized crime, and terrorism, the phenomena of cyber terrorism as a global challenge is becoming a challenge for Kosovo, as the following quotes detail: "Cyber-terrorism is an increasingly attractive choice for terrorists, because it can be accomplished with only modest financial resources, with anonymity, and from a great distance. Cyber-terrorism has its greatest potential for damage in conjunction with coordinated physical attacks. The prefix cyber is used here because the terrorist attacks or uses technology" (Kosovo National Strategy, 2016: p 7).

"Cyberterrorism may be defined as the premeditated, methodological, and ideologically motivated dissemination of information, facilitation of communication, or attack against digital information, computer systems, and/or computer programs which requires advanced planning and is intended to result in social, financial, physical, or psychological harm to noncombatant targets and audiences; or any dissemination of information which is designed to facilitate such actions"(Britz, 2014: p 152).

"There has been much concern and speculation over the past few years that terrorists could turn to launching cyber-attacks against critical infrastructure. However, while the so-called Islamic State (IS) online propaganda appears technologically advanced and their hackers may be well versed in encrypted communication tools, their cyber-attack tools and techniques remain rudimentary. They still purchase domain-hosting services, downloading software and renting botnets for distributed denial-of service (DDoS) attacks rather than developing their own cyber weapons" (Europol, 2019: p 20).

"Due to the anonymity provided, many criminals may feel more comfortable operating in the darknet market than on the surface web or even in the physical world" (Kremling, 2018: p 236).

"In contrast to the computer-focused crimes discussed thus far, it has been argued that the internet plays a significant and growing role in computer-assisted terrorist offences. In other words, terrorist groups make use of the internet in support of their conventional, terrestrially based activities. Such uses of the internet can be seen to fall into a number of distinct types" (Yar, 2006: p 58).

According to the National Cyber Security Strategy and Action Plan 2016-2019 in Kosovo, the use of Information and Communication Technologies (ICTs) has been spreading rapidly since 2000, and ICTs play important roles in all aspects of life. "Internet penetration in Kosovo is 88.8%, which is similar to the European Union (EU) average, and Kosovar habits in cyberspace tend to be also similar to global trends" (Internet World Stats, 2019). The government organizations which provide services in critical infrastructure sectors such as energy, water re-

sources, health, transportation, communication, and financial services have shifted their daily business onto the internet. These systems improve the quality and the speed of the services being provided, thus helping organizations to work more productively, and contributing to the improvement in living standards. But at the same time they are exposed to different threats in cyberspace. These threats use vulnerabilities inherent in ICTs, and may cause denial of service or abuse of service attacks, resulting in potential damage (loss) to human lives, high scale economic losses, disturbance of public order, and threats to national security. "Globalization has also empowered terrorist groups by enabling an increase in the volume, range and sophistication of propaganda materials. Any computer of modest capability can be used by terrorist groups and their sympathizers to create propaganda leaflets, posters and even magazines in large quantities at very low cost" (Baylis et al., 2017: pp 410-111). Similar to the majority of countries in the region, and also beyond, another challenge faced by Kosovo security institutions is the use of the internet, social media and various computer applications for the communication and dissemination of extremist ideologies. "Using the internet to change the people's minds is more powerful than blowing up a server, and there's nothing new about propaganda" (McFate, 2019: p 16). Certain individuals or groups, using the privacy procedures and policies of companies that manage various applications, aim to communicate safely and without being detected by security agencies. "While certain platforms are more abused than others, the sheer number of Online Service Provider (OSPs) exploited for terrorist purposes presents a challenge for disruption efforts. These include forums, file-sharing sites, paste bins, video streaming/sharing sites, URL shortening services, blogs, messaging/broadcast applications, news websites, live streaming platforms, social media sites and various services supporting the creation and hosting of websites" (Europol, 2019: p 48).

The use of cyberspace for terrorist purposes in Kosovo is limited to spreading propaganda and the ideology of Islamic radicalism, while also supporting terrorist activities. "A 20-year-old computer science student from Kosovo described by the Justice Department as 'the first terrorist hacker convicted in the United States' was sentenced to two decades in prison for providing the Islamic State with a "kill list" containing the personal information of roughly 1,300 U.S. military members and government employees" (Blake, 2016). This is about a young man from Kosovo, Ardit Ferizi, who started hacking at a very young age, being part of various groups of hackers, such as the "Kosova Hacker Group" and the "Albanian Hacker Group". In August 2014 he travelled to Malaysia to study computer science; during his stay, he intervened in the US Department of Defence's system, stealing personal data from US soldiers, which he passed on to senior ISIS terrorist structures. So, given the enormous use of the internet in Kosovo and the many young people indoctrinated with extremist views who have the ability to use the internet, which can be used either in support of terrorist activities or for cyber-terrorism attacks, it is necessary for the security institutions in Kosovo to prioritize the fight against this phenomenon.

4 Legal Framework and State Mechanism

The Kosovo institutions, despite being faced with problems inherited from the past, as well as poverty and poor economic levels, have managed to establish a contemporary legal infrastructure for preventing and combating terrorism, including cyber terrorism. Kosovo, as a member of the Global Coalition against ISIS, has consolidated its legal basis, where in addition to the Criminal Code that defines the criminal offences of terrorism, it has also adopted a

law On the Prohibition of Joining Armed Conflicts Outside State Territory, and has amended its law to prevent routing of money and terrorist financing, which is a solid base for dealing with this issue. "The Government of Kosovo strengthened its existing counterterrorism provisions and approved a new counterterrorism strategy for 2018-22. The new counterterrorism strategy provides a comprehensive approach to preventing and combating terrorism and is one of the government's strategic priorities. On March 30, the Assembly passed the Law on Critical Infrastructure, which aims to identify, preserve, and protect national and European critical infrastructure" (US Department of State, 2019: p 97). The purpose of this law is, as stated, to preserve and protect national and European critical infrastructure, and also to protect the citizens of the Republic of Kosovo; to prevent incidents; to minimize potential damage to critical infrastructure and general wealth, and to minimize economic and social losses; to ensure government stability; and to enhance resilience.

The primary legislation in the field of Cyber Security includes:

- Constitution of the Republic of Kosovo[1]
- Criminal Code of the Republic of Kosovo[2]
- Criminal No. 04/L-123 Procedure Code[3]
- Law No.03/L –166 on preventing and fighting cyber crime[4]
- Law No. 06/L –014 on critical infrastructure.[5]
- Law No. 04/L-145 on information society government bodies[6]
- Law No. 04/L-094 on information society services[7]
- Law No. 04/L-109 on electronic communications[8]
- Law No. 05/L-030 on the interception of electronic communications[9]
- Law No.03/L – 172 on the protection of personal data[10]
- Law no. 04/L-076 on the police[11]
- Law no. 03/L063 on the Kosovo Intelligence Agency[12]
- Law no. 04/L-213 on international legal cooperation in criminal matters[13]
- Law no. 04/L-052 on international agreements[14]
- Law No. 04/L-064 on the Kosovo forensic agency[15]
- Law No.04/L –004 on private security services[16]
- Law No. 03/L-046 on the Kosovo security force[17]
- Law No.03/L –178 on the classification of information and security clearances[18]

1 http://www.kushtetutakosoves.info/repository/docs/Constitution.of.the.Republic.of.Kosovo.pdf
2 https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413
3 https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2861
4 http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf
5 https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
6 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20government%20bodies.pdf
7 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20services.pdf
8 http://www.kuvendikosoves.org/common/docs/ligjet/109%20Law%20on%20Electronic%20Communications.pdf
9 https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
10 http://www.kuvendikosoves.org/common/docs/ligjet/2010-172-eng.pdf
11 http://www.kosovopolice.com/repository/docs/Law_on_Police.pdf
12 http://www.assembly-kosova.org/common/docs/ligjet/2008_03-L063_en.pdf
13 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20international%20legal%20cooperation%20in%20criminal%20matters.pdf
14 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20international%20agreements.pdf
15 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20Kosovo%20Forensic%20Agency.pdf
16 http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20private%20security%20services.pdf
17 http://www.kuvendikosoves.org/common/docs/ligjet/2008_03-L046_en.pdf
18 https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690

The government of Kosovo has taken positive steps in building institutional mechanisms against terrorism, including cyber terrorism. According to the Kosovo National Cyber Security Strategy, below are the institutional mechanisms related to the role and coordination of activities of the main stakeholders that have a role in cyber security in Kosovo.

The National Cyber Security Coordinator is the Minister of Internal Affairs or his authorized representative, who is responsible and mandated to coordinate, guide, monitor and report on the implementation of policies, activities and actions in connection with the National Cyber Security Strategy.

The Secretariat is a body established with the function of collecting information and data from other institutions, analysing and assessing the gathered information, and developing analytical reports for the National Coordinator and the National Cyber Security Council. In addition, the Secretariat disseminates timely information to all appropriate stakeholders, supporting the National Action Plan for Cyber Security.

The Ministry of Internal Affairs (MIA) has a functional role in achieving the objectives set out in this strategy. The Kosovo police, as the law enforcement agency within the MIA, have full authority in combating all forms of cybercrime. The MIA takes the leading role in coordinating the strategy, monitoring the implementation of the Action Plan, and drafting periodic reports. The MIA is also responsible for the formulation and monitoring of policies and legislation in the field of general security and cyber security. The Kosovo Police have the main responsibility for combating all forms of cybercrime, through the Department for Cyber Crime and other supporting structures within the Kosovo police force. The Kosovo police also serve as the point of contact, 24/7, for international cooperation in the field of cybercrime.

The Kosovo Judicial Council ensures that the Kosovo courts are independent, professional and impartial, in order for the judicial system to be more efficient in the fight against cybercrime.

The Kosovo Prosecutorial Council ensures that the prosecution system in Kosovo is independent, impartial and professional in exercising the pursuit, investigation and detection of cybercrime offences, and represents indictments before courts on behalf of the state. The Prosecution Service and the courts are the institutions responsible for prosecuting perpetrators and their appropriate punishment, and the confiscation of property and assets gained through criminal activities.

The Kosovo Security Council Secretariat, as an integral part of the Security Council of Kosovo, prepares periodic reports and analysis for the Government of the Republic of Kosovo and the Security Council of Kosovo dealing with political issues of security, and provides assistance in drafting security policies in Kosovo, including capacity building, policy and research instruments, and providing administrative and functional support for the Security Council of Kosovo.

The Kosovo Intelligence Agency identifies threats endangering security in Kosovo. These threats are considered to be those relating to territorial integrity, institutional integrity, constitutional order, stability, and economic development, as well as global security threats against Kosovo.

The Ministry of Justice prepares and develops legislation in the field of justice, and coordinates and develops international judicial cooperation in criminal matters.

The Ministry for the Kosovo Security Force (MKSF) develops and strengthens the cyber security of communications and information systems for the MKSF/KSF, systems which are used for performing tasks in accordance with the constitutional mission. The KSF may be engaged in support of civil authorities in the protection of data and critical infrastructure in the event of a crisis in the country.

The Ministry of Economic Development ensures quality of service and technical standards in the field of telecommunications; develops policies to promote competition in the field of telecommunications; examines the needs and requirements of customers in telecommunications; supports information technology and innovations; supports access to technology for all citizens of Kosovo; and encourages the development of training systems for information technology.

The Ministry of Finance, through the Customs, the Financial Intelligence Unit and the Tax Administration, helps in strengthening cyber security and in preventing and combating cybercrime.

The Ministry of Education, Science and Technology plays an important role in prevention and awareness raising through the development of curricula, the organization of awareness-raising activities for the use of the internet, and extracurricular activities.

The Ministry of European Integration makes sure that the legal framework and policies of the Government of the Republic of Kosovo are in accordance with the legislation and policies of the EU.

The Regulatory Authority of Electronic and Postal Communications is a regulatory body which implements and monitors the regulatory framework defined by the law on electronic communications, the law on postal services, and the development policies in the field of electronic communications and postal services.

The Agency for an Information Society (AIS) coordinates, manages and monitors the processes and mechanisms of electronic governance in relation to ICT infrastructure, the expansion of internet services and content websites in the institutions of the Republic of Kosovo, and the accumulation, management, dissemination and storage of data, through the creation of the national electronic data centre and by providing safety and protection of electronic communications infrastructure and data. The AIS, as appropriate, helps relevant institutions in combating cybercrime and ensures the protection of personal data in electronic form, in accordance with the legislation in force.

The National Agency for the Protection of Personal Data ensures that controllers comply with their obligations on the protection of personal data, and that data subjects are informed about their rights and obligations in accordance with the Law on the Protection of Personal Data. It also provides advice to the Assembly of Kosovo, the Government, local authorities and all holders of public authority in Kosovo with regard to issues on the protection of personal data, as well as advising all private institutions concerning the protection of personal data.

5 Challenges and Recommendations

Critical information infrastructure is becoming the target of increasingly complex cyber-attacks more frequently. Such attacks are specifically aimed at particular targets by terrorists and hackers looking for sensitive information, or with the aim of destroying this critical information infrastructure. "There are certain types of cyberattack that might create the kind of dramatic effects that terrorists desire. For example, shutting off the supply of electricity to a major city or taking down the air traffic control system would likely generate fear, especially if such demonstrations of control over critical infrastructures were accompanied by credible threats to conduct additional cyberattacks" (Caldwell and Williams, 2016: p 172). "This becomes even more problematic when the technique of terrorism is moved to the cyber realm. Just as not all acts of fear-inflicted violence are terrorism, not all activities of terrorists in cyberspace constitute cyberterrorism. Cyberterrorism, like terrorism, is a tactic used by terrorists, and one main element of that tactic is to create fear in a population, something that is more difficult to accomplish in cyberspace" (Kremling, 2018: p 236).

"Significant growth of internet users in recent years in Kosovo has brought with it increased danger of computer crime and cyber-attacks. Although so far there have been no cases of serious penetration and damage to systems with state data, various criminal activities were enough to highlight the weaknesses of computer networks in Kosovo, which is still considered in the development stage" (Kosovo National Strategy, 2015: p 12). One of the challenges that therefore needs to be addressed is the weak and vulnerable computer network in Kosovo, and so it is recommended that the institutions responsible for cyber security and the fight against terrorism develop and implement procedures and practices to provide protection to critical infrastructure. In order to have more efficient treatment of cyber security incidents and better protection of critical information infrastructure, I believe that institutional mechanisms should be created for this issue, such as the State Authority for Cyber Security and the creation of reaction units to cyber incidents (CERT) in state, public and private institutions which possess critical information infrastructure. It is also recommended that through the strengthening of CERT national capacities, an effective interaction between institutions both inside and outside the country should be ensured.

Citizens often fall victim not only to fraud and fake news, but also to the propaganda of terrorist groups on the internet. "Jihadist propaganda on the net is highly dynamic, adaptable, and professional. In the past years, its quantity and quality have been steadily on the rise, with increasingly diverse internet material glorifying the militant fight and vilifying certain groups of people, such as non-Muslims, Jews, Shias, and others" (Frankenberger, 2017: p 67). Even in Kosovo, the challenge itself is the spread of extremist ideology and the support of terrorist groups through the internet, and this of course presents added challenges for the country. The citizens do not have enough knowledge of the dangers of using the internet, and this is an indicator that it is necessary to raise the awareness of citizens or internet users. This can be achieved through various campaigns, conferences, brochures and publications, education and training, and so on. Also, cooperation with the private sector through public-private partnerships should be promoted and strengthened.

One of the most important challenges for Kosovo's institutions in combating cyber terrorism is strengthening cyber security. Initially, it is necessary to complete the legal infrastructure, such as the approval of the Law on Cyber Security, as well as the Law on Public Key Infra-

structure. Contemporary cyber security legislation would lay the groundwork for strengthening institutional capacity, setting priorities, and clearly defining the meaning of the terminology associated with cyber terrorism. Cyber defence, however, remains a challenge that needs to be addressed by Kosovo's institutions. The lack of a national strategy for cyber defence is seen as a shortcoming in the security system, and a lack of protection of critical infrastructure from cyber terrorism attacks. Also, this strategy would be more important for determining the role and responsibility of the institutions and defining cyber defence, which is mainly used in a military context, but may also be related to criminal and espionage activities. "Accurately defining cyber defence is equally important. In the context of a specific environment, cyber defences analyze possible threats and help to devise and drive the strategies necessary to counter malicious attacks or threats. A range of activities are involved in cyber defence when protecting the concerned entity and for responding to the threat landscape. These include: reducing the appeal of the environment to possible attackers; understanding the critical locations and sensitive information; enacting preventive controls to ensure attacks would be expensive; attack detection capability; and strengthening reaction and response capabilities" (Galinec, 2018: p 15). Given this, in order to strengthen efficiency in the fight against cyber terrorism, it is strongly recommended that the National Strategy for Cyber Defence, which consists of following duties, Protect, Detect, Respond, and Recover, be drafted and approved.

6 Conclusion

The efforts of Kosovo's institutions in the fight against violent extremism and terrorism have increased significantly and consistently. The government of Kosovo has made countering extremism and terrorism a priority, and has taken positive steps in drafting new legislation and creating a responsible state mechanism. As a result of the measures taken by the Kosovo institutions, both in terms of prevention and of strengthening international cooperation, as well as criminal prosecution, the threats of violent extremism and terrorism have been significantly minimized. So far, Kosovo has not directly faced terrorist or cyber-terrorist attacks, but what currently challenges Kosovo the most is the dimensions of the spread of extremist ideology and Islamic radicalism through the internet, which may possibly increase the phenomenon of cyber terrorism. Cyber-terrorism is an increasingly attractive choice for terrorists because it can be accomplished with only modest financial resources, with anonymity, and from a great distance. The use of cyberspace for terrorist purposes in Kosovo is limited to spreading propaganda and the ideology of Islamic radicalism, but it also supports terrorist activities. A 20-year-old computer science student from Kosovo, during his stay in Malaysia, intervened in the US Department of Defence's systems, stealing personal data from US soldiers, which he passed on to senior ISIS terrorist structures.

In Kosovo, the use of Information and Communication Technologies (ICTs) has been spreading rapidly, and ICTs play important roles in all aspects of life. Internet penetration in Kosovo is 88.8%, which is similar to the EU average, and Kosovar habits in cyberspace tend to be also similar to global trends. So, given the massive use of the internet in Kosovo, and the many young people indoctrinated with extremist views who have the ability to use the internet, which can be used either in support of terrorist activities or for cyber-terrorism attacks, it is necessary that the security institutions in Kosovo prioritize the fight against this phenomenon. There is an imposed need to strengthen cyber security and the capacity to protect critical infrastructure from cyber terrorism. It is necessary to complete the legal infrastructure and

strengthen institutional capacity, to increase security, and to minimize the vulnerability of the computer network in Kosovo. In this respect, the lack of strategy and mechanisms for cyber defence can be seen as one of the major challenges to Kosovo's efforts to combat cyber terrorism. Given this, it is strongly recommended that the National Strategy for Cyber Defence be drafted and approved, in order to strengthen efficiency in the fight against cyber terrorism.

7 References

1. Baylis, John; Smith, Steve; Owens, Patricia (2017). The Globalization of World Politics. An Introduction to International Politics. New York. Oxford University Press.
2. Blake, Andrew (September 24, 2016). Islamic State hacker sentenced for assisting terrorist group with 'kill list'. The Washington Times. https://www.washingtontimes.com/news/2016/sep/24/arditferizi-hacker-who-aided-islamic-state-senten/ Retrieved on 26.04.2020.
3. Britz, Marije T. (2013). Computer Forensics and Cyber Crime – An Introduction. New Jersey: Pearson.
4. Caldwell, Dan; Williams Jr, Robert.E. (2016). Seeking Security in an Insecure World. Lanham, Maryland. Published by Rowman &Littlefield.
5. Country Report on Terrorism (2019.) https://www.state.gov/reports/country-reports-on-terrorism-2018/#Kosovo Retrieved on 02.03.2020
6. Diogenes, Yuri; Ozkaya, Erdal (2018). Cybersecurity, Attack and Defense Strategies. Birmingham: Packt Publishing.
7. European Commission (2019). Available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-kosovo-report.pdf
8. Europol (2019). European Union Terrorism Situation and Trend Report 2019. Available at:
9. Europol (2019). Internet Organized Crime Threat Assessment (IOCTA). https://www.europol.europa.eu/iocta-report (15.02.2020)
10. Frankenberger, Patrick (2017), Is the Internet a Factor in Radicalization? Jihadist propaganda is targeting youngsters. Retrieved on 08.03.2020 from https://www.praeventionstag.de/daten/module/buecher/en/ISBN-978-3-96409-063-8/6-Frankenberger.pdf
11 Galinec, Darko (2018). Resilience is Key; how to thwart known, and unknown, dangers. per Concordiam, Journal of European Security and Defence Issues,Vol.9,Issue 1, Georg C. Marshall Centre, Garmisch-Partenkirchen, Germany. Retrieved on 01.03.2020 from: https://perconcordiam.com/perCon_V9N1_ENG.pdf https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat
12. https://www.internetworldstats.com/stats4.htm (02.03.20202)
13. Kosovo National Strategy (2015). National Cyber Security Strategy and Action Plan 2016-2019
14. Kosovo Police (2020). Kosovo Police Annual Work Report 2019. Prishtina.
15. Kremling, Janine; Parker, Amanda M. Sharp (2018). Cyberspace, Cybersecurity, and Cybercrime, Thousand Oaks, California: SAGE Publications, Inc.
16. Maher, Shiraz (2016). Salafi-Jihadism, The History of an Idea. New York. Oxford University Press.
17. McFate, Sean (2019). The New Rules of War. New York. HarperCollins Publishers.
18. Yar, Majid (2006). Cybercrime and Society. London: SAGE publications.

Section II.

Cyber Terrorism and Security Implication for Critical Infrastructure Protection

1 Hyper Threats to Critical Infrastructures in the Region of South-Eastern Europe: A Wake-Up Call for South-Eastern European Leadership

Metodi Hadji-Janev

1 Introduction

The security environment has changed dramatically over the past few years. This change is ongoing and is happening faster than South-Eastern European (SEE) leaders think. The change is occurring in terms of diplomacy and global political competition, economics, modern technologies and innovation, and in the context of security and military affairs. These changes, put together, have affected the monopoly of power previously granted to states and organizations that states have formed. Thanks to the general power shift, non-state actors can asymmetrically challenge nation-states from cyber and physical space, and thus interfere in strategic affairs, influence policy and decision-making, and consequently produce organizational and conceptual changes to security in the SEE countries and around the globe.

Hence, policies to identify and protect critical infrastructure (CI) or critical information infrastructure (CII), among others, have dominated SEE diplomatic, policy and security elites over the past decade. Focusing on critical infrastructure protection (CIP) or critical information infrastructure protection (CIIP) to some degree has resulted in a loss of the sense of geopolitical awareness. Nevertheless, the rise of emerging state actors with hybrid types of regime, internal EU fatigue, NATO internal latent competition, and advances in information and communication technologies (ICT) are unequivocally introducing geopolitics into the SEE policymaking calculus. Moreover, hybrid base threats blending the peace and war types of activities coming from both cyber and physical space and with methods that exploit modern society's vulnerabilities have become a dominant concern for the democratic governments in the region of SEE.

One specific segment of the geostrategic competition that has so far not been addressed properly is the artificial intelligence (AI) race. The quest for efficiency is introducing AI into everyday lives faster than SEE policy and security makers can imagine. AI is expected to en-

hance the functioning and efficiency of goods and services across healthcare, transportation, and financial services, and to significantly improve business efficiency. However, the trend of weaponizing AI systems, and the intent to use them for strategic, political and military purposes, among others, raises great concerns in the context of CIP and CIIP. The ability of AI to collect and process massive data and supersede human cognitive and physical limitations (from decision-making to real physical actions) has already stimulated ethical, moral, legal and serious security debates around the globe. AI systems and applications are thus challenging the existing standards and principles of law based on human limitations and performance capabilities. At the same time, AI applications and systems are becoming a new threat and attack vector for CI and CII. Potential malfunctioning or errors based on the algorithm insufficiencies or unpredicted assumptions during deep learning processes can cause threats beyond the AI employer's imagination. The ability to hack the algorithms or feed AI with misinformation in an interconnected and interdependent world is making AI a perfect attack avenue for both state and non-state actors with malicious agendas.

While debates about the implications of AI are becoming more frequent around the world, the subject is rarely discussed during SEE-based security forums. This article therefore intends to stimulate debate about AI applications in the SEE security context, and more specifically in the CIP and CIIP context. It briefly addresses the changing security environment and explains how threats to SEE security have evolved from conventional through unconventional and cyber-based to hybrid-based threats. The main argument throughout the article is that the AI race in the security and defence sector is giving a whole new dimension to geostrategic competition, and that this race is elevating asymmetric, cyber and hybrid-based threats to a whole new hyper-threat level. After explaining the hyper threats, the article provides reasons why the SEE leadership needs to consider these threats in the context of CIP and CIIP. Finally, it provides some recommendations that must be considered for better CIP and CIIP in the world of hyper threats.

2 The Security Environment has Changed and is Changing Fast

Intensified globalization, technological development, and the return of geopolitics shape the security reality in the region of SEE (Lachert, 2019). All these changes in SEE reflect the framework of CIP and CIIP. The transition after the Cold War, among other things, in the security sector has urged SEE to move from the massive defence type of organization to a crisis management approach and protection of critical infrastructures (Hadji-Janev & Jovanovski, 2013). Nestled under Euro-Atlantic integration processes, the armed forces followed NATO-led transition and integration, while the remainder of the security sectors (law enforcement and internal affairs including crisis management, disaster, and protection) transitioned under the EU framework, leading to transition and integration. To be able to cope effectively with the emerging security trends (predominantly coming from non-state actors), western democracies have introduced (and SEE countries have followed) the critical infrastructure protection concept (CIP) (Cyber edu, 2007) or the critical information infrastructure concept (CIIP) (Willke, 2007). These concepts were supposed to replace the robust and inert defence systems with a more federated type of approach to security, shared between the public and private sectors.

Technological development and the rise of information and communication technologies in the region of SEE brought many positive, but also some negative, effects. Cyberspace now has political, economic, security (defence), and emotional-psychological effects on SEE societies. It reflects not only the modernity, but also the increased vulnerability of SEE societies. Protecting CI and CII in this digital and interconnected world has become a serious challenge. Cyberspace and the internet of things (IoT) have brought a whole new set of vulnerabilities that security experts need to consider in their risk assessment matrixes (Marisetty, 2019). In the age of ICT expansion and connectivity, the Cold World predictability of security threats is long gone, and the potential of cascade effects urges security experts to advise measures and policies that challenge the core of democracy (Nye, 2018). This new reality has enabled non-state actors, groups, and individuals, to exploit modern technologies and to pose strategic challenges by threatening national or regional critical infrastructures. The ability to hide, explore vulnerabilities, communicate, mobilize and transfer resources, influence and recruit support and executers, fund their activities remotely and project ideology and influence, previously available only to states, is now available to individuals and groups with radical, religious, violent and political objectives. Thanks to technology, terrorist organizations are able to challenge the SEE countries' security, among other ways thorough CI and CII (Badie, 2012).

The emergence of the new actors' (other than the EU and NATO) involvement in the region has, nevertheless, given a whole new dimension to the security of SEE. The interplay between Russia, China and to a certain degree Saudi Arabia and the UAE has (re) introduced geopolitics into the security calculus (Feyerabend, 2018). As a result, the security environment is highly complex and unpredictable. Exploiting non-traditional military threats that blend through the different sectors of society introduced "hybridity" into the security assessments of the SEE countries. Yet the interconnectivity and interdependence of technology, with civil services and private and public sector service providers for everyday life (transport, communication, energy, health, money, safety, etc.), along with different processes and events (such as migration or pandemic diseases such as the coronavirus) are the perfect set-up for creating unpredictable cascade effects.

Today, the actors that can cause security threats to SEE countries vary. Individuals and groups with different agendas ranging from personal frustration or greed (criminals) or a quest for a better life (migrants) to individuals and groups with a political goal (terrorists) are causing asymmetric threats to SEE CII (Yonah, 2018). State actors who want to project their influence through state proxies, civilian and military infrastructures, and personnel by fabricating news and creating "fake news" phenomena to undermine democratic and Euro-Atlantic integration processes, or by corrupting economic sectors for economic gain, pose hybrid threats to SEE CII and CIP (F2N2, 2019).

At the same time as these processes are ongoing in the global security arena, the quest for proficiency in all sectors of society urges the development and implementation of artificial intelligence applications (Bostrom, 2017). The processes of turning these AI applications into AI systems are heavily shaping the geostrategic context. Hence, the geopolitical interplay shaped, among other things, by the AI race is giving new momentum to security around the world by turning the asymmetric, cyber and hybrid-based threats into a "hyper threat" to SEE CI and CII (Siddiqui, 2018). Before we explain how and why hyper threats need to be considered in SEE CIP and CIIP, it is important to understand what the "hyper threats" are.

3 From Asymmetric, Cyber and Hybrid Threats to Hyper Threats to South-Eastern European Countries' CI and CII

The term "hyper threat" is not a new "buzz word" that has just recently begun to dominate geo-strategic and security debates. During World War II the term combined many concurrent theatres of war. Giving the technological development of that time it is understandable that the revolution in military affairs that occurred prior to WWII led the idea of a "pan-war" to influence the understanding of the term "hyper".

Little has been written about hyper war and hyper threats. Most of the existing debates in the modern context connect this term to a desire to explain threats that come from the interconnectivity and interdependence of the modern way of living put in the context of AI systems. The origin of the word, however, comes from the Greek term "hyper" meaning over or above. Usually this term is used to express something that is beyond what is already known, defining an abundance of something.

In the modern context, hyper threats in their essence have AI systems' performance and ability to collect, process, and disseminate data at a higher volume and a greater velocity. As General John R. Allen asserted, "What makes this new form of warfare unique is the unparalleled speed enabled by automating decision-making and the concurrency of action that will become possible by leveraging artificial intelligence and machine cognition" (Allen & Hussain, July 10, 2017).

Similarly, Stuart Lauchlan argued that "hyper warfare is the idea that future war could take place at such a high level of strategy, technology and destruction that its effects would be worse than the Second World War between 1939 and 1945" (Lauchlan, 2019). Euhus believes that hyper war requires more strategic comprehension than just the tactical effects of AI systems (Euhus, 2019).

The GLOBSEC NATO Adaptation Initiative analysis, on the other hand, concluded that "Advances underway in security and defence-related technologies that span the conflict spectrum from Hybrid War at the lower end, to Hyper War at the future high end, will be rapid and dramatic. Hybrid War will continue to drive requirements for enhanced intelligence collection, cyber-security, and critical infrastructure protection. Given the reliance of Alliance societies on web-vulnerable infrastructures, the effects of a cyberattack could lead to significant if not catastrophic physical damage" (GLOBSEC, 2018).

From all of the above, it seems that applying AI systems in the security context brings an ability that is beyond just the asymmetric cyber capacities or hybridity. The asymmetry of these systems spans from their availability right up to the ethical, moral and legal boundaries of their applications. AI systems are expanding very fast. Terrorist organizations have so far proved creative and ready to employ whatever serves their cause (Heffelfinger, 2013). They would not be hesitant to employ AI systems and applications to achieve their strategic ends. Hacking these systems, overriding their algorithms and subordinating them to the terrorists' goals is not impossible. Terrorists or hackers working in these capacities could endanger existing SEE governments' AI systems or partner nations' systems performing critical functions or missions. As Tomáš Valášek of Carnegie Europe argued, "AI can be effectively deployed to undermine trust among countries fighting on the same side by discrediting their intelligence (Valášek, 2017).

States' (or their proxies') use of AI systems to expand intelligence, surveillance and reconnaissance capacities supersedes the gain of the asymmetric strategies, cyber espionage, and hybridity. AI systems and applications are able not only to collect but also to process massive amounts of data in a short time; something which requires significant skilled manpower. In a world of mega data, the internet of things and multi-vector and multi-domain based threats, fast decision-making is a priority. AI systems can overcome the "cognitive burden" and avoid instinctive, emotional and rapid decision errors (Barton, 2019).

Furthermore, collecting important data and adequately processing it could allow the opponent (state or non-state actors) to exploit vulnerabilities beyond predictable capacities. Amir Husain, founder and CEO of SparkCognition Inc., observed that "the advent of hyperwar opens up the reinterpretation of our geostrategic future" (Ackerman, 2018). Most CIP and CIIP plans and procedures are based on the underlying assumption of the limitations of human capacities.

These limitations could, for example, be in the context of:
- Manoeuvrability (to be in a different place in a short period of time);
- Mass (to overwhelm defenders' capacities in a short period of time);
- Economy (to act with surgical precision and cause collateral damage that could have negative consequences or additional logistical requirements in terms of replacement of forces after long engagement and stress etc.);
- Competency ("nerds" rarely have skills that require intensive and long physical training);
- Coordination – unity of efforts (to swarm the target or to cause the effect of an advanced persistent threat and overcome any redundancies with an ability to simultaneously disable cyber and physical defences in a coordinated manner);
- Above all AI can perform in an exclusive cognitive complexity (making a decision under stress, after a long engagement with higher precision and without instant errors) (Walch, 2019).

AI thus affects two key important variables for CIP and CIIP: time and space. AI can transfer data, performance, and even behaviour with greater velocity and with a higher volume. "Reinforcement learning" (an area of machine learning concerned with how software agents ought to take action in an environment in order to maximize the notion of cumulative reward) is already practised in the gaming industry and is giving significant results in the autonomous automobile industry (Marr, 2018). Skills and knowledge (developed tactics, techniques and procedures) can be replicated in almost no time even remotely. The instant transfer learning capability cannot be compared with recruiting terrorists or developing a hackers' army. This requires time, and there are specific conditions that must be satisfied. The ability to overcome the essential pre-requirements for CIP and CIIP by employing AI systems and at the same time to cause asymmetric and hybrid threats via cyberspace is raising the threat to a whole new "hyper" level.

Debates about the development of AI and its impact on society are rare in the region of SEE. Up to a point, this is understandable given the fact that the effects of AI have only been acknowledged on the margins of security and innovation debates. The consideration of the impact of AI to SEE societies as a whole and in the context of CIP and CIIP is urgent.

4 Why the South East European Countries Need to Reconsider CIP and CIIP in the World of AI

The explosion of technological development, even without AI, urges political leadership, strategists and security experts from SEE to reconsider CI and CII. The complexity and unpredictability of the interconnected and interdependent security environment filled with the AI systems race have dramatically stimulated the evolution of the classic approach to the classification of CI and CII (European Commission, 2020). There are several reasons why SEE countries need to reconsider their approach to CIP and CIIP.

Defining what is considered as CI and CII is an unfinished job. Defining and designating what is considered CI or CII is important in the operational (security) context, as well as in the context of the law (The U.S. Congress, 1988, p 54). The concept helps to provide a framework for better protection and regulation. The Internet of Things (IoT) trend is changing the reality we know very fast (Bur, 2017). This is reflected in how we understand security and how we approach protection. Hence electrical and nuclear power plants, chemical factories, and the finance, health, food, and transport industries, along with government agencies, rightfully deserve the "critical" designation. Nevertheless, there are other industries and services that enable these critical infrastructure organizations to properly function. Incapacitating these "enablers" could either slow down or prevent the effective functioning of the designated critical infrastructures. Therefore, in a world of constant and rapid technological change, minimizing vulnerabilities is a never-ending story (Ismail, 2018).

The alleged interference of Russian proxies in the US election is the best argument for this thesis. After the 2016 presidential election in the US, the US Department of Homeland Security (DHS) designated elections systems as part of the US nation's critical infrastructure. At the time of the designation, then-DHS Secretary Jeh Johnson observed, "Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact, and in law" (The U.S. Election Commission, 2017). Critical infrastructure is a DHS designation established by the Patriot Act and given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Patriot Act, 2001, Sec. 1016(e)). When the US DHS was established in 2002 and designated as the agency responsible for CIP, the institution developed the National Infrastructure Protection Plan (NIPP). In addition to this, US Presidential Policy Directive 21 established the Federal Government's "strategic imperatives" in its approach to the nation's critical infrastructure. Although these documents were established in a different time, none of them mentioned the electoral system as critical infrastructure (The US Election Assistance Commission, 2017a).

Knowledge is changing fast. Fuller estimated that up to 1900, human knowledge doubled approximately every century (Fuller, (1982). According to him, by 1945 it was doubling every 25 years, and by 1982 it was doubling every 12-13 months. Citing IBM, Marc Rosenberg estimates that in 2020 human knowledge will be doubling every 12 hours (Rosenberg, 2013). Thus, creativity in exploiting different tools for achieving different ends is constantly evolving. Terrorists surprised us during the 9/11 attacks and have literally "hacked" the security concepts and understanding of homeland security. This was in terms of actors that could

launch an armed attack, in terms of the means to launch such an attack, and in terms of the priority to protect the potential target. This "hack" did not just challenge operational wisdom, but also created shockwaves inside the legal community.

The threat from terrorists is already here and is evolving from external threats to an internal threat. It is well-established among the academic, pundit and intelligence community that SEE has emerged as a battleground for radical militant Islamism. Both anecdotal and empirical evidence confirm this thesis (Bodansky, 2001). The bomb attack on a police station in the central Bosnian town of Bugojno in June 2010 (BBC, 2010), the 2011 attack on the US Embassy in Bosnia (Alic, 2011), the 2012 attack and murder of 5 civilians in Macedonia (Dimitrioska, 2012), and the 2012 attack on Israeli tourists in Bulgaria (BBC, 2012), along with numerous reports of prevented attacks or arrests (e.g. in Bosnia, Serbia, Croatia, Kosovo, or Cyprus) (Hadji-Janev, 2012), confirm that the threat from these adversaries is real. Recent trends in the active support of radical Islamic groups in the Syrian resistance, however, have shown that the threat has changed from imported to home-grown. Furthermore, the growing amount of internet-based recruitment for these supports, along with the alleged on-line radicalization prior to the aforementioned attacks and attacks around the globe connected with the region, raise serious concerns over terrorist use of cyberspace in the region of SEE.

The threat vectors are evolving. The means to launch an attack and endanger CI and CII are rapidly changing. As an example, the history of using unmanned aerial vehicles (UAV) is astonishing. According to O'Donnell, the earliest recorded use of a UAV dates back to 1849, when the Austrians attacked the Italian city of Venice using unmanned balloons which were loaded with explosives (O'Donnell, 2019). Fast-forward to the aftermath of 9/11, and the CIA began flying armed drones over Afghanistan as part of the war against the Taliban. The first CIA drone-based kill operation took place in February 2002, when an unmanned Predator drone was used to target a suspect thought to be Osama bin Laden (Dormehl, 2018). Soon, however, these exclusive "gadgets" were commercially available and began to pose security implications. The region of SEE is not unfamiliar with the potential security implications of UAVs. The advancement and proliferation of public-use UAVs are much more complicated than that which SEE countries witnessed during the football incident between Serbia and Albania (Ames, 2014). Today UAV has become more readily available and more sophisticated, supporting new capabilities such as increased data collection and autonomous behaviour. According to a RAND think-tank study, UAVs are reshaping the cybersecurity world in two key ways: "Firstly, UAS [referring to UAV as systems so using UAS instead of UAV – author] present a new kind of critical cybersecurity target. Critical law enforcement or data collection missions using UAS could be undermined by cyber attacks on these platforms. Secondly, UAS in the hands of adversaries could present novel avenues for cyber attacks, with the UAS themselves serving as "cyber weapons" intended to deliver malicious content or enable kinetic impacts" (Best et al., 2020).

The point of this analysis is to emphasize that the threat from UAVs is only one example of how threat vectors can vary and endanger CI and CII. Threats to CII do not exclusively come from cyberspace. The Stuxnet computer worm attack on an Iranian nuclear power plant will definitely rewrite the cyber terrorism playbook (Chery, 2010). In this context, David Geer offered statistical arguments clearly speaking of the increased physical danger risks of cyber terrorism (Geer, 2014). If the story about "Operation Orchard" by Erich Follath and Holger Stark, published in Spiegel, in 2009 is true, then it is clear why denying the terrorist threat

to SEE cyberspace or CII in the region of SEE will need an update (Follath & Stark, 2009). The disappointment of the Ukrainians in 2016 in US-supplied drones (Stewart, 2016), or the ransomware or supply chain-based attacks on key personnel that manage CIP or CIIP, are just some of the examples of how the threat vectors evolve. However, wait for it; the biggest, the fastest, the unexpected, something which goes beyond is yet to come.

Artificial intelligence applications turned into systems are a threat to CI and CII. The United States Department of Defence (DoD) has forged innovative uses for AI in defence and security. Initially, AI was used to assess the readiness of military vehicles or to identify insurgent targets. Today, these efforts have shifted into a higher gear under a US strategic initiative focused on harnessing AI to advance security and prosperity (HPC, 2019). At the same time, these advantages have started to become a liability.

It is true that currently most of the digitalized supervisory of the CIP or CII in the SEE countries is separated from the internet. Nevertheless, the Stuxnet incident proved that this separation is not a solution. Analyzing potential threats from Russia to the US electric power grid as CI, Ian Fitzgerald observed that security experts can no longer rely on traditional methods of intrusion detection (Fitzgerald, 2019). Giving the example of a coordinated cyber attack from staging targets (smaller companies or a start-up that at some point work for the energy sector) to the designated attack targets (companies that generate, distribute and transmit electricity), he argued that traditional cybersecurity can eventually be hacked. His argument was that AI systems need to replace humans. While this is possible, the potential to hack these systems is open.

For example, the US Army uses facial recognition to train AI. However, assessing potential vulnerabilities has, at the same time, pushed the US Army to seek solutions. Backdoors into facial recognition AI platforms, specifically, are a real worry, as if they were compromised it could set off a chain reaction in which AI learning could be corrupted (Osborne, 2020).

On the other hand, some of the emerging strategic actors in the region of SEE, such as China or Russia, are heavily involved in this race. Its challenge straddles the boundaries of ethics and legality to security and existential issues and challenges. It is already known that China has less ethical and legal sensitivity in trading security for privacy. China's determination to become a world leader by 2030 is no longer a secret (Triolo et al., 2018). In this line, China has already proved skilful in using the private sector to achieve strategic ends via cyberspace. China's efforts to develop complex sensor networks in the private sector with disrupting potential for the military domain raise concerns in the context of CIP and CIIP for two reasons (Jans, 2018). Firstly, because as in the context of nuclear, chemical and biological weapons, these means (weapons) are desirable to terrorists. Secondly, there are no technical and legal standards for AI systems such as heavy regulations of the nuclear, chemical and biological sectors. Russia also wants to exploit the disruptive potential of AI. The Russian President, Vladimir Putin, has already declared that the competition is ongoing by saying: "Whoever becomes the leader in this sphere will become the ruler of the world." A swarm-based attack led by an AI system starting from staging targets (small companies based in SEE, and related to both the defence industrial complex in the US and acting as a service provider for a critical sector in SEE) is inevitable. Moreover, in this interconnected and interdependent world, the existing allied platforms that utilize AI to protect CI or CII could become a problem and a liability to the SEE CI and CII, which leads us to the next important reason for considering AI as a source of a "hyper" threats to SEE CI and CII.

AI systems will eventually be implemented and will drastically change the approach to CIP and CIIP. Although AI applications and systems are, to a certain degree, science fiction in the SEE CI and CII, SEE strategists need to begin to develop concepts that will embrace AI in the process of CIP and CIIP. Many have already argued that AI will profoundly change the organizational planning and coordination of security. The AI systems' ability to fix disruption of decision-making processes by their enormous speed of development and their ability to learn fast and adapt is a desire for more efficient and up-to-date CIP and CIIP. Fitzgerald's example is relevant in this context: "Using AI or machine learning to determine network baselines, even as those baselines shift, allows Chief Information Officers - (CIOs) to identify model breaches based on abnormal user behaviour". The US Department of Homeland Security has piloted AI tools for detecting cyber-network intrusions and malicious activities as a replacement for human intelligence and a quest for more efficient protection of its CII (Berteau, 2018).

Given the Euro-Atlantic agenda of all of the SEE countries, it is important to mention that both the EU and NATO have recognized the potential of AI and have decided to tackle this issue. In 2018 the European Commission put forward a European Approach to Artificial Intelligence and Robotics (The European Commission, 2018). It deals with the technological, ethical, legal and socio-economic aspects to boost the EU's research and industrial capacity and to put AI at the service of European citizens and the economy. The EU believes that an "anticipatory approach is needed to deal with AI's transformation of the labour market. It is necessary to modernize Europe's education and training systems, including up-skilling and re-skilling European citizens" (The European Commission, 2018). Although the EU does not consider AI in a security context, some of its Member States have already developed strategies (the French one being the most notable) (Villani, 2018), and the EU believes that new legal and ethical questions should also be considered.

NATO has not dedicated a special summit to the issue. However, the Allied Command Transformation has initiated a series of debates and has considered the willingness, ability, and means to deploy cutting-edge technologies, AI chief among them (NATO ACT, 2019). While it is true that all of the SEE countries follow either EU or NATO guidance in the security context, there are two issues for the SEE states in the context of CIP and CIIP: first, there are no EU or NATO guiding standards for these infrastructures, and second, the protection itself depends on the Member State's capabilities.

The strategic and operational approach to CIP and CIIP and cybersecurity strategies may be outdated and needs improvement. Rapid change and development in security as well as in technology unequivocally dictates that the current approach, both from the security aspect to CIP and CIIP and in national cybersecurity strategies, needs an update. While it is true that there are strategies in place that cover CIP or CIIP in all the SEE countries, there are two challenging facts that require attention.

Firstly, strategic approaches among the stakeholders differ, and when put into practice, i.e. operationalized, they give different results and outcomes on the ground (when effective protection needs to be implemented in terms of procedures, tactics, and techniques). Regardless of the different views on whether the EU Common Security and Defence Policy is a competing framework for NATO membership of the SEE countries, one thing that is clear is that NATO integration dominated changes in the SEE defence sector (Valášek, 2018). On the other hand,

the general security sector (law-enforcement), including a focus on CIP and CIIP, has been driven by the EU CSE framework and other relevant EU policies. Even now, put into the context of AI, as we have seen, the EU is refraining from considering the security implications of AI, while NATO debates are more open to exploring the effects of AI systems, including as a weapon. Although this may not look important at first glance when operationalizing different standardizations, and different legal approaches producing different prioritizations, risk assessment matrices, structures, and legal frameworks, this type of difference is well known in the fight against terrorism vs. global war on terrorism, as well as in the cyber domain.

Secondly, most of the current crisis management postures (usually leading the CIP and CIIP) have arguably proved incapable in practice. Specifically, EU and NATO integration has helped the SEE countries to migrate from a total defence concept to a crisis (emergency) management concept under the democratic construct. The problem, however, is that recent natural disasters and migrant crises have shown that the crisis management sectors in most of the SEE countries rely heavily on the defence sector (the armed forces to be more precise) (Pirovska, 2018). This means that in many cases and to a certain degree these sectors have been developed on paper or just because the "EU and NATO told us so".

The changed security reality, with the geopolitics heavily in place and the world of AI systems capable of raising asymmetric, cyber and hybrid threats to a new hyper level, urges the SEE leadership to seriously reconsider the CIP and CIIP sectors.

5 Some Recommendations for a Better CIP and CIIP Approach in the World of Hyper Threats

To effectively cope with the ongoing trend of hyper threats, the SEE leadership needs to start talking openly about AI systems and the geopolitical interplay in the context of effective CIP and CIIP. Understanding the strategic importance of defence in the changed security environment, the new EU Commission President, for example, has urged for a "geopolitical commission" and "technological sovereignty" for the Union in strategic sectors (Koenig, 2019). More than 30 countries around the world have already published their national AI strategies (Dutton, 2018). Following behind what other EU and NATO members did may have been acceptable in the past, but not anymore. Both internal EU fatigue and the unfinished (and now even more complicated) business of integration on the one hand and the NATO internal struggle on the other (Rizzo, 2020), are leaving no other options for the SEE leaders.

A strategic update and, consequently, profound changes in the SEE organizational, operational and cooperation framework in the context of CIP and CIIP may be inevitable. On 14 November 2019, the EU Institute for Security Studies (EUISS) and the Finnish Presidency of the Council of the EU co-organized a conference in Brussels on EU-NATO relations and Artificial Intelligence, where experts concluded that while "the exact impact" of AI "…remains unclear, there was consensus that AI-enabled systems would inevitably transform defence across the board" (The EU Institute for Security Studies, 2019). Furthermore, given that national defence and security is not the main driver of the development of AI, there are concerns about the erosion of the national military and security ability to maintain its technological edge and ensure the uptake of its concerns by civilian developers. The former US Secretary of Defence, James Mattis, during the announcement of the US National Defence Strategy, underlined that

"success does not go to the country that develops a new technology first, but rather, to the one that better integrates it and more swiftly adapts its way of fighting"(Mattis, 2018).

The changes and strategic updates need to be realistic and based on the SEE contemporary security assessments and perception under the Euro-Atlantic framework. The SEE countries no longer have the luxury of simply implementing security concepts that work for the EU or NATO Allies; without a proper adaptation that reflects the cultural perspectives or other region-based dynamics, these concepts will not give the expected results. Of course, general trends need to be reconsidered and put into the SEE security context.

SEE governments need to reconsider prevention. Reducing risk and mitigating cascade effects in the new, unpredictable and complex security environment, require that critical infrastructure organizations must take a more holistic view of the critical infrastructure ecosystem. A cultural shift under the whole of society's mode of application is necessary. Not just security personnel but all the administration and related private-sector employees in the CIP and CIIP system need a whole new level of awareness of the contemporary hyper-based threats. Embracing a holistic zero-trust approach that prioritizes prevention strategies over reactive detection methods and avoiding an "it is not going to happen to me" culture is urgent. Therefore, existing detection or consequence management policies and procedures need to be reconsidered in the context of prevention.

The SEE leadership needs to rethink resilience in the age of AI applications and systems. A US Department of Homeland Security study concluded that one of the major risks to CIP in the age of AI is potential mass unemployment (The US Homeland Security, 2017). Led by efficiency, many private sector companies in the chain of CIP and CIIP in SEE will eventually implement AI systems. At the same time, the threat vectors landscape is drastically changing, which urges the SEE leadership to reconsider not just employment policies but also contingencies in the security protocols for effective CIP and CIIP with AI systems. Therefore, an open dialogue in advance and a regulatory platform that will reduce new potential vulnerability gaps and data privacy concerns under the SEE governments' leadership is necessary.

Mitigate risks with training and awareness. The human factor is the number one security risk to SEE CI and CII. At the same time, SCADA- (Supervisory Control and Data Acquisition) run systems and the whole cybersecurity policy and industry related to CI and CII in SEE are predominantly led by IT experts. While this group of SEE society remains a valuable factor in CIP and CIIP, they lack security (not safety) training and geopolitical awareness. A brief overview of the educational and training institutions in SEE would lead one to conclude that except for some programmes and curriculums there is a general separation between defence and security, policy, legislation and economic and IT-based educational programmes and curriculums. Furthermore, the same separation exists in the private sector. Corporate management rarely has a holistic approach to corporate security, and the requirements are just profit-oriented. National security considerations are either sporadically considered if there is a legal requirement, or not considered at all. While many of these companies address supply chain risks by certifying the cybersecurity practices of their partners, basic security awareness and training often lags behind other industries (Czarny, 2020). Hence, the SEE governments need to reconsider this and initiate a multidisciplinary training approach, as well as stimulating multidisciplinary professionalization of administration and private sector employees.

Establish lessons learned or lessons identified practices and codify best practice. Although AI systems represent a science fiction for now and will introduce novelty, sharing best practices and lessons identified and learned is a must for SEE. In general, this practice is very poorly developed in many of the SEE countries in the CIP and CIIP context. A closer look into governments' budgeting rarely finds funds devoted to this type of activity (if any at all could be found). By developing models and forums for lessons learned, SEE will improve prevention, consequence management, and resilience to hyper-based threats. Moreover, this will help in prescribing and codifying these practices into regulation. This will eventually create a platform to raise awareness and mitigate upcoming hyper threats before it is too late.

6 Conclusion

Technological development, along with the intensified process of globalization and changes in the global political scene, has introduced new, highly unpredictable security threats. The contemporary security environment is complex and filled with asymmetric, cyber and hybrid-based threat vectors. Non-state actors and some states are using cyberspace and modern technologies to challenge South-Eastern European democracies through different sectors of society. The ongoing geostrategic competition and the artificial intelligence (AI) race are bringing new uncertainties to the context of critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP). AI applications and systems are defying assumptions about human limitations in terms of space and time. As a result, their application in the security and defence sector is merging asymmetric, cyber and hybrid-based threats into a new level of hyper threat vectors.

SEE leaders need to seriously consider the potential impacts of AI in the general security and specific CIP and CIIP contexts. AI is already changing perspectives and the understanding of what we consider as CI or CII. The threat in these terms is two-fold. Interconnectivity and interdependence intended for efficiency and welfare can cause unpredictable cascade effects. Compromising AI applications or systems that run CI and CII even of a friendly or partner country can cause severe strategic, economic and security consequences. In a digitally dominated world where AI applications and systems control and execute crucial functions, knowledge is changing fast and with that, the existing threats and threat vectors are evolving to hyper-threats.

The trend of digitalization with the purpose of efficiency is heading toward the conclusion that AI will eventually be implemented in the CIP/CIIP processes. This, however, will drastically change the approach in the overall process of CIP/CIIP. Therefore, the existing strategies, policies and tactics, techniques and procedures for CIP and CIIP need to be revised and updated to meet the current situation. Before that, however, SEE leaders need to comprehend that the hyper threats are around the corner and will become reality.

7 References

1. Ackerman K. Robert, (February 8, 2018), "Hyperwar Is Coming Faster Than You Think", Signal AFCEA, accessed at: https://www.afcea.org/content/hyperwar-coming-faster-you-think
2. Alic, Anes, (November 01, 2011), *III-Planned terror attack on US Embassy in Sarajevo*, ISA Intel, available at: . http://www.isaintel.com/2011/11/01/ill-planned-terror-attack-on-us-embassy-in-sarajevo/
3. Allen R. John & Hussain Amir, (July 10, 2017), "On Hyperwar" Fortuna's Corner, accessed at: https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain/,)
4. Badie Bertrand, (2012), "Transnationalizing Diplomacy and Global Governance" in Kerr, Pauline & Wiseman, Geoffrey, (Eds.) Diplomacy in a Globalized world, Theories and Practices. Oxford University Press.
5. Barton Tim, (2019), "AI offers the ability to reduce the cognitive burden on soldiers", Video interview with Sarah Sicarrd, C4ISRNET, accessed at: https://www.defencenews.com/video/2019/10/21/ai-offers-the-ability-to-reduce-the-cognitive-burden-on-soldiers/
6. BBC, (June 27, 2010), "One Killed In Central Bosnia Bombing", BBC News, retrieved February 2, from: http://www.bbc.co.uk/news/10428626
7. BBC, (July 19, 2012), Bulgaria Blast, Suicide bomber kills Israeli, BBC News, available at: http://www.bbc.co.uk/news/world-europe-18897772
8. Berteau David, (May 15, 2018), "More signs pointing to AI's growth in the federal market," Washington Technology, accessed at: https://washingtontechnology.com/articles/2018/05/15/insights-berteau-ai-trends-opportunity.aspx
9. Best L. Katharina, Schmid Jon, Tierney Shane, Awan Jalal, Beyene M Nahom, Holliday A. Maynard, Khan Raza, Lee Karen, (2020) *How to Analyze the Cyber Threat from Drones*, RAND, accessed at: https://www.rand.org/pubs/research_reports/RR2972.html
10. Bodansky Yossef, (2001), *Bin Laden: The Man Who Declared War on America.* New York: Forum.
11. Bostrom Nick, (February 09, 2017), "Strategic Implications of Openness in AI Development", Wiley Online Library, accessed at: https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12403
12. Bur Jessie, (November 29, 2017), "IoT is changing the meaning of 'critical infrastructure'", Federal Times, accessed at: https://www.federaltimes.com/smr/cybercon/2017/11/29/iot-is-changing-the-meaning-of-critical-infrastructure/
13. Chery Steve, (October 10, 2010), "How Stuxnet will rewrite the cyberterrorim playbook", accessed at: http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook
14. Cyber edu, (2007), "Critical Infrastructure Protection Defined and Explained" accessed at: https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip
15. Czarny Benny, (January 31, 2020), " Embracing a Prevention Mindset to Protect Critical Infrastructure", DarkReading, accessed at: https://www.darkreading.com/vulnerabilities---threats/embracing-a-prevention-mindset-to-protect-critical-infrastructure-/a/d-id/1336907
16. Dormehl Luke, (September 11, 2018), "The history of drones in 10 milestones" Digital Trends, accessed at https://www.digitaltrends.com/cool-tech/history-of-drones/
17. Dimitrioska, Pandorce (April 13, 2012), Five murdered at Iron Lake, There are no suspects, (Original: петтмина уб*иени кај Железарското Езеро*, *Осомничени нема*), Alfa TV, available at: http://www.time.mk/read/85fe05db07/a5bc958d44/index.html

18. Dutton Tim, (June 28, 2018), "An Overview of National AI Strategies", Medium.com, accessed at: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

19. Euhus T. Brandon, (2019), "A Clausewitzian Response to "Hyperwarfare"", Parameters, accessed at: https://www.questia.com/library/journal/1G1-580097642/a-clausewitzian-response-to-hyperwarfare)

20. European Commission, (February 19, 2020), "White Paper, On Artificial Intelligence – a European approach to excellence and trust", COM(2020) 65 final, p10, accessed at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

21. F2N2, (December 21, 2019), "Russia's Strategic Interests and Tools of Influence in the Western Balkans" , accessed at: https://f2n2.mk/en/russias-strategic-interests-and-tools-of-influence-in-the-western-balkans/

22. Feyerabend C. Florian, (2018), "The influence of external actors in the Western Balkans", Konrad Adenauer Stifrung, accessed at: https://www.kas.de/c/document_library/get_file?uuid=194afc48-b3be-e3bc-d1da-02771a223f73&groupId=252038

23. Fitzgerald Ian, (2019), "Securing Critical Infrastructure with Artificial Intelligence", CIO Review, accessed at: https://cybersecurity.cioreview.com/cioviewpoint/securing-critical-infrastructure-with-artificial-intelligence-nid-26995-cid-145.html

24. Follath Erich & Stark Holger, (November 2, 2009), "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor", Spiegel Online International, accessed at: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

25. Fuller B. Richard, (1982), *Critical Path*. Library of Congress.

26. Geer David, (February 12, 2014), "Statistics point to increased physical danger risks of cyberterrorism", CSO Online, accessed at: http://www.csoonline.com/article/2134376/malware-cybercrime/statistics-point-to-increased-physical-danger-risks-of-cyberterrorism.html

27. GLOBSEC, (2018), "Future War NATO? From Hybrid War to Hyper War via Cyber War". GLOBSEC.

28. Hadji-Janev, Metodi, (2012) "Managing the consequences of terrorist attacks: the case of Macedonia", in: Chaleta D. & Shemella P. (Eds.) *Managing the Consequences of Terrorist Acts - Efficiency and Coordination Challenges*, 2012, ISBN: 978-961-92860-5-0, available at: http://www.ics-institut.com/research/books/4.

29. Hadji-Janev, Metodi and Jovanovski, Vlatko (2013) The concept of resilience and protection of critical infrastructure against natural and man-made disasters in Republic of Macedonia". In: *Book of Papers 6th International Conference "Crisis Management Days"*, Nova Gorica, 6th International Conference.

30. Heffelfinger Christopher, (July 2013), "The Risks Posed by Jihadist Hackers", CTC Sentinel, Vol.6 Issue 7, accessed at: https://ctc.usma.edu/the-risks-posed-by-jihadist-hackers/

31. HPC, (July 29, 2019) "AI Enters the Front Lines of National Defence and Security", HPC Wire com, accessed at: https://www.hpcwire.com/2019/07/29/ai-enters-the-front-lines-of-national-defence-and-security/)

32. Ismail Nick, (January 22, 2018), "The Internet of Things: The security crisis of 2018?", Information Age, accessed at: https://www.information-age.com/internet-things-security-crisis-123470475/

33. Jans Karlijn, (July 10, 2018), "NATO Needs to Get Smarter About AI", Atlantic Council, accessed at: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-to-get-smarter-about-ai/

34. Koenig Nicole, (December 26, 2019), "The Pitfalls Of A 'Geopolitical' European Commission", BIRN, accessed at: https://balkaninsight.com/2019/12/26/the-pitfalls-of-a-geopolitical-european-commission/

35. Lachert Jakub, (July 8, 2019), "Western Balkans and Geopolitics", Warsaw Institute Review, No11, Issue 4, accessed at: https://warsawinstitute.org/western-balkans-geopolitics/

36. Lauchlan Stuart (2019), "Armageddon by AI – declarations of Hyper War to scare Dr Strangelove", accessed at: https://diginomica.com/armageddon-ai-declarations-hyper-war-scare-dr-strangelove

37. Marr Bernard, (September 28, 2018), "Artificial Intelligence: What Is Reinforcement Learning – A Simple Explanation & Practical Examples", Forbes, accessed: https://www.forbes.com/sites/bernardmarr/2018/09/28/artificial-intelligence-what-is-reinforcement-learning-a-simple-explanation-practical-examples/#f4f5fb4139ce.

38. Marisetty Suresh, (May 1, 2019), "Why You Should Care About Threat Modelling", Security Blog, accessed at: https://community.arm.com/developer/ip-products/security/b/security-ip-blog/posts/why-you-should-care-about-threat-modelling?utm_source=google&utm_medium=cpc&utm_campaign=2019_ebg-security_mk01-1_na_na_bol&utm_content=blog&utm_term=%2Biot%20%2Bvulnerabilities&gclid=Cj0KCQjw9ZzzBRCKARIsANwXaeKdcOd-W_XNAkboeaLWvb8twcNebacriKmStJdfeX0VvE4STcV_a0aAl_yEALw_wcB

39. Mattis N. James, (January 19, 2018), "Remarks by Secretary Mattis on the National Defence Strategy", US Department of Defence, accessed at: https://www.defence.gov/Newsroom/Transcripts/Transcript/Article/1420042/remarks-by-secretary-mattis-on-the-national-defence-strategy/

40. NATO ACT, (October 25, 2019), "Artificial Intelligence – A Game Changer for the Military", accessed at: https://www.act.nato.int/articles/artificial-intelligence-game-changer-military)

41. Nye Joseph, (November 13, 2018), "Protecting Democracy in an Era of Cyber Information War", Hoover Institution, Fall Issue, 318, accessed at: https://www.hoover.org/research/protecting-democracy-era-cyber-information-war

42. O'Donnell Shea, (June 16, 2019), "A Short History of Unmanned Aerial Vehicles", Consortiq, accessed at: https://consortiq.com/media-centre/blog/short-history-unmanned-aerial-vehicles-uavs.

43. Osborne Charlie, (January 27, 2020), "The US Army uses facial recognition to train AI. Now, it needs to protect it", ZDNet, accessed at: https://www.zdnet.com/article/the-us-army-uses-facial-recognition-to-train-ai-now-it-needs-to-protect-it/

44. Patriot Act, (2001), the US Government Publishing office, accessed at: https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

45. Pirovska Uranija, ed. (2018), "Annual report for 2018 – The rights of refugees, migrants and asylum seekers in the Republic of Macedonia", Helsinki Committee for Human Rights of the Republic of Macedonia, accessed at: https://mhc.org.mk/wp-content/uploads/2019/05/Help-On-Route-ANG-2018-final.pdf

46. Rizzo Rachel, (February 01, 2020), "NATO: the challenge from within", Observer Research Foundation, accessed at: https://www.orfonline.org/expert-speak/nato-challenge-from-within-60977/

47. Rosenberg Marc, (April 13, 2013), "Knowledge Doubling Every 12 Months, Soon to be Every 12 Hours", Industry Tap, accessed at: https://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950

48. Siddiqui S., Kuly, (December, 2018), "Artificial intelligence and the risks of a 'hyper-war'", Asia Times, accessed at: https://asiatimes.com/2018/07/artificial-intelligence-and-the-risks-of-a-hyper-war/

49. Stewart Phil (December 21, 2016), "Exclusive: U.S.-supplied drones disappoint Ukraine at the front lines", Reuters, accessed at: https://www.reuters.com/article/us-usa-ukraine-drones-exclusive-idUSKBN14A26D

50. The European Commission, (2018), "Shaping Europe's digital future, Artificial Intelligence" accessed at: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

51. The EU Institute for Security Studies, (November 14, 2019), "The EU, NATO and Artificial Intelligence", Conference Report, accessed at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20NATO%20AI%20-%20Report.pdf

52. The US Congress, (1988), "The Nation at Risk, Report of the President's Commission on Critical Infrastructure Protection", United States. Congress, Senate, Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Volume 4.

53. The US Election Commission, (2017), "Elections – Critical Infrastructure, Election Management", Resources accessed at: https://www.eac.gov/election-officials/elections-critical-infrastructure

54. The US Election Assistance Commission, (2017a), "Starting Point: US Election Systems as Critical Infrastructure", accessed at: https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

55. The US Homeland Security, (July 2017), "Narrative Analysis Research Paper, Artificial Intelligence", National Protection And Programs Directorate | Office Of Cyber And Infrastructure Analysis, accessed at: https://info.publicintelligence.net/OCIA-ArtificialIntelligence.pdf

56. Triolo Paul, Kania Elsa, & Webster Graham, (January 26, 2018), "Translation: Chinese government outlines AI ambitions through 2020", New America, accessed at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/

57. Yonah Alexander, (2018), "Security Challenges in the Balkans", The Inter-University Centre for Terrorism Studies, accessed at: https://potomacinstitute.org/images/stories/publications/Security_Challenges_in_the_Balkans_Report.pdf

58. Valášek Tomáš, (August 31, 2017), "How Artificial Intelligence Could Disrupt Alliances" Carnegie Europe, accessed at: https://carnegieeurope.eu/strategiceurope/72966.)

59. Valášek Tomáš, (February 16, 2018), "European defence vs. NATO: Not the right fight", Politico, accessed at: https://www.politico.eu/article/european-defence-vs-nato-not-the-right-fight/

60. Villani Cédric, (March 8, 2018), *For a Meaningful Artificial Intelligence Towards a French And European Strategy for AI,* Mission assigned by the Prime Minister Édouard Philippe, accessed at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

61. Walch Kathleen, (December 22, 2019), "Why Cognitive Technology May Be A Better Term Than Artificial Intelligence", Forbes, accessed at: https://www.forbes.com/sites/cognitiveworld/2019/12/22/why-cognitive-technology-may-be-a-better-term-than-artificial-intelligence/#7c8cd006197c

62. Willke J. Bradford, (September 19, 2007), "A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events", Carnegie Mellon University, accessed at (https://www.enisa.europa.eu/topics/csirts-in-europe/files/event-files/ENISA_best_practices_for_ciip_Willke.pdf

2 Cyberterrorism Threats to Critical Infrastructure: Coordination and Cooperation from Brussels to South-Eastern Europe and back

Robert Mikac, Krešimir Mamić, Iva Žutić

1 Introduction

Physical and virtual infrastructure makes it possible to maintain the current level of development of individuals, society, organizations and states, as well as their progress. It includes static elements such as bridges, tunnels and pipelines; dynamic elements such as numerous transport platforms like rail, air and road vehicles; and virtual ones such as the internet, digital services and their content. These and numerous other examples of infrastructure – besides ensuring that development, investment and quality of life make environments that have a better combination of individual and collective solutions more competitive than others – are characterized by openness, accessibility and mass use. Infrastructure is expected to be reliable, long-lasting, cost-effective and continuously progressing, for a modern way of life and constant acceleration in all social and economic processes.

Infrastructure as a term and concept concerning its essential function – to be a medium for the production, transmission and exchange of various products and services – is viewed from three fundamental perspectives. Firstly, we look at it as a series of objects, networks and systems that have a specific and predetermined function (social, economic, security); secondly, as providing services to numerous individual users; and thirdly, noting that all infrastructure uses IT support for its functioning. The emphasis in the first case is on the mechanical parts of the infrastructure, in the second on the possibilities it provides, and in the third on its dependence on its IT component. The interactivity of these perspectives is beyond question, and for the sake of completeness of understanding and analysis, they should be considered together as much as possible.

It is important to emphasize that not all infrastructure is critical, nor is all critical infrastructure equally valuable. For the operational definition of critical infrastructure in this paper, we take a sufficiently broad definition from the European Commission: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets

which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments" (European Commission, 2004: p 3). Concerning responsibility for the protection of critical infrastructure, we will refer to the Council of the European Union's conclusion: "The primary responsibility for protecting critical infrastructures falls on the Member States, owners, operators and users (users being defined as organizations that exploit and use the infrastructure for business and service provision purposes). Member States authorities will provide leadership and coordination in developing and implementing a nationally consistent approach to the protection of critical infrastructure within their jurisdictions, taking into account existing Community competences. The responsibility for carrying out risk and threat assessments therefore lies primarily with the Member States" (Council of the European Union, 2007: p 2). According to the above, it is evident that the states are primarily responsible for protecting critical infrastructure in collaboration with owners, managers and users, while the EU can help them coordinate all the processes. This is an important inference for subsequent discussion.

Critical infrastructures possess, have in place, create and/or are exposed to certain security risks that are significant to their functioning or to the processes they enable. These risks may be natural (such as earthquakes, fires, floods, storms, ageing, climate change and the like); technical and technological (caused by processes and components in the operation of critical infrastructure); or intentionally or unintentionally created by humans (such as improper handling, theft, vandalism, sabotage, espionage, terrorism). Risks created by people with intent are called threats and can be internal and external. Internal threats are generated within the system being protected, while external threats are generated by attackers not directly connected to the critical infrastructure. This study generally focuses on the threats of terrorism, and specifically on cyberterrorism against critical infrastructure, regardless of its origin.

Terrorism has many definitions, but for this paper we have decided to use the following one: "Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them" (United Nations, 1994). For cyberterrorism, we use the straightforward and broad definition of the Merriam-Webster dictionary (2020): "Terrorist activities intended to damage or disrupt vital computer systems." Therefore, cyberterrorism in this study represents an active threat and/or attack on the IT components of critical infrastructure to achieve specific political goals. However, there is a need to differentiate cyberterrorism from other forms of cyber-attacks to critical infrastructure and misuse of the internet for terrorist purposes. The main challenge of cyberterrorism is to prove a substantial political impact of the attack and an intention to provoke coercion against a state or international organization for individual political decisions.

Of all the security risks and/or threats to the functioning of critical infrastructure, terrorism is one of the most significant. It is essential to highlight that although it is one of the most significant it is by no means the most important, to avoid the logic trap of sectoral experts who claim that the jobs they are engaged in are more important than others. Catherine De Bolle, Executive Director of Europol, believed that: "In 2018, terrorism continued to constitute a major threat to security in EU Member States" (Europol, 2019: p 4), and for the Security and Intelligence Agency of the Republic of Croatia: "Terrorism is still the most prominent and the most visible threat to the international security and the security of European citizens" (2018: p 10).

However, why is terrorism one of the most significant security threats to the functioning of critical infrastructure? Because of its background, unpredictability and unexpectedness. Because it represents an act which is politically inspired, an act which involves violence or the threat of violence, and an act which has a strong psychological impact, as well as because of the consequences that arise. These consequences (manifested in human suffering, property damage, financial loss and damaged reputation) are likely to be of a lesser degree than a devastating natural or technical and technological event. Still, they are far more worrying for politicians and decision-makers, because they indicate vulnerability to human attack, the possibility of critical infrastructure being threatened by someone from the outside, and the way in which national systems of particular interest were not sufficiently protected. All of the above concerns the subjective side of looking at and dealing with security risks and threats. We, as authors, academically and professionally dealing with various security fields, are verifiably aware that countries are investing far more diverse resources in counter-terrorism, which is most likely to cause far fewer consequences than more apparent risks (such as natural or technical-technological) which, if materialized, would cause far-reaching consequences. We have stated this to emphasize the position that not only are we aware of the threat of terrorism, but also that its risks should not be exaggerated.

These considerations lead us to the research problem – which we want to observe from different dimensions – which is, how much is critical infrastructure (honestly) at risk of cyberterrorism in the European Union, South-Eastern Europe and the Republic of Croatia?[1] We will examine the above by considering the types of cyber threats against critical infrastructure, the proportion of cyberterrorism within the entire spectrum of threats, and how many such attacks have been attempted and implemented against critical infrastructure. The subject of the research we wish to analyze is set out to consider public policies and activities to protect critical infrastructure from terrorist threats at the level of the European Union, South-Eastern Europe and the Republic of Croatia. The research objective is to investigate the extent to which the official policies of the entities under review in the area of protection of critical infrastructure from terrorist threats are operational in implementation. The reason behind this is the fact that protection of critical infrastructure is unenforceable without proactive national and international coordination mechanisms, as well as inter-organizational cooperation within counter-terrorism processes. With regard to the research objective, it should be noted that the strategies, directives and laws inevitably state the necessity and exigency of protecting critical infrastructure from threats of terrorism. Therefore, the main research question of this paper is: How much are public policies of protection of critical infrastructure from (cyber)terrorism operationalized in practice? The purpose of this research is to provide, through the results of the study, recommendations concerning stronger cooperation and coordination in this area.

This research is a qualitative study that seeks to answer the problem, subject and objectives of the research, and the research question. We have opted for qualitative research because it aims to provide a more in-depth insight into the subject, to achieve a holistic approach to the research, and to explain the conclusions we have reached. The methodological framework of this research is composed of system theory and the following research methods: generalization, the deductive method, the inductive method, the analysis method, and the synthesis method. System theory is used in interdisciplinary research to study the relations and relationships of the system parts and

1 We will explain the role of the Union later. The Republic of Croatia is used as a link between the Union and South-Eastern Europe, as it belongs to both entities (politically it is an integral part of the Union and geographically it is located in the region of South-Eastern Europe, where it has a shared history, numerous links and significant collaboration in many areas with certain countries).

the functioning of the system as a whole. It will serve to analyze the actions of different actors and set-up mechanisms and processes.

The method of generalization will be used to observe specific countries of South-Eastern Europe (Croatia, Bosnia and Herzegovina, Serbia, Montenegro, Northern Macedonia and Kosovo) through the prism of the Republic of Croatia, since the other countries mainly follow the path and development of normative acts and operational activities (the issue of Euro-Atlantic integration, peacekeeping missions, civil protection, critical infrastructure and so on) modelled on the Republic of Croatia. The other countries of South-Eastern Europe will not be considered in this study because of their extraordinary heterogeneity and significant diversity from the specified countries.

With the deductive method, we will derive individual points of the view from the general ones. If we determine the level of normative regulation and cooperation at the level of the EU, we can draw an inevitable conclusion about the regulation and activities of the protection of critical infrastructure at the level of the Republic of Croatia. The inductive method, however, will lead us to general conclusions based on individual facts, which means that by analyzing the capacity to protect critical infrastructure from terrorism in the Republic of Croatia, we will come to an understanding of the coordination capacity at the level of the EU.

The method of analysis will be used to investigate individual parts in relation to the whole through the breakdown of complex structures. With this method, we will analyze the entire system of protection of critical infrastructure both at the EU and the Croatian level by analyzing the subsystems, elements and measures of protection (holders of authority, participants and operational forces, public policies, principles of functioning and activation within the system, etc.).
We will use the synthesis method to explain specific settings by compiling simple pieces into more complex ones. That is, we will explain the system of protection of critical infrastructure from terrorism at the EU and Croatian levels by linking the processes of identification, specification and protection of critical infrastructure, the application of sectoral and cross-sectoral benchmarks, the importance of establishing public-private partnerships, and data secrecy protection. Throughout our research based on system theory and the methods outlined above, we will uphold a cross-cutting approach to combine and compare the results of the research and ultimately to be able to provide recommendations based on the research.

Research set up in this way has some limitations. The first limitation is in the selected research samples, the European Union and the Republic of Croatia as representative of both the EU and of part of South-Eastern Europe; the analysis of these two entities will only lead to a partial picture of the subject area, since a more in-depth analysis would need to cover all the countries of South-Eastern Europe, which is beyond the scope of research appropriate to one article.

The next limitation should also be explained in the light of the subtitle of this paper: *Coordination and Cooperation from Brussels to South-Eastern Europe and Back*. The observed countries are highly oriented towards Brussels in many ways, including the areas of interest of this research. They aspire to join the European Union and the NATO Alliance (except for Serbia, which is militarily neutral and does not intend to apply for full membership of NATO), and see Brussels as a natural place for coordination and cooperation. Brussels does serve as a point of coordination, but without a management function, which it is important to point out.

This brings us to the final limitation, also partly related to the subtitle, which represents a dichotomy in the implementation of official policies and operational activities from Brussels to South-Eastern Europe and back. Countries in the EU and those seeking full membership are aligned with Brussels' guidelines in the area of protection of critical infrastructure and the issue of cooperation in the prevention and fight against terrorism. The challenge is that although Brussels (where all Member States are represented in the development of policies adopted in Brussels) sets development guidelines in both areas, it cannot affect the implementation of Member States' national policies, much less those of non-members. As critical infrastructure and the issues of preventing and combating terrorism are areas of national security in each country, the countries themselves decide on their level of cooperation with other countries and with Brussels. Concerning Brussels itself, the multiple capital city, although both organizations (the EU and NATO) are based in Brussels and have their own policies and coordination mechanisms for critical infrastructure protection, we have pragmatically decided to consider only activities that come from the European Union, because the role of NATO is much smaller in this area. Likewise, we consider this area to be a predominantly civil matter, and we will consider it as such. We do not dispute the position and role of armed forces in the protection of critical infrastructure, but we also place that outside the scope of our interest in this research. So, when we mention Brussels, we mean the activities of the European Union.

This paper is divided into several sections. First, we introduced the foundational concepts, set specific relationships, and explained the research framework. The following section summarizes the indicators of cyber threats against critical infrastructure. This is followed by a section dedicated to the EU, outlining the strategic and normative framework of the critical infrastructure protection area, with particular reference to threats of terrorism. The section is accompanied by the same overview for the Republic of Croatia. Next, we analyze the operational level of protection of critical infrastructure at the EU level, which will be presented through the cross-sectoral activities of professional communities dealing with critical infrastructure and counter-terrorism, to determine their links and cooperation. The same will be done for the Republic of Croatia. In the Conclusion, we will summarize the research findings and propose specific recommendations for improving cooperation and protecting critical infrastructure from terrorism.

2 Cyber Threats to Critical Infrastructure

Cyber threats are threats of disruptions and attacks towards IT infrastructure. The European Union Agency for Network and Information Security (ENISA), in its *Threat Landscape Report* from 2018, identified 15 main cyber threats in the world: malware (malicious software designed to cause intentional damage to IT infrastructure – viruses, worms, spyware, Trojan horses); web-based attacks (through web systems such as browsers, extensions, websites and web services); web application attacks (using weaknesses in web services and applications); phishing (defrauding information by posing as a legitimate company and sending emails and messages with a malicious attachment, URL, etc.); disturbed denial of service – DDoS attack (disruption to the regular traffic of a server, service or network by overwhelming it with internet traffic); spam (flooding users with unsolicited emails or messages); botnets (connected devices that are running bots, i.e. software applications that run automated tasks like DDoS attacks); data breaches (successful outcomes of cyber threats as leakage or exposure of data); insider threat (within a company or organization); physical manipulation/damage/theft/loss

(of a storage device); information leakage; identity theft; cryptojacking (or cryptomining – use of device processing power to mine cryptocurrencies); ransomware (ransom of blocked files and devices); and cyber espionage (ENISA, 2019: p 9). All of the above cyber threats could be used against critical infrastructure, and if their character and consequences had political goals, they could be identified as cyberterrorism.

Malware is the most common cyber threat (ENISA, 2019: p 26), and there have been several well-known malware attacks against critical infrastructure across the world. Uncovered in 2010, a computer worm named *Stuxnet* caused substantial damage to Iran's nuclear programme, as it targeted supervisory control and data acquisition (SCADA) systems. It is widely believed to have been unleashed by Israel and the United States (Nakashima & Warrick, 2012). *Industroyer* was malware used in a cyber-attack on a power grid in Ukraine on December 17, 2016, which cut off power to a fifth of Kyiv. This attack was the second attack on Ukraine's power grid; the first was in 2015 (Polityuk et al., 2017). In 2017, the malware *Triton* was discovered in Saudi Arabia, attacking a petrochemical plant by disabling instrumented safety systems (ENISA, 2019: pp 28-29). Web or web application based attacks can also be used as an attack on critical infrastructure through an unsuspecting insider or client by spamming campaigns or trojans. In 2007, after a controversy about moving a communist-era monument, the Bronze Soldier, from the centre of Tallinn to a military cemetery, Estonia was hit by cyber-attacks orchestrated by Russians. Attacks in the form of a spam campaign spreading false news sparked riots by a Russian minority, and at the same time extreme levels of internet traffic took down the online services of government bodies, banks and media (McGuinness, 2017).

A web-based attack unveiled in 2018 "abused the deep packet inspection hardware, used by Turks telecom, redirecting customers in Turkey and Syria to download spyware" (ENISA, 2019: p 33). Although this does not sound as sinister as previous threats, phishing is so prevalent that "90% of malware infections and 72% of data breaches in organizations originate from phishing attacks" (ENISA, 2019: p 40). With spearphishing these attacks are specifically targeted, like sextortion scams towards rich or influential individuals, or individuals with access to sensitive business data. Nation-state actors use spearphishing as a primary infection vector for espionage and disruption operations (ENISA, 2019: p 42). However, to utilize spearphishing, the hackers first need to get their hands on individual records, i.e. perform data breaches. The best-known incident, *Cambridge Analytica-Facebook,* is one of six social media data breaches, while the healthcare sector leads with 27% of incidents (ENISA, 2019: p 64). As a direct result of global service connectivity and its dependency on the Internet of Things (IOTs) there is a warranted threat from DDoS attacks on nations' critical infrastructure such as hospitals, public transport, and so on. Utilizing DDoS, botnets attacked Ricardo Anaya's campaign website during Mexico's presidential elections and the Ukraine president's website, and are responsible for the failure of operations of the largest train service provider in Denmark (ENISA, 2019: pp 47-48).

Insider threat accounts for 77% of data breaches in companies, exists in every government, organization or company, and can be a threat from (a) intentional malicious insiders, (b) negligent insiders, and (c) unintentionally compromised insiders (ENISA, 2019: p 69). Types of data that are at risk of breach from insider threats are financials, costumers/employees' data (57%); credentials, passwords (52%); sensitive personal information (49%); trade secrets, research product designs (32%); employee data (31%); and network, infrastructural control (27%) (ENISA, 2019: p 71). Unintentionally compromised insiders make unintentional data

breaches by way of phishing (67%), weak/reused passwords (56%), unsecured devices (44%), sharing passwords (44%) and unsecured WiFi networks (32%) (ENISA, 2019: p 72). An individual usually leaks information by unintended disclosure (72.2%), while hacking or malware is responsible for 27.1% of leakage and physical loss only 0.1% (ENISA, 2019: p 79). Most data leakage incidents happen in governmental organizations (ENISA, 2019: p 81), such as when the fitness tracking app Strava, via collected information, disclosed the locations of US, Russian and UK secret military bases in Syria and Afghanistan (ENISA, 2019: p 82). Cryptojacking is a relatively new cyber threat it but has already found its way to critical infrastructure in Europe: "in February 2018, the first incident of cryptomining malware was found in SCADA systems of a water utility" (ENISA, 2019: p 95).

Ransomware is a dire cyber threat that targets critical infrastructure, usually healthcare organizations, by ransoming medical devices. Unlike cybercriminals who create ransomware for the ransom, the assumption is that nation-state actors create ransomware as a cover for cyberterrorism, like they did with the WannaCry (North Korea suspected) and NotPetya (Russia suspected) attacks. WannaCry attacked mostly healthcare organizations, infecting more than 200,000 computers in 150 countries and collecting more than 312 ransom payments, and the Boeing aircraft manufacturing company (ENISA, 2019: p 103). NotPetya mostly infected computers in Ukraine, including those of the National Bank of Ukraine, while the ransomware PyLocky targeted European countries in 2018. Nevertheless, we must be very careful here about connecting cyberterrorism and states, because it raises the question of how much we are willing to label a country with cyberterrorism.

Cyber espionage, a nation-sponsored type of cyber-attack, has been utilized in a more significant amount in recent years against "industrial sectors, critical and strategic infrastructure across the world including government entities, railways, telecommunication providers, energy companies, hospitals and banks", and "focuses on driving geopolitics, stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields" (ENISA, 2019: p 107). The most active and capable cyber actors in economic espionage in the world are Russia, China and Iran, with North Korea not far behind. Some well-known cyber espionage threat-groups or campaigns are *ZooPark* (targeted Android users in Asia and North Africa and an independence referendum in Kurdistan); *Powerstats* and *Pipefish* (targets users in West and South-West Asia, North Africa, and the Middle East); an Iranian campaign, Myket, via updates in the marketplace; and *Operation Parliament* (infiltrating top governmental, judicial, military and intelligence bodies, as well as large companies, mostly in the Middle East and North Africa) (ENISA, 2019: p 111). Most critical for the EU is the Russian campaign *APT28*, which has targeted the Emmanuel Macron campaign, the Montenegro Parliament, Embassies in Europe and Russia, and the European Defence Agency, as well as compromising the networks of the German Bundestag, the French television network TV5 Monde, WADA (the World Anti-Doping Agency), FIFA (Fédération Internationale de Football Association) and a Ukrainian military mobile app (Council on Foreign Relations, 2020).

Looking at the bigger picture, but also focusing on the Republic of Croatia, the Security and Intelligence Agency of the Republic of Croatia states the following: "NATO and the EU members are often under attack by malicious cyber campaigns aimed at undermining the protected communications and information systems. The Republic of Croatia has been a target of a series of cyber-attacks in recent years. These were the so-called APT attacks (Advanced Persistent Threat) which are long-term undetected attacks characterized by high level of expertise, highly complex organization and a plan of attack that includes careful targeting (govern-

ment agencies, critical infrastructure etc.), acquisition of the necessary IT infrastructure that ensures the anonymity of the attacker (usually located in third states), tactics for malicious software implementation (fake e-mail, weblinks, an "infected" device, etc.), infection of the target's ICT system and activation of malicious software in order to steal confidential data from the target, disable its activities, or harm the system. Due to their complexity and costliness, it is reasonable to suspect that individual states sponsor APT attacks. The attacks have targeted mainly protected communications and information systems of state institutions of NATO and the EU members, aimed at collecting intelligence on their diplomatic, military and economic activities. Some of these hacker APT groups are Turla and APT28/Sofacy which have been attacking protected communications and information systems of the members of NATO and the EU for years" (2018: p 26). It should be noted further that in 2019 there were 1129 identified or reported cases of cyber-attacks in Croatia, which is a surge of 65%, mostly phishing, phishing URL and web defacement, and prevention of the spread of MikroTik (malicious cryptocurrency mining software) and a fake password store page (Ivezić, 2020). With regard to critical infrastructure, attacks were noted on banks, schools and other educational institutions, the Croatian Post (Ivezić, 2020), and INA (the Croatian Oil industry) which has been attacked by ransomware infection (INA.hr, 2020).

It is challenging to detect the proportion of cyberterrorism within the entire spectrum of cyber threats and terrorism. This is the main reason why we take several different perspectives into account. ENISA states that just as European countries have raised their efforts to fight terrorism in recent years, they have also done the same in the field of cyberterrorism. Still, terrorism is much easier to detect than cyberterrorism. A great deal and more cyberterrorism is camouflaged behind other cyber threats, as noted in previous paragraphs, and it may seem more benign than it is, as was revealed when explaining spearphishing and unintentionally compromised insiders. For this reason we can separate cyber threat agents' groups into insiders, hacktivists (protesting political/geopolitical decisions affecting national/international matters), script-kiddies, and cyber-criminals, -spies, -offenders and -terrorists (ENISA, 2019: p 119). Europol highlights the topic of the convergence of cyber and terrorism that "[t]here has been much concern and speculation over the past few years that terrorists could turn to launching cyber-attacks against critical infrastructure. However, while the so-called Islamic State (IS) online propaganda appears technologically advanced and their hackers may be well versed in encrypted communication tools, their cyber-attack tools and techniques remain rudimentary" (2019: p 20). In its reports, Europol does not note potential cyber activities of the countries which could be connected via analytical methods with cyberterrorism.

The most common differentiation between cyber-criminal and cyberterrorism is the connection of cyberterrorism with the nation-state. Countries are more and more beginning to understand that they cannot fight cyberterrorism alone, as the cyber-sphere has no borders. Cyberterrorists use legitimate services, mostly social media, to spread propaganda and hysteria via online trolling, bots, fake news, abuse of search engines algorithms and so on to recruit and to raise funds so that they can attack critical infrastructure under the guise of cyber-criminals (banks) and hacktivists (industries). The already-mentioned *Cambridge Analytica-Facebook incident* is a case of a misinformation/disinformation campaign which impacted the UK referendum on EU membership, as the data of 2.7 million EU users of Facebook were used to micro-target and mobilize voters via propaganda and fake news (ENISA, 2019: p 127). Cambridge Analytica was employed by the official Leave.EU referendum campaign, which is being investigated for its Russian-backed financing (Wright, 2018; Kirkpatrick, Rosenberg,

2018; Hern, 2019) and its own ties with the Russian government (Cadwalladr, Graham-Harrison, 2018), and as the primary goal of the campaign, which used data breaches to spam voters, was political, it could be argued that the incident was a case of cyberterrorism. However, it would be hard to prove.

At the end of this section, we need to point out that we have not been able to find a single reference to an example of cyberterrorism in the literature available for analysis. However, we have come across the following opinions: "There has not been so far a single recorded instance of cyber-terrorism" (Argomaniz et al., 2016: p 80, cited in Pierozzi, 2018: p 1) and "although cyberterrorist attacks have not yet materialized, increased level of "know-how" in ICTs will arguably make them more likely to occur" (UNOTC, UN CTED and Interpol, 2018: p 22). This puts before us the analytical challenge of considering and articulating our research topic. We can conclude that cyber threats pose a tremendous and significant threat to critical infrastructure, but so far, no cases of cyberterrorism have been officially recorded, i.e. it is difficult to prove that a particular cyber act is an act of terrorism. This does not mean that the danger does not exist and that it will not occur soon, and therefore, it should be researched.

3 A Strategic and Normative Framework for the Protection of Critical Infrastructure at the EU Level

The EU began to develop critical infrastructure protection in the early part of the 21st century – generally speaking, as a reaction/influence – for three major reasons. The first significant reason is the response to the 9/11terrorist attacks in the United States in 2001, and the follow-up to the US example of the strategic and normative regulation of the area (the Americans represent the global leaders in developing new concepts for strengthening resilience and protecting critical infrastructure). The second reason is a response to terrorist attacks in Europe, in Madrid (2004) and London (2005), where elements of critical infrastructure, as in the case of 9/11, were used to carry out the attacks. The third reason is the impact of the older EU Member States, which developed and put in order the subject matter decades ago in their respective legislations. So, due to both external and internal impulses, EU experts began to regulate the subject matter for the sake of the EU itself, in cooperation with the Member States, and then with other organizations and countries. The following section provides an overview of the strategic and normative acts, as well as particularly significant programmes for the development of this area at EU level.

The first EU security strategy, adopted in 2003 under the title *European Security Strategy: A Secure Europe in a Better World*, mentions infrastructure in a section on the dependency and vulnerability of Europe in the transport, energy, information and other sectors (Council of the European Union, 2003). The next security strategy, *Internal Security Strategy for the European Union: Towards a European Security Model* from 2010, which is primarily focused on internal security, mentions critical infrastructure only once, in the sense of protecting it in order to ensure a high quality of life in Europe (European Council, 2010). In the first *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* from 2013, considerable attention was paid to the need to protect critical infrastructure and critical information infrastructure from all threats, including cyberterrorism (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). In the strategy document *A Global Strategy for the European Union's Foreign And Security*

Policy from 2016 (which replaced the security strategy of 2003), the term and concept of critical infrastructure was significantly emphasized in the need to strengthen the resilience of infrastructure and to invest in its further development and its protection in various areas, including in the cyber domain (European External Action Service, 2016).

The review of strategic documents is followed by an overview of the development of the regulatory framework.

In June 2004, the European Council requested that the European Commission begin developing a comprehensive normative framework for critical infrastructure protection in the European Union. Based on this request, the European Commission first drafted a *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism*, which outlines what Europe should do to prevent terrorist attacks on critical infrastructure, improve emergency preparedness, increase resilience and develop the ability to respond to attacks (European Commission, 2004). The document initiated intensive work by the bodies of the EU, in cooperation with the Member States and individual experts, to develop the EU's regulatory framework and identity in the field of critical infrastructure. The following year the European Commission drafted a *Green Paper on a European Programme for Critical Infrastructure Protection*, which suggested solutions for setting up critical infrastructure protection programmes and the creation of a Critical Infrastructure Warning Information Network (CIWIN) (European Commission, 2005). The next input to the Commission came from the Justice and Home Affairs Council of the Council of the European Union, which in December 2005 requested the drafting of a proposal *European Programme for Critical Infrastructure Protection*. In line with this request, the following year the Commission developed and published the said Programme, which considered all threats to critical infrastructure, with terrorism remaining a primary focus and concern (European Commission, 2006).[2]

Reviewing the document in question, in 2007 the Council of the European Union concluded that the ultimate responsibility for managing critical infrastructure protection solutions rests with the Member States, within their national borders (Council of the European Union, 2008). That same year, the Council passed a *Decision establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks'*. The programme recognizes a number of security risks. It focuses on supporting Member States' efforts to prevent terrorist attacks and to prepare for the protection of people and critical infrastructure from the risks of terrorist attacks (Council of the European Union, 2007). In 2008, the Council issued a key document in the field of critical infrastructure protection in the EU, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection* (hereinafter: Council Directive 2008/114/EC), which lays out the EU's interest in the comprehensive protection of critical infrastructure against all risks and threats at the Member State level and the EU as a whole, instead of the primary focus on the threat of terrorism (Council of the European Union, 2008).

[2] In 2013, the document was updated and replaced by a new document from the European Commission called *Commission staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructure more secure,* while the purpose and objectives remained the same.

The regulatory framework for the protection of critical infrastructure in cyberspace and critical information infrastructure was initiated by the enactment of *Regulation (EC) No 460/2004 on establishing the European Network and Information Security Agency* (European Parliament and Council of the European Union, 2004). This regulation was replaced by *Regulation (EU) No 526/2013 concerning the European Network and Information Security Agency* (European Parliament and Council of the European Union, 2013), which was called the *European Union Cybersecurity Act*. It was finally replaced by *Regulation (EU) No 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification* (European Parliament and Council of the European Union, 2019). The same bodies issued another important document during 2016: *Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union* (hereinafter: NIS Directive) (European Parliament and Council of the European Union, 2016).

All these documents have become a framework for critical infrastructure protection, defining the direction of action required by the actors, and outlining the mechanisms that need to be developed and put in place to ensure that cooperation on the protection of critical infrastructure and critical information infrastructure is effectively enforceable. However, what is challenging in the field of research of this paper is that 'cyberterrorism' in the EU policy environment may be deemed a misnomer, since it has not yet been explicitly defined at EU level (Pierozzi, 2018: p 1) and that "neither the definition nor the context of the term cyberterrorism have reached so far a broad consensus within the (international) instances dealing with this topic" (CyberROAD, 2016: p 17). So, the conclusion is that if the 'cyberterrorism' in the EU policy environment is not framed through clear policies and guidelines, then it is difficult to talk about protecting critical infrastructure from such a threat.

By reviewing and analyzing strategies and key normative documents, we have come to several important points that need to be highlighted for further discussion: a) the European Union points out that there is a great deal of critical infrastructure in its territory (the territory of the Member States) whose disruption or destruction would have significant, transboundary effects; b) bilateral cooperation between the Member States needs to be upgraded with comprehensive EU-wide solutions; c) the responsibility for protection lies with the Member States and critical infrastructure operators, and the EU can assist them in these efforts; d) the EU has primarily focused its initial discourse on critical infrastructure protection on defence against terrorism, and e) over time, other risks are increasingly accepted and considered.

3.1 A Strategic and Normative Framework for the Protection of Critical Infrastructure in the Republic of Croatia

In the same way as the European Union, the Republic of Croatia set its first strategic discourse on critical infrastructure from the aspect of protection against terrorism. In 2008 the *National Strategy for the Prevention and Suppression of Terrorism* states: "In principle, terrorist threats can vary between individual attacks on highly symbolic values, attacks aimed at causing as many casualties as possible, spreading as much fear and as much destruction as possible, and attacks on critical national infrastructure" (Government of the Republic of Croatia, 2008: Point 8). While the strategic documents mentioned below considered critical infrastructure primarily from the central interest position of the said documents, the *Republic of Croatia Protection And Rescue Plan* of 2010, as the most crucial document for planning the operation of the security and rescue forces and the organization of civil protection systems in response

to major accidents and disasters, addresses critical infrastructure in the context of reviewing the obligations of participants involved in implementing protection and rescue measures (Government of the Republic of Croatia, 2010). The *Republic of Croatia Threat Assessment from Natural and Technical-Technological Disasters and Large Accidents*, from 2013, mentions critical infrastructure in a broader range of protection against natural and anthropogenic sources of threat (Government of the Republic of Croatia, 2013a). The *National Strategy and Action Plan for the Suppression of the Proliferation of Weapons of Mass Destruction*, from the same year, cites the protection of critical infrastructure and populations from a crisis caused by weapons of mass destruction as a specific objective (Government of the Republic of Croatia, 2013b).

All the strategic documents of the period addressed the issues of critical infrastructure protection from their specific standpoints. Such a trend was present until 2013 and the adoption of the *Critical Protection Act*, which constitutes systemic law in this area and which transposes Council Directive 2008/114/EC into Croatian legislation. The law has a comprehensive approach to addressing all risks and threats to critical infrastructure, and delegates responsibility for their protection to critical infrastructure owners or managers (Government of the Republic of Croatia, 2013c).

In 2015, two new security strategies were adopted, the *National Strategy for the Prevention and Suppression of Terrorism* and the *National Cyber Security Strategy*. Both are significant because the area of critical infrastructure is strongly recognized and represented. The *National Strategy for the Prevention and Suppression of Terrorism* recognizes the terrorist threat and potential attacks on national critical infrastructure whose disruption or interruption of the delivery of goods or services could have severe consequences for national security, human health and lives, property and environment, security and economic stability, and continued government functioning. The Strategy sets out a series of measures that need to be implemented to protect critical infrastructure from terrorist attacks (Government of the Republic of Croatia, 2015a). In the *National Cyber Security Strategy,* the area of critical infrastructure is much more prominent than in all the previous national strategies, assessments and plans, primarily through critical communications and information infrastructure, which is defined as communication and information systems whose malfunctioning would significantly disrupt the operation of one or more national critical infrastructures. As in the previous example, the Strategy sets out several necessary measures to ensure that critical infrastructure is as protected as possible (Government of the Republic of Croatia, 2015b).

The next significant period for the development of a strategic and normative framework for critical infrastructure protection is recorded during 2017 and 2018. In 2017, the *National Security Strategy of the Republic of Croatia* and the *Homeland Security System Act* were adopted. The Strategy states, as one of the nine strategic objectives, "achieving the highest level of security and protection of the population and critical infrastructure", in which it outlines the elements required to develop security policies related to critical infrastructure protection (Croatian Parliament, 2017a). The *Homeland Security System Act* was adopted to put the Strategy into practice in the part related to the establishment of a homeland security system and related security risk management, crisis management and critical infrastructure management. The Act makes key provisions to ensure the harmonized implementation of all regulations governing security measures and procedures of national importance, in particular, the protection of critical infrastructure (Croatian Parliament, 2017b). The last in a series of

significant laws adopted was the *Act on the Cyber Security of the Key Service Operators and Digital Services Providers* (Croatian Parliament, 2018). The Act aims to ensure a high level of cybersecurity in providing the services necessary for carrying out key social and economic activities. This Act transposed the NIS Directive into the legislation of the Republic of Croatia.

The Republic of Croatia is very similar in strategic and normative terms to the development of the strategic and normative framework at the EU level (with some time lag). All the analyzed documents outlined the need for the best protection of critical infrastructure, the strengthening of cooperation between stakeholders in the protection of critical infrastructure, and the development of the system and all necessary processes. The state of implementation will be analyzed and presented in the next part of this paper.

According to analytical and empirical findings, the observed countries in South-Eastern Europe (Bosnia and Herzegovina, Serbia, Montenegro, Northern Macedonia and Kosovo) have recently established strategic and normative frameworks for critical infrastructure protection at different stages of implementation. Besides this, none of the observed countries has a system in place for the protection of critical infrastructure and, in numerous activities, the Republic of Croatia is a specific model for them in the area concerned. We can conclude, by the method of generalization, that the current situation in the Republic of Croatia in the field of critical infrastructure protection (and protection from threats of terrorism and cyberterrorism) is something that is yet to come to these countries.

4 Implementation of Critical Infrastructure Protection at the EU Level

In the following quote, the authors summarize the key challenges facing all actors at EU level when talking about cooperation in the field of critical infrastructure protection: "The European Union and its member states face very unique challenges in critical infrastructure protection (CIP) policy. In the past few years, the European Commission has adopted a number of policy initiatives in this field, including Directives and Communications to promote the enhancement of preparedness, security and resilience. However, a number of outstanding problems remain. First, member states are at varying degrees of maturity with respect to the development of a comprehensive and effective CIP policy. Second, there are islands of cooperation across the EU member states but no overall concept of operations at the EU level. Third, partnerships and relationships are scattered across countries (each individual country has and will maintain unique relationships with private sector owner operators and global companies that enable them). Fourth, critical EU infrastructure is also scattered across many different countries" (Heammerli and Renda, 2010: p 3).

Let us consider what forms and mechanisms of cooperation the EU has managed to develop and their functionality. To support the Member States, the European Commission engaged its own Joint Research Centre, which supports cooperation between states, industries and critical infrastructure managers in the scientific field. Subsequently, the Commission has put its focus on the development of different cooperation platforms between the Member States, owners/managers of critical infrastructure, and interested professionals. A concrete measure is to hold meetings of national contact points within the official format of the European Commission, which are usually organized twice a year. At these meetings, the Member States have

the opportunity to exchange best practices and achievements at all stages of the protection of national and European critical infrastructure. The Commission is the organizer and moderator, finances the costs of all national contact points, prepares meeting materials, presents the latest relevant results of the various programmes and projects, supports the initiatives and, most importantly, enables the cooperation between the Member States.

In addition to this formal network, the Commission strongly encourages the Member States to participate with their representatives in an informal network of experts within the framework of the European Reference Network for Critical Infrastructure Protection (ERNCIP). This network aims to provide a framework within which experimental facilities and laboratories can share knowledge and expertise to align test protocols across Europe, leading to better protection of critical infrastructure against all types of threats and dangers and to the creation of a single market for security solutions.

Another significant opportunity that the European Commission offers to all stakeholders in the field of critical infrastructure protection is project funding. Through the programme *'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks'*, 140 million EUR was invested in operational cooperation and activities between 2007 and 2013, and over 120 projects were funded. The projects were extensive in scope and involved all sectors where critical infrastructure could be identified. Their primary purpose was to ensure the advancement of knowledge, a better understanding of the functioning of critical infrastructure at all levels, and the scientific groundwork for current and future research, and to provide public policy recommendations.

The next significant step in establishing cooperation and sharing of knowledge and experience at the European level was to design and launch the Critical Infrastructure Warning Information Network (CIWIN), which was announced in the *Green Paper on a European Programme for Critical Infrastructure Protection* in 2005, gradually created with a modular approach, and became operational in January 2013. The purpose of the network is to exchange information on risk mitigation strategies and measures in the protection of critical infrastructure. It has been developed as a proprietary web platform of the European Commission for all interested experts from the Member States in the field of critical infrastructure (Mikacet al., 2018: pp 95-99).

This has been an overview of some of the Commission's activities to create postulates and interconnect different stakeholders of critical infrastructure protection systems. There is more to these activities, but we believe that we have adequately outlined the activities of the Commission which foster cooperation between the Member States and the EU bodies. Below, we explore the level of collaboration in the area of critical infrastructure protection against (cyber)terrorism.

The protection of critical infrastructure against the threats of terrorism at EU level comes from key EU documents dealing with counter-terrorism issues. The *European Union Counter-Terrorism Strategy* is built around four strands: Prevent, Protect, Pursue, Respond. Protection is a key part of the Strategy. It states that "reducing the vulnerability across Europe of critical infrastructure to physical and electronic attack is essential." In the part that deals with responsibility, it says "while Member States have the primary responsibility for improving the protection of key targets, the interdependency of border security, transport and other cross-border infrastructure require effective EU collective action" (European Council, 2005: pp 10-11). It is important to single out how, in line with the Strategy, the Member States have the primary

responsibility for combating terrorism, and that the EU can help them in several areas, such as strengthening national capabilities; facilitating European cooperation; developing collective capability; and promoting international partnerships. Even more important is to underline that in the EU *Directive on Combating Terrorism* – which is significant because it reinforces the legal framework so that conduct related to terrorism is covered more comprehensively, and directs the Member States in what to do about counter-terrorism cooperation – there is no reference to critical infrastructure protection (European Parliament and Council of the European Union, 2017). Thus, the key document under which the law enforcement agencies of the Member States, as well as the EU's common bodies (such as Europol and Eurojust), act in the field of counter-terrorism does not refer them to the protection of critical infrastructure.

Also, two additional challenges noted by Laris Gaiser should be highlighted. First, "EU members are pursuing fragmented policies; consequently, this has led to a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats." Second, "Critical Infrastructure Protection (CIP) Contact Points requested by EPCIP to facilitate the exchange of information and emergency management coordination financed and established by governments never reached the needed efficiency given that single local reference offices have been appointed following divergent approaches and sometimes incomparable priorities. Even the Computer Security Incident Response Teams Network just provides a forum where Member States' National CSIRTs can cooperate, exchange information, and build trust" (Gaiser, 2018: pp 51-56). To this, we can add our findings that in individual countries, Critical Infrastructure Protection Contact Points are Ministry of Defence officials who do not have sufficient quality cooperation with representatives of the law enforcement agencies primarily responsible for critical infrastructure protection.

It is also necessary to note the opinion of Filippo Pierozzi that the "EU lacked a wide-ranging approach to tackle cyberterrorism. While the EU has stepped up its efforts to face the terrorist use of the internet, cyberterrorism is considered as a threat with a "high potential, but low probability" and therefore not enshrined in crisis management mechanisms" (Pierozzi, 2018: p 7). This explanation may be a logical answer as to why the EU has not yet developed an area of cooperation to protect critical infrastructure from cyberterrorism.

All the aforementioned challenges derive from the organization and the mode of work at both the European Union and Member States' agencies involved in law enforcement activities. Policies and lines of work that are put in place and function properly at EU level (hence the quality of cooperation between the Member States) are related to legal migration and integration; irregular migration and return; the Common European Asylum System; Schengen, borders and visas; organized crime and human trafficking; cybercrime; and counter-terrorism and radicalization. There a number of challenges here, but we will highlight just three of them: 1) no area of work deals with the protection of critical infrastructure, and so these activities are scattered; b) law enforcement agency cooperation is conducted based on the silo principle[3], where activities and actors are primarily focused on their line of work; and c) there is insufficient cooperation and coordination between the different silos, and too little focus on critical infrastructure protection. To conclude this section, we can point to analytical conclusions and empirical insights that the protection of critical infrastructure is not high on the priorities of the various EU bodies or the law enforcement agencies of the Member States cooperating in a number of security areas under the auspices of the EU.

[3] Extracting resources from within the country.

4.1 Implementation of Critical Infrastructure Protection at the Republic of Croatia Level

"Different public agencies (legislative bodies, regulators, etc.) set a plethora of norms, rules and standards on safety and security issues in different CI sectors. Terrorism-related intelligence, which is needed to evaluate current types and levels of threat to CI, is often collected by multiple agencies answerable to different ministries. Effective crisis management and response measures require the ability of several public entities (at the local, municipal, regional and national level) to play their part in a smooth and quick manner. Also, in many cases a number of entities may be involved in a given security function. Such is the case of the aviation sector, where the competent authority, airport management and law enforcement bodies may share responsibility for the protection of airports, air navigation aids and services" (UNOTC, UN CTED and Interpol, 2018: p 107). This hypothesis can be applied globally and locally, and as such, will be used for an examination of the implementation of critical infrastructure protection at the Republic of Croatia level.

It should be emphasized that despite the development of a solid strategic and normative framework related to the issue of critical infrastructure protection, the Republic of Croatia has not yet established a system for critical infrastructure protection. Despite the efforts and initiatives of the competent system-building authority and individual stakeholders from the competent ministries that have recognized the importance of this activity, the necessary functionality of the system has not been developed to a level where it can be considered an operating system (Mikac, Cesarec, Larkin, 2018: p 111), which is not to say that critical infrastructure is not protected by many other systems and lines of work. However, if a critical infrastructure protection system were in place, it would undoubtedly be more efficient, faster and more integrated than it is now. Let us start by looking at the current state of things.

The *National Strategy for the Prevention and Suppression of Terrorism* (both the 2008 version and the current 2015 one) recognizes the dangers and potential consequences that would occur if terrorists attacked critical infrastructure. It should be pointed out that Croatia has a very robust, operational and effective system of prevention and suppression of terrorism. The challenge in terms of protection of critical infrastructure is found in the exchange of data and information between state bodies and critical infrastructure operators. Cooperation between the Security and Intelligence Agency and the police is beyond question, as well as their cooperation with and provision of the necessary information to state bodies. However, there is a lack of flow of information from the level of state bodies (representing sectoral coordinators) to critical infrastructure operators in specific sectors. In some sectors, cooperation does exist, but in some, it does not. This shows that the system is not established in all its potential, and brings us to the situation that Dario Malnar and Nikola Mlinac describe in following words: "Despite the construction of national protection systems and efforts to centralize activities, critical infrastructure protection is still a largely fragmented activity, sectorally defined through the competences of various ministries and other state bodies. Such dispersion of security and the particularization of facilities makes it difficult to concentrate intelligence efforts and adversely affects the effectiveness of action" (Malnar and Mlinac, 2014: p 1013).

The domain related to the protection of critical infrastructure from natural and technical-technological disasters and large accidents is better regulated, because it belongs to a civil protection system that is functional and, unlike the previous example, has no obstacles in operation and activity. This can be partly explained by the challenge of dealing with sensitive,

proprietary and intelligence data that is not arranged in such a way as to enable the rapid and efficient flow of critical information to critical infrastructure operators.

Relating to the protection of critical infrastructure in cyberspace, the *National Cyber Security Strategy* reveals many things by which we can see that we still do not have a system in place to protect critical infrastructure, although we do strive towards it. However, the first significant step in the formation of a future system can be made; namely, by enacting the *Act on the Cyber Security of the Key Service Operators and Digital Services Providers,* identifying Key Service Operators and Digital Services Providers, and establishing new bodies (a National Cyber Security Council and an Operational Technical Coordination for Cyber Security) and connecting them to the bodies responsible for national cyberspace protection activities, and thus to critical infrastructure. In this domain, in the years ahead, it will be necessary to elaborate procedures and the effective cooperation of all actors.

It should be noted that in 2017, the *National Security Strategy of the Republic of Croatia* stated that "documents defining the policies and methodologies for managing critical infrastructure and limited national assets will be produced and will clearly determine which parts must remain majority state-owned, thereby making it impossible to compromise vital functions of importance to the state and the population in cases of business instability" (Croatian Parliament, 2017a). This has not been done, and according to the current state of affairs, we have not found any information that this is being done. Besides, this and the Strategy mentioned above highlight the importance and need for public-private partnerships in the field of critical infrastructure protection. It does exist, but not as an organized and coordinated activity by the state; it just comes down to individual case studies.

In connection with the construction of a critical infrastructure protection system, high-quality direction is given by the 2017 *Homeland Security System Act*, which was adopted to put the *National Security Strategy* into practice in the part related to the establishment of a homeland security system and related security risk management, crisis management and critical infrastructure management. The Act makes key provisions to ensure the harmonized implementation of all regulations governing the security measures and procedures of national importance, in particular, the protection of critical infrastructure (Croatian Parliament, 2017b). Nevertheless, this has not materialized in the three years since the law was passed, just as most of the provisions of the 2013 *Critical Protection Act* have not been implemented.

Finally, we have another interesting remark to make. Although all the actors in charge of coordinating critical infrastructure protection activities are located in the same Ministry (Ministry of the Interior), albeit in different organizational units, they do not have the kind of cooperation that would be expected by looking through the prism of critical infrastructure. This is very similar to the cooperation challenges we have seen at the EU level.

The Republic of Croatia has a high-quality strategic and normative framework for critical infrastructure protection, but it lacks a certain set of regulations that it has committed itself to draft. Most of all, it lacks a system with clear competencies, procedures and mutual responsibilities of all actors in these processes. We can also cite these remarks for the observed countries in South-Eastern Europe.

5 Conclusion

Critical infrastructures, in their regular functioning, depend significantly on the support of information systems. At a time of intensive development of information and communication technologies, it is almost unthinkable to fulfil the key functions of critical infrastructure without the significant role of information technologies, especially in the field of their protection. The day-to-day development of new technological advances in the field of information and communication technologies, in addition to significantly contributing to the functionality and protection of critical infrastructure, also opens up numerous opportunities for the misuse of technologies, which can consequently impair the stability of systems and in some cases bring about their destruction. By analyzing the terrorist threat and possible consequences of a cyberterrorism attack on critical infrastructure, it can be concluded that the consequences of such an attack could have far more severe and lasting effects on critical infrastructure than other forms of terrorist threat.

It is for this reason that the two security phenomena (i.e. terrorist threats and a cyberterrorism attack on critical infrastructure) need to be more closely linked, both at the policy level and at the operational level of cooperation of the competent authorities in the implementation of critical infrastructure protection and the fight against terrorism.

In order to show the current level of protection, from the very development of the policy document right up to its implementation on the ground, we have taken the example of the European Union and the Republic of Croatia. Through our research, we have been able to demonstrate that there is a disproportion between the development of security policies for the protection of critical infrastructure and their implementation in practice. Our recommendations urge an even more reliable and robust strategic and normative framework for critical infrastructure protection, in which cyber threats, including cyberterrorism, are more emphasized. Next, we believe that more space should be devoted to developing guidance from strategic and normative documents through implementation guidance to actors in the critical infrastructure protection process with clear responsibilities and competencies and a coordinating role in these processes. Our third recommendation goes towards the need for more comprehensive and better coordination and cooperation between the operational elements of the implementation of critical infrastructure protection – from the EU level to all countries of interest in this research – because if most stakeholders in these processes are aware of the need for critical infrastructure protection, the above should be proactively implemented and thus the system and its procedures will be developed through a bottom-up approach.

6 References

1. Cadwalladr, C., Graham-Harrison E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian, 17 March.* Retrieved March 14, 2020, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
2. Council of the European Union (2008). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection*. Retrieved March 5, 2020, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
3. Council of the European Union (2007). *COUNCIL DECISION of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks'*. Retrieved March 5, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0124&from=EN
4. Council of the European Union (2003). *European Security Strategy: A Secure Europe in a Better World.* Retrieved March 8, 2020, from https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf
5. Council on Foreign Relations (2020). *APT 28.* Retrieved March 12, 2020, from https://www.cfr.org/interactive/cyber-operations/apt-28
6. Croatian Parliament (2018). *Act on the Cyber Security of the Key Service Operators and Digital Services Providers.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_64_1305.html
7. Croatian Parliament (2017a). *National Security Strategy of the Republic of Croatia.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/full/2017_07_73_1772.html
8. Croatian Parliament (2017b). *Homeland Security System Act.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2489.html
9. CyberROAD (2016). *Cyber Terrorism Stakeholder Needs and Threats Evaluation.* Retrieved March 8, 2020, from http://www.cyberroad-project.eu/m/filer_public/2016/05/02/d61_cyber_terrorism_stakeholder_needs_and_threats_evaluation.pdf
10. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved March 8, 2020, from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
11. European Commission (2013). *Commission staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructure more secure*. Retrieved March 8, 2020, from https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf
12. European Commission (2006). *European Programme for Critical Infrastructure Protection.* Retrieved March 8, 2020, from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786
13. European Commission (2005). *Green Paper on a European Programme for Critical Infrastructure Protection.* Retrieved March 8, 2020, from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52005DC0576

14. European Commission (2004). *Communication from the Commission to the Council and the European Parliament: Communication on Critical Infrastructure Protection in the fight against terrorism.* Retrieved March 2, 2020, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702

15. European Council (2010). *Internal security strategy for the European Union: Towards a European security model.* Retrieved March 8, 2020, from https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf

16. European Council (2005). *The European Union Counter-Terrorism Strategy.* Retrieved March 8, 2020, from http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204

17. European External Action Service (2016). *A Global Strategy for the European Union's Foreign and Security Policy.* Retrieved March 2, 2020, from https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

18. European Parliament and Council of the European Union (2019). *Regulation (EU) No 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* Retrieved March 2, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

19. European Parliament and Council of the European Union (2017). *Directive on combating terrorism.* Retrieved March 2, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN

20. European Parliament and Council of the European Union (2016). *Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.* Retrieved March 2, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

21. European Parliament and Council of the European Union (2013). *Regulation (EU) No 526/2013 concerning the European Network and Information Security Agency and repealing Regulation (EC) No 460/2004.* Retrieved March 2, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0526&from=EN

22. European Parliament and Council of the European Union (2004). *Regulation (EC) No 460/2004 on establishing the European Network and Information Security Agency.* Retrieved March 2, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0460&from=EN

23. European Union Agency for Network and Information Security (2019). *ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends.* Retrieved March 8, 2020, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

24. Europol (2019). *European Union Terrorism Situation and Trend Report 2019.* Retrieved March 5, 2020, from https://www.europol.europa.eu/sites/default/files/documents/tesat_2019_final.pdf

25. 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. https://hrcak.srce.hr/file/303484

26. Government of the Republic of Croatia (2015a). *National Strategy for the Prevention and Suppression of Terrorism.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/full/2015_10_108_2105.html

27. Government of the Republic of Croatia (2015b). *National Cyber Security Strategy.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html

28. Government of the Republic of Croatia (2013a). *Republic of Croatia threat assessment from natural and technical-technological disasters and huge accidents.* Retrieved March 5, 2020, from http://upvh.hr/wp-content/uploads/2017/02/PROCJENA-web-20.03.2013..pdf

29. Government of the Republic of Croatia (2013b). *National Strategy and Action Plan for the Suppression of the Proliferation of Weapons of Mass Destruction.* Retrieved March 5, 2020, from https://vlada.gov.hr/UserDocsImages//Sjednice/Arhiva//71.%20-%206.pdf

30. Government of the Republic of Croatia (2013c). *Critical Protection Act.* Retrieved March 5, 2020, from https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html

31. Government of the Republic of Croatia (2010). *Republic of Croatia Protection and Rescue Plan.* Retrieved March 2, 2020, from, https://narodne-novine.nn.hr/clanci/sluzbeni/2010_08_96_2707.html

32. Government of the Republic of Croatia (2008). *National Strategy for the Prevention and Suppression of Terrorism.* Retrieved March 2, 2020, from, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_139_3896.html

33. Heammerli, B., Renda, A. (2010). *Protecting Critical Infrastructure in the EU.* Brussels: Centre for European Policy Studies. https://www.ceps.eu/wp-content/uploads/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf

34. Hern, A. (2019). Cambridge Analytica did work for Leave.EU, emails confirm. *The Guardian, 30 July.* Retrieved March 14, 2020, from https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm

35. INA.hr (2020). Announcement Cyber-attack. *21 February.* Retrieved March 12, 2020, from https://www.ina.hr/en/announcement-cyber-attack/

36. Ivezić, B. (2020). Broj cyber napada lani u Hrvatskoj skočio 65 posto. *Poslovni.hr, 22 January 2020.* Retrieved March 12, 2020, from https://www.poslovni.hr/sci-tech/broj-cyber-napada-lani-u-hrvatskoj-skocio-65-posto-361907

37. Kirkpatrick, D., Rosenberg, M. (2018). Russians Offered Business Deals to Brexit's Biggest Backer. *The New York Times, 29 June.* Retrieved March 14, 2020, from https://www.nytimes.com/2018/06/29/world/europe/russia-britain-brexit-arron-banks.html

38. Malnar, D., Mlinac, N. (2014). Sigurnosno-obavještajna komponenta zaštite kritične nacionalne energetske infrastrukture Republike Hrvatske. In: S. Tatalović (Ed.), *Dani kriznog upravljanja, Zbornik radova V. međunarodne konferencije.* (pp 1007-1020). Velika Gorica: Veleučilište Velika Gorica. http://dku.hr/wp-content/uploads/2016/09/DKU-zbornik-radova-2014.pdf

39. McGuinness, D. (2017). How a cyber attack transformed Estonia. *BBC.com, 27 April.* Retrieved March 14, 2020, from https://www.bbc.com/news/39655415

40. Merriam-Webster dictionary (2020). *Cyberterrorism,* Retrieved March 2, 2020, from https://www.merriam-webster.com/dictionary/cyberterrorism#h1

41. Mikac, R., Cesarec, I., Larkin, R. (2018). *Critical Infrastructure: The platforms for a successful development of nations security.* Zagreb: Jesenski and Turk

42. Nakashima, E., Warrick J. (2012). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post, 2 June.* Retrieved March 5, 2020, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

43. Pierozzi, F. (2018). EU and Cyberterrorism. Added Value or Chimera?. *The Centre for Cyber Security and International Relations*, pp 1-11. https://www.cssii.unifi.it/upload/sub/eu%20and%20cyberterrorism.pdf

44. Polityuk, P., Vukmanovic O., Jewkes S. (2017). Ukraine's power outage was a cyber attack: Ukrenergo. *Reuters, 18 January.* Retrieved March 5, 2020, from https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

45. Security and Intelligence Agency of the Republic of Croatia (2018). *Public report 2018.* Retrieved March 12, 2020, from https://www.soa.hr/files/file/Public-Report-2018.pdf

46. UN Office of Counter-Terrorism, UN Security Council Counter-Terrorism Committee Executive Directorate and INTERPOL (2018). *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*. Retrieved March 5, 2020, from https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf

47. United Nations General Assembly (1994). *Measures to Eliminate International Terrorism*. Retrieved March 5, 2020, from https://undocs.org/en/A/RES/49/60

48. Wright, R. (2018). Arron Banks and the mystery Brexit campaign funds. *Financial Times, 5 November.* Retrieved March 14, 2020, from https://www.ft.com/content/4610a4be-dde2-11e8-9f04-38d397e6661c

3 A Critical Infrastructure Protection Perspective on Counter-Terrorism in South-Eastern Europe

Alexandru Georgescu, Adrian Victor Vevera, Carmen Elena Cîrnu

1 Introduction

Terrorism is a severe threat to South Eastern Europe (SEE). The region features all of the significant root causes of terrorism (Albrecht & Getoš, 2010), including a persistent lack of trust, a history of conflict, unresolved group tensions, weak institutions and relatively weak economies. Matei (2009) wrote that "post-Cold War security challenges and threats no longer come from organized, hierarchical state actors, but rather from non-state, easily adaptable, network-centric groups and organizations (such as terrorist, organized crime (OC), money laundering and human trafficking groups), which have progressively succeeded in altering the traditional geographic borders between countries, as well as between domestic and foreign threats".

The presence of organized crime, especially in its transborder version, acts as a facilitator for terrorism both directly and indirectly, through its corrosive influence on institutions, trust, the rule of law and the allocation of scarce resources (Busuncian, 2007). Historically severe economic recessions, involving hyperinflation and widespread poverty have been the companions of social upheaval and armed conflict. At the same time, the region has borne witness to uncontrolled migratory flows and resurgent influences instrumentalizing radicalization and persistent group animosity.

Counter-terrorism efforts are also required to decrease the likelihood of the materialization of such an event, and to increase the resilience of societies to terrorist intent, threat perception and action. This article argues in favour of the development and application of a systemic framework of Critical Infrastructure Protection (CIP) by the governments in the region, in concert with other powers like the US and blocs such as the EU and NATO. Critical Infrastructure (CI) includes "those physical and cyber-based systems essential to the minimum operations of the economy and government" (PDD-63, 1998) and comprises infrastructures, key assets and key resources (DHS, 2003). CI is a natural target for terrorists and other co-

ercive actors and the evolution of the security environment suggests growing threats to the region and beyond stemming from digitization, chaotic development, interdependencies and geopolitical dynamics.

Certain countries within South-Eastern Europe are already applying this framework, but the non-EU states remain a gap in the security governance of a region whose interconnections are growing as a result of catch-up growth patterns, the regionalization and Europeanization of trade and the geopolitical initiatives required to build new infrastructure in this strategic region. We argue that CIP efforts will provide added value to security outcomes by increasing societal resilience, allocating scarce resources to the most vulnerable areas and introducing security by design as a principle in the building, operation and regulation of critical infrastructure. We conclude with a series of proposals related to CIP in South Eastern Europe, especially the non-EU states.

2 Critical Infrastructure Protection

Critical Infrastructure Protection has emerged as a comprehensive framework that offers the toolbox, principles and perspectives required to describe and manage a complex system of systems, first through an all-hazards approach and then through one based on resilience. This final concept is the ability of a system or asset to resist the impact of a disruptive event with minimum damage, minimal disruption and rapid resumption of an acceptable level of functioning so as to minimize the impact on related systems (Gheorghe et al, 2018). It began with the Presidential Commission on Critical Infrastructure Protection in 1998, and it was applied in the US and spread throughout the world, especially in the EU, as a governance mechanism after the September 11 attacks. The attacks proved the interdependencies of critical infrastructure and the possibility of cascading disruptions and unexpected escalations in interconnected systems. At its most basic, CIP offers a philosophy for describing the operation of complex systems and developing methodologies to assess criticality, so that scarce security resources, including the attention of decision-makers within the competent authorities, can be directed to the areas of maximum usefulness. It is impossible to protect all critical infrastructures, all the time and completely. While overall societal resilience must grow, decisions must be made with regard to the most important infrastructures, assets and resources to protect, as these will also be the most likely targets for adversaries.

2.1 Critical Infrastructure

At the basis of the functioning of any society is an interconnected system of systems comprised of infrastructures, which are socio-technical systems made up of physical assets, organizations, communication links and governance mechanisms which produce the goods and services necessary for the functioning of society. Infrastructure taxonomies vary significantly from country to country, even in the EU, but generally designate energy infrastructure; railways, roads and ports; the chemical and nuclear industries; information and communication technology; food and water supplies; health, education and finance; defence capabilities; and even public administration.

Infrastructures are critical when their destruction or disruption would cause loss of life, casualties, significant material damage, and loss to national prestige and confidence in authorities on the part of citizens and investors. The ANZCTC (2015) stated “CI extends across many

sectors of the economy, including banking and finance, transport, energy, water, health, food and grocery and communications. It also includes key government services, manufacturing and supply chains. The ubiquitous nature of CI and our collective reliance on it means that protecting and ensuring its continuity is essential to the nation's economic prosperity, national security and social wellbeing". CI must therefore be protected from a wide variety of risks, vulnerabilities and threats; the latter may be either deliberate or accidental, natural or artificial, localized or distant, contained or systemic, and so on. The figure below describes the main dimensions through which critical infrastructures and their relationships to each other and their security environments are defined.

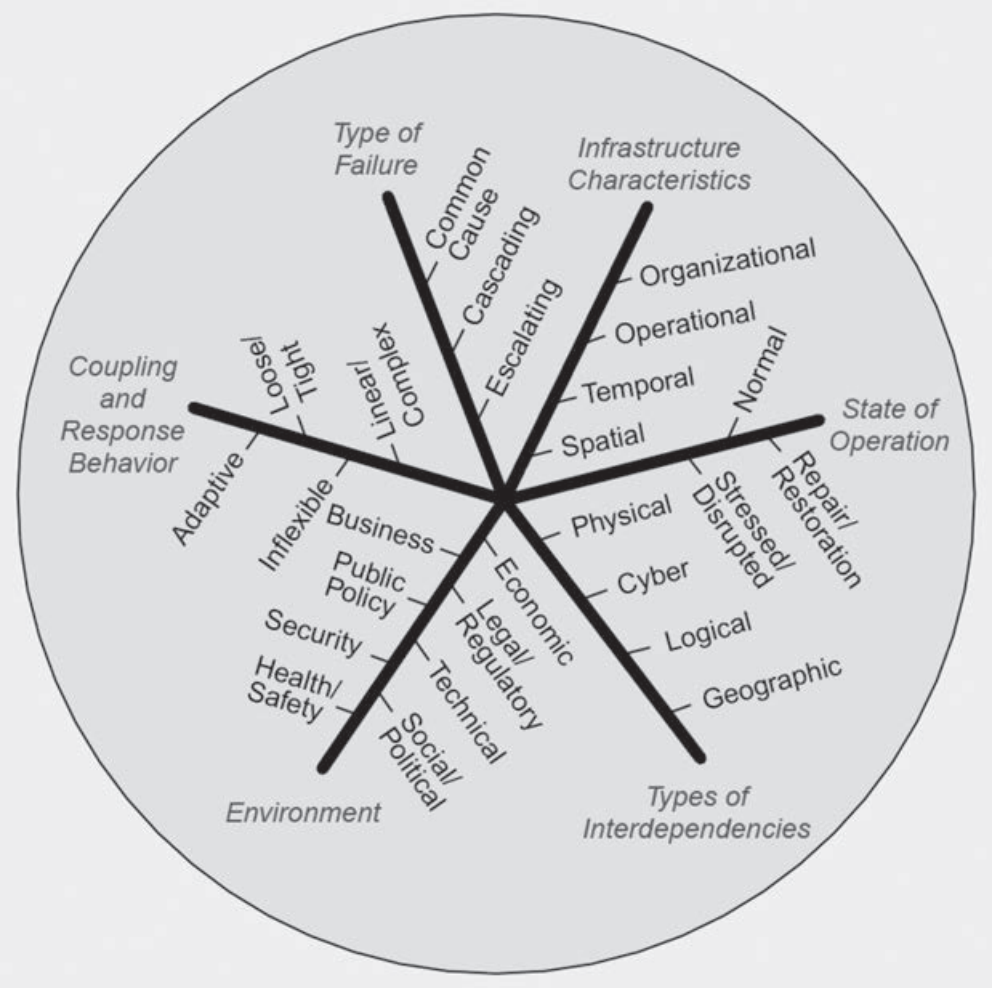


Figure 1: The main concepts of the CIP framework (Source: Rinaldi et al., 2001)

This article does not propose to offer a comprehensive view of the issues, but we will highlight the features of CIP which contribute to its usefulness. We will explore the interdependencies between infrastructure components and the infrastructures themselves. These interdependencies may be physical, geographical, informational, cybernetic, sectorial, political/policy and social (Gheorghe & Schläpfer, 2006), though other taxonomies exist. These interdependen-

cies provide the vectors for the transmission of risks, vulnerabilities and threats, not just those stemming from the security environment, but also those created through interactions between the infrastructures or infrastructure components, leading to complexity and unanticipated system behaviours (Keating et al, 2014).

The Covid-19 pandemic of 2020, especially, has highlighted the interdependencies of several categories of critical infrastructure, with the inadequacy of the critical health infrastructures and the attendant emergency measures having an impact on most facets of social life and the economy, which can be conceptualized as transport infrastructure, food supply infrastructure, financial infrastructure and so on, as well as the cross-border impact of infrastructure disruption, either partial or total. It has also highlighted the potential of physical, cyber, or supply chain attacks on health infrastructure to disrupt the normal functioning of society and to aggravate ongoing crises.

The ambiguity and uncertainty of complex systems constitutes a challenge for owners/operators and for state authorities. The materialization of an event which leads to a crisis can lead to disruptions propagating throughout an entire system, in ways both expected and unexpected, due to the "fortuitous alignment of breakages" and other factors enabling rapid transmission (Pescaroli & Alexander, 2016). These factors include a lack of system adaptability, insufficient margins, lack of substitution in resources, lack of flexibility, lack of reserves, and often stem not from system failure, but from the results of desired efficiencies and costs savings. The resulting phenomenon leads to the prolongation and aggravation of crises, as well as to unexpected escalations and other interactions, both within national borders, and also beyond them (Pescaroli & Alexander, 2016).

Critical infrastructure is naturally vulnerable to deliberate disruption. Terrorists may themselves use an intuitive or even a professional version of criticality theory to plan their actions so they can generate the maximum impact (short, medium and long-term) with the least costs or fewest risks of failure. The targeting of critical infrastructure is also becoming a preferred activity of state-sponsored actors, as a means of hybrid warfare disrupting both civilian and military infrastructure, and placing pressures on the target society's economy, civil society and politics. It therefore becomes a supremely useful means of coercion against a rival or an adversary, who must act to reduce the vulnerability to these methods. This may serve as a preamble to a classic conventional military conflict, or as a strategy to avoid conventional warfare and an armed response through plausible deniability and measures below the threshold of war.

The SEE region features several characteristics, from a CI point of view, which impact the security environment:

- A heterogeneity of state entities when it comes to resources, government capacity and membership in CIP-relevant international organizations (the EU, NATO etc.);
- In the case of former Communist nations, a lack of basic infrastructure for modern economic processes, and the advanced decay of the existing, often extensive, infrastructure, which is often nearing the end of its planned lifespan;
- A weaker institutional capacity, with low levels of trust and social capital, affecting the positive cooperation between state authorities and local communities or between business organizations (the majority or plurality of CI operators) and the authorities;
- A drive for catch-up growth which prioritizes speed over security, and leads to differences in the rates of advancement between profit and efficiency-oriented actors and security-oriented authorities. The CI inventory develops more rapidly than the state capacity to

keep up with shifts in the security environment, while weak regulations and liability laws incentivize underinvestment in infrastructure security by owners/operators;
- The regional economic transition has also, historically, meant that governments have little experience in crafting regulations that keep in mind the differences in incentives and organizational cultures between authorities and CI owners/operators, many of them private, as well as the Public-Private Partnerships which CIP activities call for;
- A challenging security environment which, as explained previously, is also conducive to terrorist operations;
- The general complexity of the area, especially with the co-existence on the ground of projects by the EU, NATO, the Russian Federation, China etc;
- The perspective of significant infrastructure inventory change in the next period, through projects fostered by the Belt and Road Initiative (or the 17+1 Initiative of cooperation between China and its Central and Eastern European Partners) or by the Three Seas Initiative. Both of these initiatives are focused on cross-border connectivity for economic growth;
- Deriving from this, we have the issue that almost all European countries face, which is the simultaneous existence of several generations of critical infrastructures, in terms of age, systems of control, status of investment in maintenance, usable remaining lifespan, creating new challenges to governance and new vulnerabilities and fragilities exploitable through terrorist action.

2.2 Critical Infrastructure Protection Governance

The concept of governance refers to the rules, organizations, structures, hierarchies and principles which guide and govern decision-making. Figure 2 shows a basic CIP framework at national level, modelled after that of Romania.

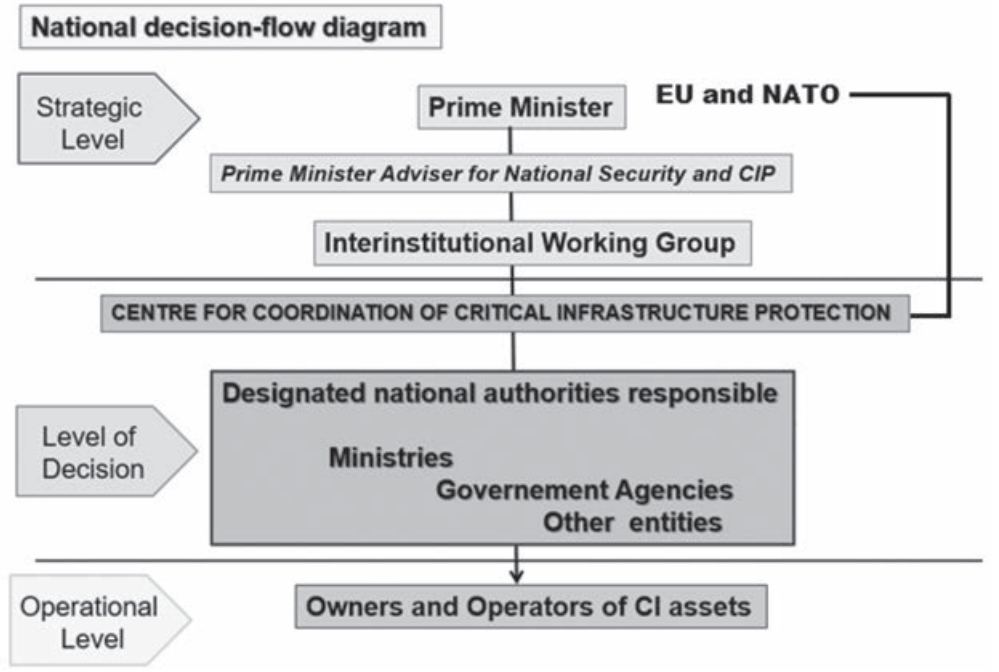


Figure 2: A simplified view of a CIP framework (Source: Mureșan & Georgescu, 2015)

Frameworks generally offer taxonomies of critical infrastructures, procedures for identifying and designating them, and the codification of the responsibilities of the CI owner/operator , such as the drafting of Operator Security Plans to be reviewed regularly or whenever the situation warrants it, and the designation of competent authorities for each CI sector and of an overall coordinating authority.

Most owners and operators of Critical Infrastructure in the West are private companies (from around 75% in the EU to 85% in the US) and this leads to significant challenges, including of coordination. An added dimension of the challenge stems from the foreign ownership and operation of certain critical infrastructures. The highest management levels of these particular organizations are located in other countries, with the attendant complexity with regard to disinvestment, lack of investment in security processes, lack of bargaining power on the part of smaller states, limited tools for inducing changes in behaviour, and so on. In addition to operational and governance issues of CIP, there may also be geopolitical considerations.

As stated above and by Helbing (2013), a great deal of critical infrastructure is networked regionally and even globally, and therefore surpasses the ability of the authorities of a single jurisdiction to govern. Even if all jurisdictions feature CIP processes, the lack of coordination or compatibility may lead to new risks, vulnerabilities and threats appearing in the gaps, especially as adversaries seek to take advantage of the situation and exploit differences in governance and in relative preparedness. This is why there are more and more global initiatives directed towards governing systemic issues, such as cyber dependencies, global trade infrastructure and technological standardization for inter-operability.

The EU, however, has built a European Programme for Critical Infrastructure Protection (EPCIP), starting with a series of documents of reference such as Directive 114/2008. While defining best practice for national systems, the European system concerns itself with Critical European Infrastructures, managed in concert with the national authorities and defined as an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008*). This recognizes the effects of the intended integration of the EU's Member States into an "ever closer Union", especially projects such as the "Energy Union", the "Single Digital Market" and the strategic transport corridors. As we will see in the final section of this paper, this presents opportunities for the CI governance of SEE nations not in the EU.

3 The Cyber Perspective on CIP and Terrorism

It is important to note that cyber environment does not only designate the ITC critical infrastructure category, but is also a cross-cutting issue, since cyber has become a medium for command, control, coordination and information gathering processes at the level of complex systems of systems (Georgescu & Cîrnu, 2019). Building on the CIP section of this article, we may say that the efficiencies in the operation of critical infrastructure which enable higher productivity and functionality have been purchased at the cost of the permeation of cyber

throughout the entire system of systems, leading to tighter couplings between systems components and the "fortuitous alignment of breakages" which may result in cascading disruptions (Pescaroli & Alexander, 2016).

The permeation of cyber is equivalent to an increase in the surface of contact between the system(s) in question and a cyber environment that is increasingly dangerous (Gokce, 2018). This leads to an increase in the opportunities and vectors for deliberate attackers to attempt to disrupt normal system operation, for whatever purpose, placing the defenders at a disadvantage.

On the side of the defenders, we find that, just as many CI owners/operators are in the private sector, there is a staggering variety of cyber preparedness levels, in terms of organization, sophistication and levels of investment. This is also matched by variations in preparedness levels for the competent authorities and decision-makers, not just in the region but throughout the EU, where the NIS Directive has only recently been universally implemented.

For attackers, we find a variety of actors, including terrorist groups, lone wolves, state-supported actors, "enemies-within", organized crime groups and other variations on the profit motive. Coburn et al. (2019) also states that state-sponsored actors have registered growth in financial motivation as a source for attacks. It is becoming more and more difficult to distinguish between cyber-terrorism, cyber-activism and organized cybercrime. Figure 3 highlights the links between cybercrime and terrorism as an enabler, by creating the tools, the resources and the opportunity for terrorists to act. Terrorists may fund their activities through cybercrime, they may steal information for planning attacks and access to a site or facility, they may acquire tools for cyberattacks or outsource services, and they may tread on the path of corruption and other frailties and vulnerabilities which organized crime leaves in institutions, companies or society in general (Stytz & Banks, 2017).

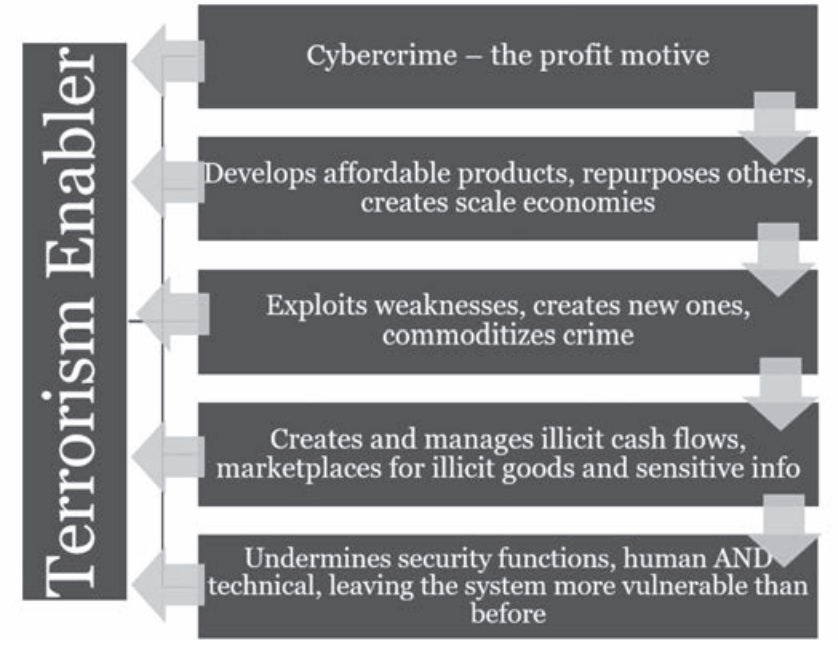


Figure 3: The link between terrorism and transborder organized crime, especially cybercrime (Source: presentation by Liviu Mureșan)

The current trends in the realm of cybersecurity, as evidenced by numerous studies in the field, for example Coburn et al. (2019) and O'Gorman et al. (2019), show that there is an increase in cybercrime that specifically targets critical infrastructure. Firstly, we have the exceptional growth in supply chain attacks through specific means – 78% from 2017 to 2018 (O'Gorman et al., 2019). Secondly, we have the various sector-based analyses which show that energy, transport, public administration, finance and others are key targets for cyberattacks, either motivated by profit, by ideology or by politics (Coburn et al., 2019).

At the same time, we are witnessing the potentially uncontrolled proliferation of cyber weapons and the possibility of their modification to suit particular needs (Georgescu et al, 2019). Even without the loss of state-sponsored cyber weapons, we are also witnessing a disconnect between attacker and skill set. Previously, the attacker would need a specific skill set and knowledge to succeed. Today, the commodification of malware and the mirroring of legitimate business processes, such as the ability to purchase hacking services, DDoS attacks and so on, has resulted in a wider range of potential attackers, "democratizing" cyber disruption, whether coming from rivals, professional criminals, activists or even terrorists (Georgescu, 2018).

Every piece of critical infrastructure in an advanced nation is controlled partly or completely through networked systems that enable specific functionalities and efficiencies involving data management, feedback loops, information gathering and processing and coordination. Every developing nation desires an infrastructure profile that ultimately increases the permeation of their critical infrastructures by cyber. This means that exposure to cyber risks is growing simultaneously with the growth in the number of attackers, their means and their potential rewards from attacks.

These trends are exacerbated by paradigm shifts such as the Internet-of-Things with billions of devices and sensors, ubiquitous computing, artificial intelligence and, least remarked of all, the growth in the use of commercial-off-the-shelf solutions for complex and vulnerable systems, such as industrial control systems and SCADA (Georgescu & Cîrnu, 2019). More and more, even military technology and satellites (Falco, 2018) are based on commercial-off-the-shelf technologies and software. Whereas previously a SCADA system would feature proprietary equipment and software, dedicated communication lines and other advantages that offered it "security by opacity" from attackers, today these systems and others rely on internet connectivity, commercial sensors and equipment, and commercial software (Nazir et al., 2017). This evolution was motivated by mounting costs and the desire to enable new functionalities and efficiencies, but has resulted in this particular vulnerability. These evolutions effectively applied the logic of fast replacing consumer goods and electronics to durable goods and, increasingly, to complex systems whose lifespan is measured in decades. The profusion of unpatched and unpatchable devices results in long-term vulnerabilities which are inherent in the system until it is upgraded, a complex process which often results in the layering of different generations of control systems in a way which may result in emergent behaviours and new, non-deliberate threats, while also possibly giving rise to system exploits which may be used by adversaries.

In conclusion, the cyber dimension of critical infrastructure has generated a persistent and evolving security problem which facilitates terrorism and other forms of deliberate disruption, and which must be addressed through systemic resilience.

4 Towards a CIP Roadmap for Increasing Resilience to Terrorist Threats

In the previous sections, we explained the usefulness of the system of systems perspective on the functioning of society to counter-terrorism efforts. Inter-dependent systems across geographical and sectorial boundaries create a topology of risk which may inform both attackers and defenders, as well as decision-makers seeking to enhance long-term resilience, which is the capacity to withstand attacks with minimum damage and rapidly regain an acceptable level of functioning while maintaining business continuity and quality of life. We have also underscored the fact that our proposed approach is already partially in place in South-Eastern Europe, through the EU and NATO Member States, though it can always be improved. Meanwhile, the South-Eastern European region and the Western Balkans feature many of the underlying conditions which, in the literature, are associated with an increase in the risk of terrorism. It is necessary to utilize all possible approaches to address this risk, reduce vulnerabilities and mitigate damage.

In this final section, we will list several possible elements of a roadmap or an action plan to improve security against terrorist threats through CIP. The heterogeneity of the region with regard to the implementation of a CIP framework is both an advantage and a disadvantage – an advantage, since it gives a regional base for cooperation in the convergence of the quality of CIP governance, while also a disadvantage, since persistent differences make acting in lockstep against transborder threats much more difficult. Thankfully, existing cooperation initiatives such as the Southeast European Law Enforcement Center (SELEC) have mediated the practice of cooperation on complex and sensitive issues, while also touching on CIP-related aspects such as financial crime and cybercrime.

4.1 Creating or Improving a Legal and Administrative Framework for CIP

The most important process that should be initiated is for the non-EU countries in the region to develop a legal and administrative framework for Critical Infrastructure Protection which is compatible and compliant with EU norms and regulations. They should do this regardless of the status of their candidacy and the challenges that may delay or thwart membership.

Every country has laws and institutions governing the security of certain critical assets or processes from specific threats such as fire, theft and sabotage. The CIP framework builds on these and ensures a holistic perspective on their protection across multiple sectors and the entire threat spectrum, thereby filling in the gaps in the protection mechanisms which a piecemeal approach would develop.

Each country in this situation will be at a different stage in the development of such a framework and its constitutive elements, and will require a personalized approach while also being included in a wider framework of cooperation which sustains the tempo of reform with regard to political will, the allocation of resources, the management of reluctant interest groups, and so on. It is to be expected that the smaller the country is, the more important civil-military cooperation becomes in CIP security processes, to overcome the barriers of the lack of resources and scale in the governance apparatus.

The systems of other countries cannot be lifted wholesale and transplanted elsewhere. They must be adapted to localized conditions, especially with regard to challenges in the security environment, the ownership and operation of prospective critical infrastructure, the internal administrative organization of each particular country, and the existing security institutions and mechanisms. The topology of the foreign ownership of critical infrastructures, key assets and key resources is also important. Each country will also require a particular roadmap for the implementation of CIP, taking into account existing laws, institutions and resources.

The basic scheme for erecting such a system is constructed in Figure 4.

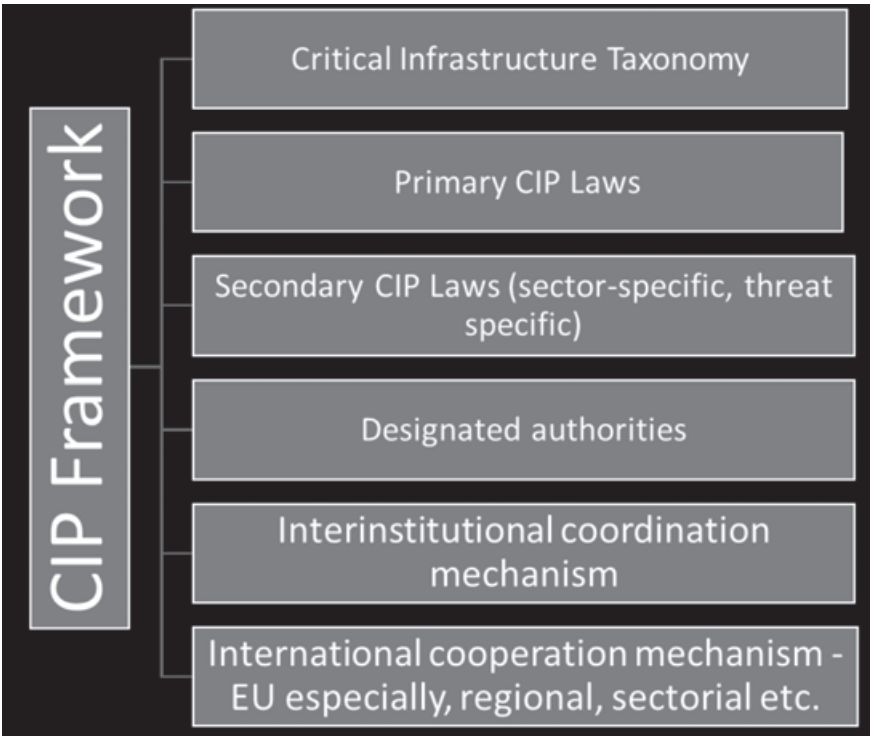


Figure 4: The main elements of a CIP Framework (Source: authors)

The EU Member States show a wide variation in CIP frameworks, especially with regard to interinstitutional cooperation mechanisms, but also with regard to taxonomies. Romania, for instance, introduced financial and cultural heritage into the CI sector list in 2018. It would behoove the various states in the region to attempt a comprehensive initial development rather than a piecemeal approach, since simply focusing on energy or on transport will foster new vulnerabilities.

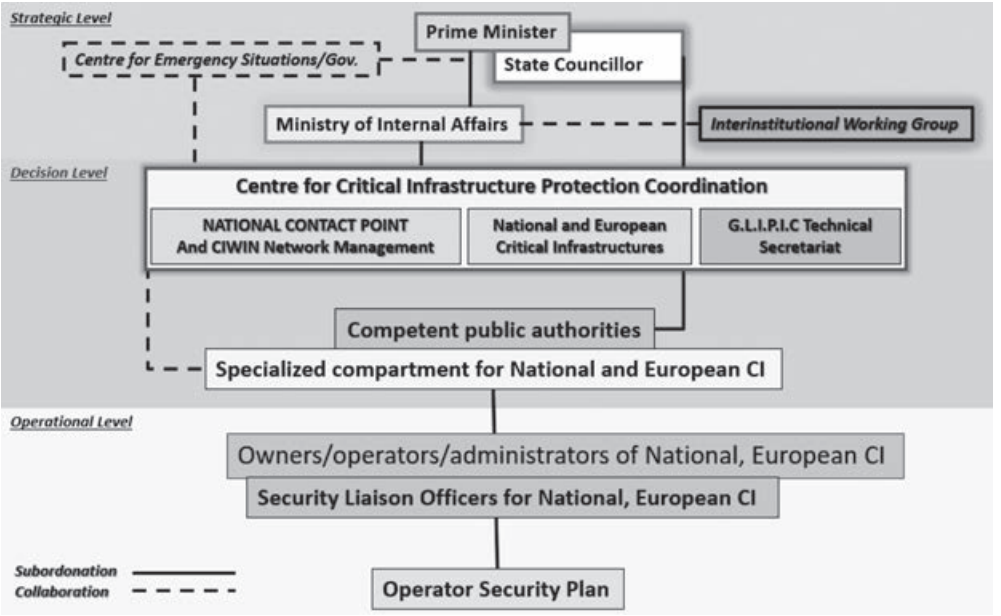


Figure 5: The Romanian model for Critical Infrastructure Protection in its basic form (upper) (Source: Mureșan & Georgescu, 2015)

Figure 5 expand on Figure 2 and reflect the Romanian model for a CIP framework that could be used as a basis for adaptation.

The end result should be a system which is as compatible with the European norms as that of any EU Member State, and thereby capable of cooperation and coordination with transborder CIP activities and existing mechanisms within the EPCIP, and also other governance mechanisms. This approach reflects not only the assistance that countries can receive, but also the reality of the regional interdependencies between critical infrastructures, and the existing governance mechanisms, making a convergent approach desirable, regardless of the state of political projects.

4.2 Cooperation with the EU

There are multiple levels of cooperation which are required within the SEE region.

The first is between the EU and the countries in question. The EU should make the implementation of the CIP framework a cornerstone of the accession process, and rate it just as highly as reforms in the judicial process and the general implementation of the "acquis". This should be accompanied by specific technical assistance for the implementation in each particular state. There are multiple models than can be applied – assistance may come at its own initiative, as part of security sector reform processes, or as part of a regional initiative such as the general cooperation framework with the EU (EC, 2020a). The latter is especially interesting as the EU-Western Balkans framework is sufficiently developed to permit a seamless integration of CIP efforts.

As hinted in the previous paragraph, the EU could make CIP a criterion for accession by labelling it as "capacity to manage the security outcomes of the interdependencies resulting from European integration". The EU is nominally involved only in the protection of European Critical Infrastructure, but it has published documents of reference pertaining to national systems as well, as one cannot have a framework for a national contribution to EPCIP without a national CIP system.

Updates to the Instruments for Pre-Accession Assistance (EC, 2020a) could also accommodate CIP transformation processes, especially since many of the areas of focus segue well into CIP areas, such as public administration critical infrastructure or food critical infrastructure. Another argument is the existence of a Western Balkans Connectivity Agenda investing in energy and transport (EC, 2020b), which are the two areas specifically addressed by EPCIP.

On the EU side, the Western Balkans Strategy (EC, 2020c) could be updated to reflect CIP processes as a priority, along with the six flagship initiatives of the European Commission in the Western Balkans. CIP efforts could be integrated without adding a new flagship initiative, as four of the initiatives already address the functioning of systems included in CIP frameworks:

- The initiative to reinforce engagement on security and migration with its focus on security, fighting terrorism and organized crime;
- The initiative to enhance support for socio-economic development, with impact on health and education, among others;
- The initiative to increase connectivity, with impact on energy and transport;
- The initiative for a digital agenda for the Western Balkans, which related to ICT infrastructure and, as remarked in a previous section, a cross-cutting issue for command, control, coordination and integration in all other critical infrastructures.

A first step in this direction would be to introduce CIP onto the agenda of the next EU-Western Balkans Summit in 2021.

In general, the EU should consider extending this form of assistance to all of its partners, regardless of whether or not accession will ever be in the cards. Whether we are discussing Eastern Europe, Turkey, or the Middle East and North Africa region, the EU features transborder interdependencies in critical infrastructure relating to energy, transport and national defence at the very least, and would therefore benefit from assisting these countries with CIP efforts and even integrating them, to a certain extent, in the EPCIP and ancillary initiatives, such as the Critical Infrastructure Warning Information Network (CIWIN).

In the long run, the EU should consider setting up a European Critical Infrastructure Protection Agency to take over and enhance EPCIP activities, and also introduce a component of cooperation with the EU's near abroad in CIP both operationally and as a "soft/smart power" and capacity building tool. Cooperation with South-Eastern European non-EU states would be an important factor in this.

The impact of the pandemic on Critical Infrastructure shows the lack of capacity and other investment of all European countries in critical health infrastructure and in the mitigation capacity of impact on related infrastructure. Changes will have to be made in the CI landscape and in CIP processes to address the stark inadequacies highlighted (GCP, 2020). Cooperation

with the SEE region will become even more important, as it is no longer just about transferring CIP expertise, but of simultaneous growth in CIP capacity across the whole of Europe.

4.3 Other Cooperation

There are also other formulas for cooperation which may enhance capacity in CIP. Those countries with NATO cooperation (such as Member States Albania and North Macedonia) could also develop CIP efforts within NATO's emerging CIP policies (Caşın, 2018). The regional politics do not allow for NATO to be an omnipresent actor in regional partnerships, but it may have a useful role to play in mediating the transfer of experience and good practice in CIP, especially for cybersecurity (Kocabas, 2017). The NATO-EU cooperation also touches obliquely on the CIP issues, especially through the common Declaration of 2016, which had 42 recommendations in 7 areas, with 32 concrete actions. The priority areas included countering hybrid threats, cyber defence and security, strengthening political cooperation and dialogue, common exercises, and maritime cooperation, as well as increased defence capacity. The overlap with CIP efforts is quite substantial, and the institutionalized cooperation between CERT-EU (the EU Computer Emergency Response Team) and NCIRC (NATO Computer Incident Response Capability) in the realm of cybersecurity is an important operational example.

We should also not neglect the role of bilateral and minilateral cooperation on CIP issues, especially when there are common interests at stake in the form of existing and impending interdependencies. EPCIP is focused on infrastructures which are critical to two or more Member States, but there is a role to be played in identifying and designating critical infrastructure affecting an EU Member State and a Western Balkan or SEE non-EU state, requiring the attention of both countries. This may involve cooperation between sectorial CERTs in the cyber realm, between the coordinating authorities in CIP, between regulating authorities, and so on. A case in point is the Iron Gates hydropower plant between Romania and Serbia. Another example is the Belgrade-Budapest railway under construction by a Chinese company as part of the 17+1 cooperation between China and its Central and Eastern European partners. As mentioned earlier, the perspective of Chinese investment in cross-border infrastructure in the CEE region, including the SEE part, raises not only political issues, but also critical infrastructure protection issues, as new interdependencies are fostered. The future pipelines crossing through the region, whichever may be built, are another opportunity for cooperation between states and between the EU and the non-EU states, in multiple possible formats, as well as an inducement to make available the resources and assistance for resilient development and governance.

4.4 Institutional Construction

One of the more successful initiatives in a regional with fraught and challenging relationships has been SELEC, which is geared specifically towards the South-Eastern Europe region, but focuses on transborder organized crime of all types, a theme which is adjacent to the issue of terrorism and even of Critical Infrastructure Protection. We contend that it would be both possible and helpful to create a South-East European Critical Infrastructure Protection Centre (SECIPC), possibly with EU backing or assistance from individual countries such as the US. Given the sensitive nature of the work undertaken, it could be placed in Slovenia. This would be another mechanism for technical assistance to generate and reform a CIP framework in the individual countries, while allowing for case by case cooperation on transferring experience and, very importantly, on the creation of links for consultation and early warning in the case

of critical infrastructure disruption or the manifestation of threats with disruptive potential. The representatives of the individual countries would come from the high level advisory and coordination body at national level for CIP operations. In the case of Romania, for instance, the main representative would be from within the Critical Infrastructure Protection Coordination Centre, which also organizes communication with European authorities.

Such an arrangement would provide an interesting form of flexibility. For instance, it could have China as an observer country, given the interest the countries in the region have displayed for the connectivity aspects of the Belt and Road Initiative. This cooperation would be more fraught in an EU-based framework, given China's designation as a "systemic rival" and the current anxieties in Brussels.

As the countries in the region enter the EU, the SECIPC would eventually be absorbed by the designated EU entity for CIP efforts, and the participants will have already experienced a much faster convergence with EU norms and practices with regard to Critical Infrastructure Protection.

Another variant, of interest in the wider region, would be to have Joint EU-NATO Integrated Operational Centres for certain CIP issues.

4.5 Trust Building

One of the main aspects that a workable framework for regional cooperation on CIP requires and, in general, any CIP effort that purports to generate resilience when it comes to transborder infrastructure networks, is trust. Building trust is key and is one of the most difficult elements of the framework, more so than the technical challenge of implementing a framework. Trust networks, with adequate safeguards, make it possible to exchange vital information of common interest pertaining to the changes in the security environment, the disruption of vital infrastructures with transborder effects, and the presence of cascading disruptions. These are all effects of terrorist activity or adjacent activities in the organized crime sector, and they are also the result of specific hybrid warfare activities.

The previous proposals, such as using the EPCIP or creating the SECIPC for operational cooperation, all have an underlying component of trust building that is implicit but remains unspoken. Countries are reluctant to share this information, even within established settings such as NATO. The ascent of cybersecurity as a cross-cutting element of the critical infrastructure security environment has also resulted in a deterioration of security outcomes, not just through the higher level surface contact between an asset or a system and an adversary-inhabited cyberspace, but also because of the reluctance of companies and countries to share any information regarding cyberattacks. NATO has tried to foster information-sharing on cyberattacks, given their role in hybrid and asymmetric warfare, especially in the context of Russian "new generation warfare", but success has been limited.

One possibility for the region would be the creation of an arrangement such as a South-Eastern European Crisis Prevention Association headquartered outside the region to act as a clearing house for information concerning CI disruptions, especially through cyberattacks. One of the other forms of cooperation which have been highlighted (such as the SECIPC) could include a Cyber Stability Board specifically to address the cyber exchange issues.

There must also be support for trust building measures between the local communities and state authorities, and between the business sectors operating CI and the state authorities, for the smoothing of internal CIP processes.

5 Conclusions

The South-Eastern European region features a challenging security environment in which a mix of factors threaten security outcomes as well as the cooperation necessary for resolving crises stemming from growing interdependencies. This article advances the view that a host of issues, including those related to certain terrorist threats, could be ameliorated through the implementation of Critical Infrastructure Protection frameworks in the region, and the pursuit of resilience in the functioning of critical infrastructure systems such as energy, transport, finance and others. These systems are interdependent not only nationally, but also across state boundaries, making cooperation necessary to address the risks, vulnerabilities and threats stemming from their operation. Terrorists may target these critical infrastructures to maximize the damage dealt and, increasingly, they have tools such as cyberattacks at their disposal and the exploitation of cybercrime in order to implement potentially devastating attacks with minimum investment and risk. The logic of "grey zone actions" with difficult attribution, under the threshold of a military response, which characterizes the murky cyber threat landscape makes such attacks against critical infrastructure a prime concern.

The article detailed a few possibilities for implementation and cooperation in the region, given that the EU Member States already have National Critical Infrastructure Protection systems aligned with EU norms and practices, along with a level of cross-border interaction and coordination capability between decision-makers. There are also other sources of good practice in CIP, giving rise to significant permutations in terms of cooperation and burden sharing for the assistance of the states in the Western Balkans (UN, 2019). We have focused on NATO and the EU because of the regional synergies and natural interdependencies, as well as the relative similarities between countries in South-Eastern Europe.

The object of this article was not to assess the state of CIP efforts in countries such as Romania, Bulgaria or Slovenia, or the existing frameworks in the Western Balkan states outside the EU, but to highlight the potential of cooperation for working towards a minimum viable level of regional CIP process performance and coordination ability that transcends the difficulties of political relationships or projects such as EU accession. A role should be played by NATO and by the United States as originator and constant developer of the CIP framework, but the EU is the only actor cooperating with all of the states in the region for the time being.

Moving forward, it is important to assess the current situation and to find a politically acceptable mechanism, in the long term, for CIP capacity building. This must focus part of the scarce security resources and decision-maker attention on the task of increasing resilience in the face of regional security trends and anticipated development in the critical infrastructure landscape, with impact also on wider European security.

6 References

1. Australia-New Zealand Counter-Terrorism Committee (2015) National Guidelines for Protecting Critical Infrastructure from Terrorism, as ANZCTC (2015), ISBN: 978-1-925290-43-1, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

2. Albrecht HJ., Getoš AM. (2010) *Researching Terrorism and Organized Crime in Southeast Europe*. In: Benedek W., Daase C., Dimitrijević V., van Duyne P. (Eds.) Transnational Terrorism, Organized Crime and Peace-Building. Palgrave Macmillan, London, ISBN 978-0-230-28147-9, https://doi.org/10.1057/9780230281479_8

3. Busuncian, T. (2007) Terrorist Routes in South-Eastern Europe. *Connections*, Vol. 6, No. 1 (Spring 2007), pp 85-102, https://www.jstor.org/stable/26323282

4. Caşın, M. (2018) *Understanding NATO's New CIP Policies: Common Efforts and Solidarity*. In Gluschke, G., Caşın, M., Macori., M. (Eds.) (2018) Cyber Security policies and Critical Infrastructure Protection. pp 311-320, Institute for Security and Safety, ISBN 978-3-00-058988-1, https://uniss.org/cyber-security-policies-and-critical-infrastructure-protection/

5. Coburn, A.W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., Harvey, T. (2019). *Cyber risk outlook*. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2019/

6. Department of Homeland Security (2003) *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, as DHS (2003) https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

7. European Commission (2008) *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri¼OJ:L:2008:345:0075:0082:EN:PDF

8. European Commission (2020a) *Enhanced EU engagement with the Western Balkans*, https://ec.europa.eu/neighbourhood-enlargement/policy/eu-and-western-balkans_en

9. European Commission (2020b) *Western Balkans Connectivity Agenda*, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/connectivity_agenda_brochure.pdf

10. European Commission (2020c) *Western Balkans Cooperation Agenda*, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/western_balkans_strategy_brochure.pdf

11. Falco, G. (2018) *Job One for Space Force: Space Asset Cybersecurity*. Cyber Security Project, Belfer Center, July 12, 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity

12. Georgescu, A. (2018) Pandora's Botnet – Cybercrime as a Persistent Systemic Threat. Future of Europe: Security and Privacy in Cyberspace, *Visio Journal* No. 3, Dec. 2018, Visio Institut, ISBN: 2536-1481-3

13. Georgescu, A. & Cirnu, C.E. (2019). Blockchain and critical infrastructures – challenges and opportunities, in *Romanian Cyber Security Journal*, ISSN 2668-1730, ISSN-L 2668-1730, Vol. 1 (1), pp 93-100

14. Georgescu, A., Vevera, V., Cirnu, C.E. (2019). The Proliferation of Cyber Weapons – Theory and Mitigation. In *Romanian Cyber Security Journal*, ISSN 2668-1730, ISSN-L 2668-1730, Vol. 1 (2), pp 37-46

15. Gheorghe A.V., Vamanu D.V., Katina P.F., Pulfer R. (2018) *Critical infrastructures, key resources, key assets. Risk, vulnerability, resilience, fragility, and perception governance*. Topics in safety, risk, reliability and quality, series 34, eBook ISBN 978-3-319-69224-1. https://doi.org/10.1007/978-3-319-69224-1. Springer International Publishing

16. Gheorghe, A., Schläpfer, M. (2006) Critical infrastructures: ubiquity of digitalization and risks of interdependent critical infrastructures, *Systems Man and Cybernetics* 2006. SMC '06. IEEE International Conference, Vol 1, pp 580-584

17. Gokce, Y. (2018) *Active Cyber Defense as a Pre-emptive Defense Measure*. In Tatar, U., Gokce, Y., Gheorghe, A. (Eds.) (2017), "Strategic Cyber Defense – a Multidisciplinary Perspective", IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2

18. Group of Concerned People (2020) *White Paper on European Critical Health Infrastructure*. Diplomat Magazine, May 13, 2020, as GCP (2020) http://www.diplomatmagazine.eu/2020/05/13/white-paper-on-european-critical-health-infrastructure/

19. Helbing, D. (2013) Globally networked risks and how to respond. *Nature* 497, pp 51-59. https://doi.org/10.1038/nature12047

20. Keating, C.B., Katina, P.F., Bradley, J.M. (2014) Complex system governance: concept, challenges, and emerging research. *International Journal of System of Systems Engineering* 5, pp 263-288.

21. Kocabas, Y.U. (2017) *Future of International Terrorism and NATO's Countering Measures*. In Morris, T., Hadji-Janev, M. (Eds.) (2017) Countering Terrorism in South Eastern Europe, pp 61-73, Vol. 131, IOS Press, ISBN: 978-1-61499-736-8, DOI 10.3233/978-1-61499-736-8-61

22. Matei, F. C. (2009) *Combating Terrorism and Organized Crime – South-Eastern Europe Collective Approaches*. Research Paper No. 133, July 2009, Research Institute for European and American Studies, https://rieas.gr/images/rieas133.pdf

23. Mureşan, L., Georgescu, A. (2016) *Critical Infrastructure Protection – Romanian Contributions and Experiences*. In Biriukov, D., Kondratov, S., Sukhodolia, O. (Eds) (2016) Green Paper for Critical Infrastructure Protection. pp 93-106, National Institute for Strategic Studies, Kyiv, Ukraine, ISBN 978-966-554-258-2

24. Nazir, S., Patel, S., Patel, D. (2017) Assessing and augmenting SCADA cyber security: a survey of techniques, *Computers & Security*, 70, pp 436-454, DOI: 10.1016/j.cose.2017.06.010.

25. O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H., Power, J.P., Corpin, M., Cox, O., Wood, P., Wallace, S. (2019) *Internet Security Threat Report*. Volume 24, Symantec, February 2019, Available at https://www-west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

26. Tatar, U., Geers, K., Georgescu, A. (2017) *A Framework for a Military Cyber Defence Strategy Workshop – Final Report*. In Tatar, U., Gokce, Y., Gheorghe, A., (2017), Strategic Cyber Defense – a Multidisciplinary Perspective, IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2

27. The United Nations (2019), *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices*, as UN (2019), https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

28. The White House (1998) *Presidential Decision Directive/NSC-63* (as PDD-63), Washington DC. https://clinton.presidentiallibraries.us/items/show/12762

29. Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Nat Hazards* 82, pp 175-192. https://doi.org/10.1007/s11069-016-2186-3

30. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21, pp 11-25. https://doi.org/10.1109/37.969131

31. Stytz, M., Banks, S. (2017) *The Nexus Between Cybercrime and Cyberterrorism*. In Morris, T., Hadji-Janev, M. (Eds.) (2017) Countering Terrorism in South Eastern Europe, pp 82-102, Vol. 131, IOS Press, ISBN: 978-1-61499-736-8, DOI 10.3233/978-1-61499-736-8-82

4 Historical and Legal Aspects of Cyber Attacks on Critical Infrastructure

Andrej Iliev, Ferdinand Odzakov

1 Introduction

With continued evolution of technology, the opportunities and challenges from cyber domain are rising. We are at a crossroads, as we move from a society already entwined with the internet to the coming age of automation and Internet of Things. In our everyday lives we can see that societies around the world more depend on modern technology, the ability to shut down or destroy critical infrastructure and to take control of machines and vehicles, directly causes economic losses to become a reality.

An analysis of the history of well-known examples of cyberattacks on critical infrastructure includes the following:

- In 2008 Russia sent tanks into Georgia, coinciding with a cyber attack on the Georgian government's computing infrastructure. This is thought to be one of the first coordinated land and cyber attacks (Cyber Security Trends 2016);
- Also in 2008, Stuxnet – a computer worm purportedly jointly designed by Israel crippled Iran's nuclear-enrichment programme by sabotaging centrifuges;
- In 2014, a German steelworks was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down;
- In 2015, in an attack which was strongly suspected to have originated in Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack. Operators at the control centre were even locked out of their systems during the attack, and could only watch it unfold (Coldwell, 2016).

In all of these, as an indication of how the landscape of war is changing, the weapon of choice wasn't guns or bombs – it was a keyboard. We can expect governments around the world to strengthen their cyberattack and defence capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But the results could be much more

subtle as to improve governments' intelligence-gathering capabilities and develop ability to surreptitiously manipulate markets, and they will continue to expand the definition and rules of engagement for cyberattacks.

The term "*cyber attack"* was first presented by author William Gibson in 1982, when he wrote his book "Neuromance". This book become very popular because it manages to explain today's virtual reality and network information activity to readers in a practical and constructive way. William Gibson defined "*cyberspace*" in a very simple way as a constructed virtual environment in which information or computer systems and networks have a dominant or primary role (Wall, 2007: pp.221-223).

The term "*cybercrime*" further symbolizes the security threats that come from the internet, actually through information and communication networks and systems. These security threats from the virtual information environment represent a breach of computer security. As we must legally define the term "security of computer" or "information systems", then the term "cybercrime" falls within the scope of criminal law. Cyber warfare, as a new model of proxy war, represents the future of modern warfare.

"Proxy" means giving someone authority to do something for another. For example: Small states uses proxy strategy to attack their stronger enemy, because they have comprehensive support from bigger state. States use proxies to project power through cyberspace, some capable of causing significant harm. In recent years, media outlets have published reports about proxies using Information and Communications Technologies (ICTs) from Northeast Asia to India, Pakistan, Middle East, and Eastern Europe (Maurer, 2016: pp 383-384).

The continual development of modern computer systems and networks means that they represent a continual proxy strategy for conducting modern cyber attacks. The high level of autonomy of computer systems and networks enables them to build an effective proxy warfare strategy in which the performer of this information operations is always at an advantage over the attacked side. On the other hand, implementing a proxy strategy of warfare over computer networks is a much simpler method than using sophisticated weaponry to perform the most advanced military operations. Vast classical armies are no longer an integral part of proxy warfare, the continued development of information technology is a necessity for executing a proxy strategy in cyber warfare, which as a mode of combat is increasingly a major segment of modern conflict, such as hybrid and comprehensive or compound warfare.

Attacks on critical infrastructure most often include: public gatherings, hospitals, shopping malls, infrastructures of strategic importance to national security, airports and other strategic facilities of the state, and through the vulnerability of their information and communication networks, the enemy can achieve a far more effective attack than by using large armed forces in which casualties could be numerous. In cyber warfare, where there is no use of military force, the attacker does not have casualties.

The Centre for Strategic and International Studies (CSIS) estimated that between May 2006 and June 2011 there were almost eighty "significant cyber incidents" that resulted in

"successful attacks on government agencies, defence and high tech companies or economic crimes with losses of a few million dollars" (Hopkins, 2012).

With a final goal of reprogramming industrial control systems, Stuxnet was a large, complex piece of malware with many different components and functionalities, a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. Stuxnet was a threat targeting a specific industrial control system like that of Iran, its ultimate goal was to sabotage a facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries (Falliere, et al., 2010: pp. 1-3).

In general, cyber-attacks can be separated into three major categories: (I) "automated malicious software" delivered over the internet, (II) "denial-of-service attacks" and (III) "unauthorized remote intrusions into computer systems". (Sklerov, 2009).

2 Historical Evolution of Cyber-Attacks on Critical Infrastructure

Critical infrastructure is vulnerable to all type of attacks, and increasingly to attacks committed through the internet. Cyber threats to critical infrastructure (CI) are an evolving security challenge that can impact global security, public safety and the economy in general. As the private sector owns and operates most of the (CI) assets networks, and governments are responsible for national security, securing (CI) against cyber threats is a shared responsibility of both the public and private sectors (H2020 700416, project, "Securing Critical Energy Infrastructures," http://www.successenergy.eu/).

The first period of the historical development of cyberattacks encompasses the technological development of information technology from the early 1980s to the end of the Cold War in the early 1990s. Here we will try to highlight the most important examples of cyber attacks and cyber operations during this decade. During 1982, then US President Ronald Reagan approved a "state secret" plan for the use of specific software capable of controlling gas supply pumps and their turbines in industrial gas production and distribution facilities in the former Soviet Union. Fortunately or unfortunately, this software was stolen by secret Russian agents during their stay in Canada. The software was able to change the flow rate of the gas pumps and thereby succeeded in causing them to malfunction. Former US Air Force Secretary and former Director of the National Reconnaissance Office, Thomas C. Reed, in his book "At the Abyss: An Insider's History of the Cold War," said that the psychological effect of this software and the effect on the Soviet Union's economic capacities, significantly speed up the process of ending the Cold War. US used cyber warfare during Iraq's invasion in 1991 (Hoffman, 2004). During Operation Desert Storm, a strategic air campaign was launched against Iraq's air defences, so that the command and control telecommunications information system was attacked by advanced computer software, causing electrical disruptions in Iraq's telecommunications information system (*Operation Desert Storm,*1997, Appendix V).

The second period of the development of cyber attacks is the next decade, from 1990 to the 9/11 terrorist attacks on the US in 2001. A virtual online war broke out between Chechens and pro-Russian forces in 1994. This virtual war on the internet simulated military operations which one or other party wanted to carry out in the field in a real sense. This sophisticated widespread action of internet psychological propaganda is known as psychological surgery.

Finally, it was found that the psychological operations were expressed through web portals and online simulations as a segment of cyber warfare which was funded through bank funds in Sacramento, California, which greatly helped to unite the Chechen Diasporas to end this cyber war as soon as possible (Thomas, 2002).

During the Second Russo-Chechen Cyber War from 1997-2001, numerous military records of assassinations of Chechen and Russian soldiers mounted on both sides appeared on the internet and official Russian and Chechen web portals.

The Russian authorities, on the other hand, conducted cyber attacks by hacking Chechen websites. The Russian Federal Security Service (FSB), with the Russian Special Forces "Spetsnaz", were responsible for preventing two Chechen web portals from operating (Bullough, 2002). This was internet psychological propaganda between the nations. What we can conclude, is that the Chechens' internet propaganda proved more successful. Digital videos and pictures of how a civilian Chechen bus was attacked by pro-Russian separatists with many of the passengers killed, and the activities in ambushes by Chechen militias on Russian military convoys, are just some of the propaganda material on internet web portals during 1999, which were officially denied by Russia.

The Kosovo crisis of 1999 is considered to be one of the first more sophisticated information wars. NATO prepared to carry out its air campaign in Serbia by bombing critical infrastructure targets in order to bring the country into collapse, thereby forcing Serbia to withdraw from Kosovo. Numerous hacker groups emerged, notably the "Black Hand", which launched serious cyber attacks on NATO's official and secret internet infrastructure. Unfortunately, although it cannot be confirmed with certainty, it is assumed that some of the hackers were from the Yugoslav Army. Their goal was more than clear to disable the NATO air military operations on critical infrastructure in Serbia. It is also assumed that the NATO missile incident at the Chinese Embassy in Belgrade was definitely the work of Serbian hackers, who managed to change the missile's flight, coordinates from its launch to the target (Bosnian Serb News Agency, 1999).

During September 2000, young Israeli hackers were able to hack into several Hezbollah and Hamas websites in Lebanon. The hackers attacked the operating systems of web portals and successfully penetrated and gave fake news through six web portals to: Hezbollah, Hamas and other organizations in Lebanon, as well as the Palestinian national authorities. This seemingly minor cyber attack escalated into an international incident. The Palestinian and other Islamic organizations called it"*a holy cyber war*" (*The Associated Press*, 2000). The hackers carried out cyber attacks against 3 high-ranking Israeli websites belonging to the Israeli Parliament, the Foreign Ministry and the Israeli Defence Forces. Later, they also launched a cyber attack on the office of the Israeli Prime Minister, the Bank of Israel and the Tel Aviv Stock Exchange. By January 2001, the cyber conflict had affected more than 160 Israeli and 35 Palestinian major web portals.

About 548 domains of Israeli websites were hacked in the Middle East. The most common cyber attacks were websites malfunctions and operating system attacks. Cyber attacks on telecommunication companies were also carried out. Palestinian hackers succeeded in destroying Israel's Net Vision, which supplied about 70% of the national internet communications.

The third and last historical period of cyber warfare begins after the 9/11 terrorist attacks on the United States in 2001. The first significant cyber-attack in this third period was in Estonia in 2007. Estonia, a small country with a population of just over 1.3 million, had a boom in the use of internet technology in a very short period of time. Similarly to many advanced countries in the implementation of internet technology, the Estonian government made the whole of Estonia a virtual domain in November 2005. Meetings at the highest national level, and other business meetings were conducted online, through the virtual domain, as well as documents signed with electronic signatures and Estonian citizens were able to vote electronically through their computers.

Estonia was ranked 23rd in readiness and implementation of advanced information technology. Over 60% of the population had electronic bank accounts, while 95% of bank transactions were made electronically. All of this was tempting to the interests of numerous hackers wanting to test the Estonian cyber defences (Farivar, 2007). On 27 April 2007, the Estonian government relocated a monument to the victims of the Soviet Armed Forces' liberation of Estonia from the fascist regime during World War II. This simple act of moving the monument from the centre of Estonian capital, Tallinn, outside the city, sparked in protests and clashes between Estonians and Russians. The protests were followed, by numerous cyber-attacks from Russian hackers targeting the operating systems of national and private firms and enterprises. During the cyber attacks the Estonian government's website, had a normal flow of 1000 emails per day and spam messages of 2,000 per second. The government network was designed to handle 2 million megabits per second and the servers were flooded with nearly 200 million megabits per second during the cyber attacks. The longest attack lasted over 10 hours and generated over 90 million megabytes of data per second. Because of this, the websites of the Ministry of Foreign Affairs and Justice were shut down until the cyber attacks on websites could be neutralized and normal service restored. The banks in Estonia were closed, which in addition to the national financial losses, was also felt in international banking (Wilson, 2008).

On 15 May 2007, Russian hackers succeeded in disabling Estonia's national telecommunications information system, E-112, although while the Estonian authorities officially acknowledged this, Russian authorities refused to admit it (Eneken, et al., 2010: pp 15-34). USA and NATO sent teams of computer security experts to help the Estonian authorities cope with the massive wave of attacks on operating systems that paralyzed the country's government websites, banking industry and media. What was of particular interest to computer security experts at the time, was that although the cyberattacks only lasted for several weeks, their intensity was really high. The coordinated and quickly activities of NATO allies stabilized the cyber security in Estonia. However, the websites of the national authorities, the State Office and the Federal National Election Committee were also targeted by cyber attacks during May 2007.

The British Security Service, the office of the French Prime Minister, and the office of the German Chancellor, Angela Merkel, have all complained to China about cyberattacks on their government networks. Merkel has even raised the issue with the Chinese president. So far, no official source in China has acknowledged involvement in these cyber attacks.

Expert estimates showed that would take several years for the development of classified information equipment and a type of cyber-worm that would be more sophisticated than commercial software, but the estimates were that cyber attacks on operating systems would be successful. Those who carried out the cyberattacks on nuclear power plants must have had access to highly restricted and classified information systems and equipment (Lewis, 2009: pp.9-11).

During 2011, Canadian government reported a major cyberattack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defense. The attack forced Canada's main economic agencies, to disconnect from the internet. In July 2011, the US Deputy Secretary of Defense stated that a defence contractor had been hacked and 24,000 files from the Department of Defense had been stolen. The Russian firm Kaspersky discovered a worldwide cyber attack dubbed "Red October", during 2012 which had been operating since at least 2007. The hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs. The primary targets of the attack appeared to be Eastern Europe, the former USSR and Central Asia, although Western Europe and North America also reported victims. The virus collected information from government Embassies, research firms, military installations, energy providers, nuclear power stations and other critical infrastructures. In 2013 the South Korean financial institutions came under cyber-attacks, when the Korean broadcaster YTN had their networks infected, in an incident said to resemble past cyber efforts by North Korea (Adair, 2009).

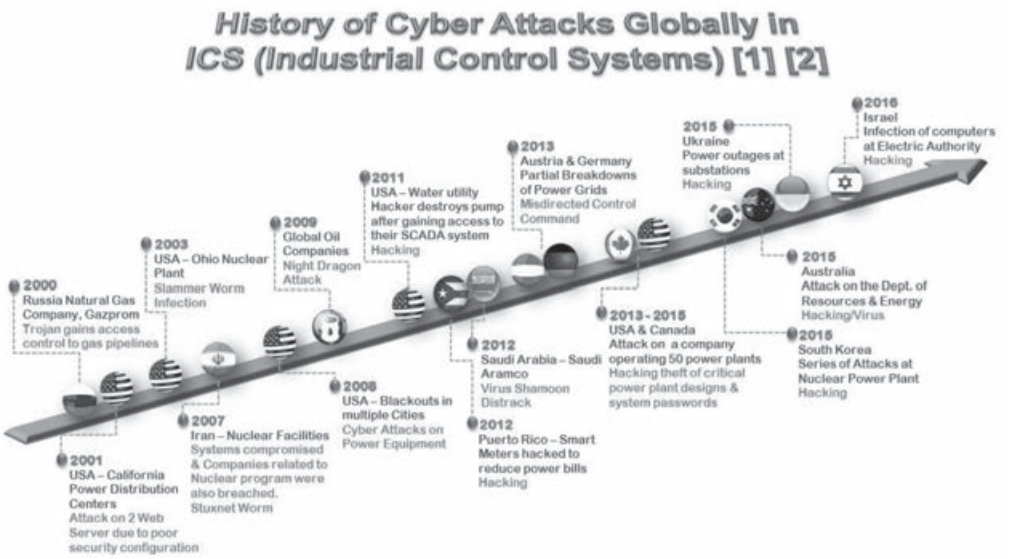


Figure 1: History of global cyber-attacks on critical infrastructure[1]

In a direct cyber-attack, ISIS' attempted to hack US electrical power companies in October 2015. In Europe, the most well-known event, until recently was the Ukrainian power grid cyber-attack in December 2015, where attackers hacked the Ukrainian utilities' networks, gained access and manually switched off power to 43 electrical substations. In December 2016, Ukraine suffered another cyber-attack, this time it was fully automated, as hackers struck an electricity transmission station north of the city of Kiev, blacking out a portion of the Ukrainian capital equivalent to a fifth of its total power capacity (Ukrainian Ministry of Energy and Coal, January 2016. http://mpe.kmu.gov.ua/minugol/control/ publish/ article? artid= 245 082298).

1 https:is5com.com/uncategorized/nov-22-2017-cyber-immunity-a-holistic-view-for-industrial-control-systems/

3 Legal Aspects of Cyber-Attacks on Critical Infrastructure

Bearing in mind the historical development and perspectives of cyber warfare, what we know so far is that the EU, together with NATO, have developed a cyber security strategy, over past few years all the NATO and EU members have developed their own national cyber security strategies that are in coordination with the European Commission and EU legislation and norms for NATO member states (Appazov, 2014: pp 38-42).

From the point of view of international law, the Estonian cyberattack can be described as an 'unjust' cyber-attack. Seen from the perspective of *jus ad bellum*, the attack lacked a sufficient just cause, and was not undertaken in any meaningful sense as a last resort. From the perspective of the just conduct of hostilities – *jus in bello* – the attack was utterly indiscriminate and disproportionate in its threat of harm, at least, when compared either to the harm Russia or its citizens were allegedly suffering, or to any legitimate military objective that might have otherwise been under consideration. The cyber attack on Estonia led NATO to establish Cooperative Cyber Defense Centre of Excellence (CCD COE) in Estonia in May 2008, with a staff of 30 specialists. It became operational in August 2008 and is part of a NATO network of thirteen accredited Centres of Excellence dedicated to training representatives from NATO member countries on "*technically sophisticated aspects of NATO operations"* (NATO Cooperative Cyber Defence Centre of Excellence,2018). The CCD COE focus is on coordinating cyber defence, and establishing policies for aiding allies during cross-jurisdictional attacks.

The European Union (EU) strategy for cyber security is based on five principles that will be priorities for the future of the EU. The EU's official stance emphasizes that cyber security is just as important as security in physical space. In accordance with the official text of the EU cyber strategy, the most important five principles are the following:

- Achieving cyber resilience;
- Reducing cybercrime;
- Developing a cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- Developing industrial and technological resources for cyber security, and
- Establishing a coherent international cyberspace policy for the EU, and promoting core EU values (European Commission, 2013: pp 4-5).

During 2016 the EU-NATO collaboration began to take shape. At a summit in Warsaw, the Presidents of the European Council, the European Commission and NATO's Secretary General signed a Joint Declaration for better security cooperation between the institutions. The Joint Declaration emphasized seven categories for cooperation between NATO and the EU. Two were directly applicable to cyber defence: countering hybrid threats, and cyber security and defence (EU-NATO cooperation – Factsheet, 2019).

The last decade's developments in digital information technology have dramatically increased interdependencies between the critical infrastructures. Energy infrastructure provides essential fuel to all other critical infrastructure sectors, as without energy, none of them can operate properly. In turn, it depends on other critical infrastructure sectors, such as communications and information technology. The image above provides a simplified illustration of the interdependencies between 16 critical infrastructure sectors, including the four critical sectors (i.e.

energy, water, communications, and transportation) that provide lifeline functions to all other critical infrastructure sectors.

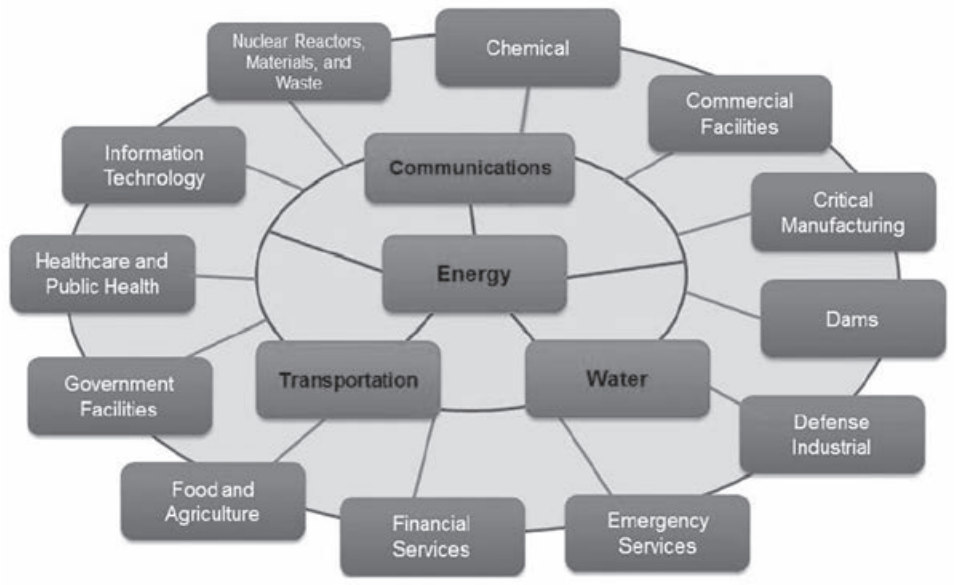


Figure 2: Critical Infrastructure Interdependencies[2]

Electricity, as part of critical infrastructure, provides essential power to the communication, transportation, water sectors and in return subsectors rely on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as the control and operation of infrastructure (communication), (Lindstrom, 2019: pp 37-41).
The EU Task Force in cooperation with NATO developed three phases for strengthening the EU's cyber defence capabilities as follows:

- Base Case: implementing the 2017 Cyber Security Package;
- Cyber Security Strategy from 2018;
- Establishing a Cyber Defence Coordinator;
- Creating a Cyber Defence Agency.

The final goal was to create the Cyber Defence Agency. This was carried out in five stages:

- The implementation of the NATO and EU Cyber Security Package from 2017, according to the EU Cyber Strategy from 2018, and the Cyber Defence Policy Framework;
- The creation of a Cyber Defence Coordinator, in coordination with the European Agency for Cyber Security (ENISA), the EU Council, and the European Commission, alongside other agencies such as the EDA;
- Under the guidance of the Coordinator and through prominent collaboration with industry, the implementation of a series of cooperation-oriented tasks that would lead to the development of a technical attribution forum;
- Under the guidance of the Coordinator, the investigation and drafting of a mandate for a governance model for a Cyber Defence Agency Stage;

2 Critical Infrastructure Protection: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of the Europe Project: H2020–CIP-01-2016–740898

- The creation of a Cyber Defence Agency that encompasses the coordinating functions of the Coordinator, ENISA's advisory capacity developed under the 2017 package, and specific, core executive functions (Scheffer, 2018: pp 65-67).

During 2019, the European Commission gave its recommendations to (ENISA) for the cyber security of modern 5G networks. This toolbox includes:

- An inventory of the types of security risks that can affect the cyber security of 5G networks (e.g. supply chain risk, software vulnerability risk, access control risk, risks arising from the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries);
- A set of possible mitigating measures (e.g. third-party certification for hardware, software or services, formal hardware and software tests or conformity checks, processes to ensure access controls exist and are enforced, identifying products, services or suppliers that are considered potentially not secure, etc.). These measures should address every type of security risk identified in one or more Member States following the risk assessment. The Member States of the EU, together with the European Commission, should identify the conditions concerning the security of public networks against unauthorized access, to be attached to general authorization and security requirements for networks and for the purposes of commitments participating in procedures for granting rights of use of the spectrum in 5G bands pursuant to Directive 2002/20/EC. The EU Member States should cooperate with European Commission to develop specific security requirements that could apply in the context of public procurement related to 5G networks. This should include mandatory requirements to implement cyber security certification schemes in public procurement, insofar as such schemes are not yet binding for all suppliers and operators. EU Members should cooperate with the European Commission to assess the effects of this recommendation by 1 October 2020, with a view to determining appropriate ways forward (European Commission. Cyber security of 5G networks, 2019: pp 7-8). This assessment should take into account the outcome of the coordinated European Union risk assessment from cyber threats.

4 Conclusion

Critical infrastructure (CI) systems will continue to depend on information systems and electronic data. Reliance on the power grid and telecommunications will also continue to increase, as will the number of attack vectors and the attack surface, due to the complexity of these systems and higher levels of connectivity due to smart networks. The security of these systems and data is vital to public confidence and safety (Dell Annual Threat Report, 2015). Cyber-attacks and sabotage of critical infrastructures are threats which are present both now and in the future. In the future we will observe an increase in attacks on data brokers, physical infrastructures, and telecommunication networks, such as global denial of service attacks on all connected services. New forms of CI, such as social media platforms, will become a prime target for cybercriminals (Kaspersky and Critical Infrastructure Protection, 2015). Exploitation of existing vulnerabilities, *"zero day attacks"* (days without attacks), and targeted phishing attacks will increase and continue to pose threats against critical infrastructures, owing to the complex mix of legacy systems and new components, combined with the need to minimize business disruption and cost, which often delays upgrades and updates. A lack of supplier support and policies also has a significant impact on the security of CI. Employees with

privileged system access will remain key targets and subject to social engineering attacks (Report on Cyber security and Critical Infrastructure in the USA, 2015). Strengthening cyber security requires a combination of prevention, detection, incident mitigation, and investigation. Addressing the vulnerabilities of critical infrastructures necessitates a cooperative approach from the public and private sectors, and connection between the local and the international dimensions. The challenge of protecting critical infrastructures requires the management of competing demands between security and privacy (Report on Destructive Cyber-Attacks Blitz Critical Infrastructure, 2015). Almost half of security professionals think that a successful cyberattack will take down critical infrastructure and cause the loss of human life within the next three years (Critical Infrastructure Readiness Report, Aspen institute, 2015).One of the three most powerful states in the world, the United States, through its government, sponsored website Cyber Seekers, constantly advertises cyber security job openings in the United States. New roles and jobs in cyber security arise beyond the typical job roles. More interactive information, knowledge and shared experience can be found on the US National Initiative for Cyber Security Education (NICE) website (see below). With the rapid development of information technology, it is more than necessary for both government and private sector employees to be educated and trained in the field of cyber attack management, and in the implementation of appropriate legal regulations and mechanisms for legal protection and cyber-attack sanctions.

In 2013, NATO's Computer Incident Response Centre (NCIRC) upgrade project from 58 million EUR for enhancement of NATO cyber defence. This major capability will help NATO better protect its networks from the increasing number of cyber-attacks against the Alliance's information systems.

As an initial example to other world states, the US government established the National Institute for Cyber Security Education (NICE). Together with the Department of Education and other agencies, NICE launched a four-pronged strategy to build a cyber secure nation through training, awareness, post-graduate educational programmes and development for federal security professionals. To meet this goal, NICE targeted a broad range of the population as prospective employees: including students and private sector partners (USA National Cyber Strategy, 2018: pp 5-8).

Cyber security reform legislation should make these arrangements permanent. Government agencies should be given the authority and resources to initiate new recruitment and education campaigns, and to extend the scope of the existing ones. Firstly, more cyber security will be needed to manage the increase in connectivity, so there will be an increase in demand for cyber security jobs. Secondly, through enhancing its presence in recruitment and education, the federal government could attract individuals to take part in these cyber security jobs who might otherwise have joined the ranks of Anonymous or other hacker groups. Granted, people who are anti-government or even apathetic towards government may not be persuaded by the government's recruitment efforts, but for those young people who exhibit exceptional computer skills and seek a community which utilizes and appreciates these skills, the recruitment and education campaigns will certainly aid governments in this mission.

The need for cyber security professionals is increasing day by day. The driving factors for this are: the increasing number of useful internet and social networks, the use of smartphones, and the electronic commerce of most financial and industrial corporations among other things. All

of this increases the interest in cyber-attacks on information systems and networks, especially in large financial and industrial corporations, whose functionality as been negatively affected not only at a national but also at a regional level, especially in the most powerful states in the world which, for example: exports electricity, natural gas and petroleum products. Many scientific papers point out that there is a shortage of staff, especially for high-quality cyber security professionals.

NATO is setting up a new Cyber Operations Centre in Mons, Belgium. The Centre will be fully operational by 2023 and will support military commanders with situational awareness to inform operations and missions and strengthen NATO's cyber defence. The centre will also coordinate NATO's operational activity in cyberspace, ensuring the freedom to act in this domain and making NATO operations more resilient to cyber-attacks (nato.int/nato_static_fl2014/assets// pdf_2019_02/2019 0208_1902 cyber-defence-en.pdf). The International Information System Security Certification Consortium (IISSCC) has made the final analysis for the workforce needed for better cyber security. The cyber security workforce gap by 2022 is on pace to hit 1.8 million experts. (USA National Initiative for Cyber security Careers and Studies, 2017).

5 References

1. Artur Appazov. Legal aspects of cyber security, University of Copenhagen,2014.
2. Bosnian Serb News Agency SRNA. *"*Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer", 28 March 1999.
3. Clay Wilson, Botnets. Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress, January 29, 2008.
4. Critical Infrastructure Readiness Report, Aspen Institute and Intel Security, 2015.
5. Cyber War Also Rages in Middle East, *The Associated Press*, 28 October 2000.
6. Cyrus Farivar."Cyber war I. What the Attacks on Estonia Have Taught Us About Online Combat", *Slate*, May 22, 2007.
7. Cyber Security Trends 2016, Cybernetic Global Intelligence.cgi-content-imagesandcode. cyberneticglobal.netdna-cdn.com/wp-contentuploads/2015/11/cyber-predictions-2016-v2, accessed on 20.10.2019.
8. David E. Hoffman. "CIA slipped bugs to Soviets", *Washington Post*, 27 February 2004.
9. Dell. Annual Threat Report, 2015. http://www.dell.com/learn/us/en/uscorp1/press-releases/2015-04-13-dell-annual-threat-report, 2015.
10. Eneken Tikk, Kadri Kaska and Liis Vihul. *International Cyber Incidents: Legal Considerations*, Tallinn, Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.
11. David S. Wall. Cybercrime: the transformation of crime in the information age, Cambridge, 2007.
12. European Commission. Cyber security of 5G networks, Strasbourg, 26.03.2019.
13. European Commission. Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013.
14. European Union External Action Service. "EU-NATO cooperation – Factsheet" (https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en).
15. French Coldwell, Chief Evangelist. National Fintech Cybersecurity Summit 2016, Sydney.

16. Gustav Lindstrom and Thierry Tardy. The EU and NATO essential partners, European Institute for Security Studies, Brussels, 2019.
17. Info Security Magazine. Destructive Cyber-Attacks Blitz Critical Infrastructure – Report. http://www.infosecurity-magazine.com/news/destructive-cyber-attacks-critical/, 2015.
18. Jaap de Hoop Scheffer. Strengthening the EU's Cyber Defence Capabilities: Report of a CEPS Task Force, Centre for European Policy Studies (CEPS), Brussels, November 2018.
19. James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Centre for Strategic and International Studies (CSIS), October 2009.
20. Jose Nazario. Politically Motivated Denial of Service Attacks, Arbor Networks, 2009.
21. Kaspersky. Critical Infrastructure Protection, 2015.
22. Matthew J. Sklerov. Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defences Against States Who Neglect Their Duty to Prevent, Military Law Review, 2009.
23. National Cyber Strategy of USA, USA, September 2018.
24. National Initiative for Cyber Security Careers and Studies. "NICE Cyber Security Workforce Framework", USA, 12 December 2017.
25. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manuel Process.
26. Nick Hopkins. China – "Targets NATO Chief" in Facebook Spying Operation, The Observer, 11 March 2012.
27. Nicolas Falliere, Liam O Murchu and Eric Chien. W32 Stuxnet Dossier, Symantec Corporation, USA, 2010.
28. Oliver Bullough. "Russians Wage Cyber War on Chechen Websites", *Reuters*, 2002.
29. Operation Desert Storm: Evaluation of the Air Campaign, U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, 12 June 1997, Appendix V.
30. Recorded Future, Real-Time Threat Intelligence for ICS/SCADA Cyber Security, http://go.recordedfuture.com/hubfs/data-sheets/ics-scada.pdf, 2014
31. Steven Adair. Korean/US DDoS Attacks – Perplexing, Disruptive, and Destructive, 31. Shadow Server Foundation Calendar blog, 10 July 2009.
32. Timothy L. Thomas. "Information Warfare in the Second Chechen War: Motivator for Military Reform?", Foreign Military Studies Office, Fort Leavenworth, Kansas, 2002.
33. Tim Maurer. "Proxies" and Cyberspace. Journal of Conflict & Security Law (2016), Oxford University Press , Vol. 21 No. 3.
34. Trend Micro. Report on Cyber security and Critical Infrastructure in the Americas, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/ reports/critical-infrastructures-west-hemisphere.pdf, 2015
35. https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref
36. https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
37. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet -cyber-defence-en.pdf
38. https://niccs.us-cert.gov/workforce-development/cyber-security-force-framework
39. https://ccdcoe. org/research/Tallinn-manual/
40. https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en.
41. https://www.thinkoutcyberbox.com.au/

5 Cyber Threats to Maritime Critical Infrastructure

Andrej Androjna, Elen Twrdy

1 Introduction

1.1 Definition of Maritime Critical Infrastructure in the Republic of Slovenia

The critical infrastructure of national importance in the Republic of Slovenia encompasses those capacities that are crucial to the country. The suspension of its operation or its destruction would have a significant impact on national security, the economy, and other key social functions, as well as on the health, safety, protection and wellbeing of the people.

The identification and designation of critical infrastructure, the principles and planning of its protection, the tasks of bodies and organizations in the field of critical infrastructure, and the communication, reporting, decision-making support, data protection and control in the field of critical infrastructure are governed by the Critical Infrastructure Act (2017). The law defines the following sectors as critical infrastructure: energy, transport, food, drinking water, healthcare, finances, environmental protection, information and communication networks and systems.

Maritime critical infrastructure is defined as a capacity whose serious malfunction or activity interruption could impede port operations in the Port of Koper for at least a week. The Port of Koper d.d. represents a great generator of development in Slovenia, so its smooth and safe operation is crucial. Any serious malfunction of the operations in the Port of Koper d.d. would affect the interruption of goods flows away from and into Slovenia. Therefore, great care should be taken to ensure the safety of this critical infrastructure.

1.2 European Critical Infrastructure

The European Critical Infrastructure (ECI) of the Republic of Slovenia is the infrastructure located within the territory of our country, and is determined in accordance with the regu-

lations governing European Critical Infrastructure. The ECI in the Republic of Slovenia is regulated by the *Regulation on European Critical Infrastructure* (2011) which transposes into the acquis of the Republic of Slovenia in the *Directive on the Identification and Designation of European Critical Infrastructures and Assessment of the Need to Improve their Protection*.

The European Union has identified ports as critical infrastructure; the term "port" means any designated land and sea area with boundaries defined by the Member State in which the port is located, and equipment and infrastructure to facilitate commercial maritime transport (Directive 2005/65/ES3).

In fact, ports are today the key intermodal hubs in both the freight and passenger transport networks of the European Union (EU). In addition to being important border checkpoints, they also play an important role in international trade. Maritime goods flows are constantly expanding, and maritime transport confirms its crucial role in the functioning of our society and our economy (SECNET, 2019).

The security of ports and the efficiency of their operations is therefore crucial not only for maritime transport, but also for their strategic role in terms of security at the regional, national and European levels. Port security is thus an opportunity to automate and simplify procedures and activities in ports (Andritsos, 2013), and can also benefit from information and communication technology (ICT).

In the context of physical and cyber security, new challenges, threats and strategies to overcome them have led to ports' automation and digital transformation, the optimization of existing processes, the monitoring of real-time operations, the interconnection of information technology (IT) and operational technology (OT), and the deployment of new technological capabilities (e.g. cloud computing, the Internet of Things (IoT), etc.).

2 Port Infrastructure

Port infrastructure and services are quite diverse across EU Member States. Over time, ports have adapted their infrastructure and services to local geographical features and activities related to their location (fishing pools, tourism, etc.) and the various challenges they have had to face. Port infrastructure ensures that vessels can be safely anchored and moored, allows vessels to pass between water areas at different levels (e.g. barriers), or provides facilities for the construction and repair of vessels (e.g. dry docks). It consists of marine (waveguides, excavation, barriers, river basins, coast, piers, moorings, etc.) and land infrastructure (inland roads, railways, promenades, etc.), administration buildings, and terminals. The management of port facilities is usually entrusted to private terminal operators who are in charge of managing and maintaining the upgrades (such as transhipment machinery, silos, special fences, control devices, passenger terminals) to carry out individual operations or activities related to the transhipment of maritime goods (shipping containers, general cargo, bulk cargo, petroleum products, etc.), passengers or motor vehicles (Ro-Ro and passenger ships), and fisheries (transhipment, inspection, etc.).

The fact is, however, that new technologies are, in principle, changing all maritime activities from navigation to freight transport management, e.g. customs clearance, setting deadlines, delivery, storage in warehouses, storage on board ship, and the management of all communi-

cations and information about the movement of goods and people to which large quantities of money-related data are connected and which are susceptible to cyber-attacks (ENISA, 2019).

2.1 Port Connections to the Hinterland

Transport connections with the hinterland are a prerequisite for the existence and development of a port. They affect the operation of each port, since without proper connections no port could provide the necessary services to its hinterland.

No special technology is required to connect ports to road transport; only truck access to the storage areas where cargo is transhipped is required. This means that in addition to the roads, a large enough parking space is needed where trucks can wait and complete all the necessary customs formalities. The entry and exit of trucks to and from a port presents a particular problem. Everybody must carry out the entry and exit procedures at a certain place, which causes congestion and therefore heavy traffic.

However, the connection of a port to the railway network does require special infrastructure. It is important that the piers where the goods are transhipped are equipped with rails, since the operation time is significantly shorter. The optimal and direct connection of a port railway infrastructure to the main railway infrastructure in an individual country is essential here, as the aim is to transport as much cargo as possible to the hinterland by train.

The technical equipment of a port and good organization of work are very important because the quality of service and the success of the port depend on this. It is therefore necessary to constantly adapt to the rapid development of transport technologies and new technological requirements such as digitization and automation. This is especially true for those port operations which are today dependent on information technology.

2.2 Port Operations

Roberts (2015) states that today cargo handling is the focus of port operations, but its tracking system is not the only one that is exposed to cyber threats. Today, ports rely as much on computer networks as they do on stevedores. Special network control systems control the loading and unloading of cargo. All types of transhipping equipment, such as container manipulators and portal transporters, now use technologies such as optical recognition of port operations management, including cargo localization, transportation, inspection, and so on. In state-of-the-art ports (Rotterdam), shipping containers are automatically loaded/unloaded and moved using GPS (Kramek, 2013). Vehicles that automatically transport cargo from terminals are also highly dependent on the efficient operation of GPS, which makes the modern port operating system vulnerable. Potential GPS jammers can make it difficult or even impossible for an entire port to operate. The closure of a port may result in a revenue loss of several million (including a consequent impact on GDP at both regional and national levels) (Orsoz, 2010; Business Wire, 2015).

3 Regulation at International and European Levels

The EU does not only have interests but also duties in global maritime security. It therefore actively contributes to safety and security at sea in different parts of the world, making use

of several existing EU instruments such as the Instrument contributing to Stability and Peace (IcSP) and the European Development Fund, as well as EU policies such as the Common Security and Defence Policy (CSDP).

3.1 Regulation at International Level

At the international level, the SOLAS Annex XI-2 was added in 2002 to the *International Convention for the Safety of Life at Sea – SOLAS* (IMO, 1974), resulting in the *International Ship and Port Facility Security – ISPS* (IMO, 2002), which introduces, in particular, measures aimed at enhancing the protection of merchant ships in international and inland liner shipping, as well as port security measures (including cyber security). The Code obliges Member States to prepare *Port Facility Security Assessments* (PFSA) for all their ports, which should take into account the specificities of the different port units (physical security, integrity structure, personnel protection systems, procedural policies, radio and telecommunications systems, computer systems and networks, and transport infrastructure), as well as containing a *Port Facility Security Plan* (PFSP) within the port boundaries (access, restricted areas, cargo handling, delivery of shipping, and security controls).

The *Convention on Facilitation of International Maritime Traffic* (FAL) by the International Maritime Organization (IMO 2017) simplifies and harmonizes the procedures of maritime transport by standardizing the use of electronic information transmission (the "Single Window" concept – SafeSeaNet), and streamlining reporting formalities for ships in the process of sailing in and out of the port.

Cyber security in international maritime space is only specifically tackled by the *Guidelines on Maritime Cyber Risk Management* (IMO, 2017) which aim to raise awareness of the protection and enhancement of the flexibility of cyber systems supporting the operation of ports, vessels, maritime facilities and other elements of the maritime transport system (IT, OT).

3.2 Regulation at the Level of the European Union

Legal acts and decisions concerning maritime safety improvement measures taken in an international environment are directly or indirectly related to EU law:

- Certain chapters of the SOLAS Convention have been transposed into the EU by several regulations: *Regulation (EC) 725/2004* relates to the enhancement of ship and port facility security and the implementation of the International Ship and Port Facility Security Code (ISPS), while *Directive 2005/65/EC* focuses on enhancing port security. *Regulation (EC) 336/2006* governs the implementation of the *International Safety Management Code within the Community – ISM* (IMO, 1995/2017) in the maritime sector of the Community, but does not apply to ports;
- *Directive 2010/65/EU* defines the formalities (FAL forms) of reporting ships arriving in and/or departing from ports of the Member States and dictates the introduction of the *SafeSeaNet* system for the secure exchange of information between Member States' maritime authorities and other authorities (e.g. customs systems).

In 2014, in support of the protection of the interests of the EU and the protection of its Member States and citizens, the EU adopted the *European Union Maritime Security Strategy* (EUMSS, 2014) and its Action Plan, which combines the internal and external aspects of EU maritime security. It tackles maritime risks and threats on a global scale, including cross-border and

organized crime, threats to freedom of navigation, critical maritime and energy infrastructure, cyber security, threats to biodiversity, illegal, unreported and unregulated fishing, and environmental degradation through illegal or unintentional releases.

With the increasing digitalization of business and the rapid development of information and communications technology, the volume of personal data collection and the flow of information about users is increasing. This creates more and more opportunities for abuse and violation of privacy rights. For this reason the EU adopted the *General Data Protection Regulation – GDPR* (2016) which aims to harmonize and raise the level of protection of personal data in various sectors of the EU, including the maritime sector.

The European Union has developed a comprehensive cyber security policy to prevent and combat cybercrime. In May 2018, a new *Cybersecurity Act* came into force to strengthen Europe's cyber resilience. The European Union Agency for Cybersecurity (ENISA) was also set up to assist Member States in effectively preventing and responding to cyber-attacks.

In connection with cyber security at the EU level, *Directive 2016/1148* (NIS Directive) was adopted concerning measures for a high common level of security of network and information systems across the Union. The maritime sector is subject to the security requirements applicable to businesses, ships, port infrastructure, ports and shipping services, including radio and telecommunications systems, computer systems and networks. It was also defined that Member States should take into account the existing and future international codes and guidelines, especially those developed by the IMO, in order to ensure a coherent approach for individual operators in the maritime sector when designating operators in the Water Transport Sector.

In addition to international and European legislative (including political) initiatives, several Member States have developed their own initiatives to improve cyber security at the national level and also with a focus on the maritime sector, such as national cyber security strategies, good practices or recommendations, for example, the French CIIP act, the British Code of Practice of Cyber Security for Ports and Port Systems, and the German "IT-Grundschutz," (ENISA, 2019).

4 Examples of Threats to Maritime Infrastructure

According to the European Commission, the economic impact of cybercrime increased fivefold between 2013 and 2017 and could increase fourfold again by 2020. By 2016, 80% of European businesses suffered damage from attacks. Since the first known attack in Estonia in 2007, both citizens and entire countries have been affected (SECNET, 2019).

Today port authorities are, more than ever, facing increasing risks with ever-increasing responsiveness, so the area of their responsibility is constantly broadening.

4.1 Infection of Authentication Data for High-Value Cargo Theft or Illicit Trafficking in a Targeted Attack

Among the more notable examples of an attack on port critical infrastructure is certainly the hacking attack in the Port of Antwerp in 2012, where computer hackers, in cooperation with drug cartels, invaded the computer system that monitors the movement of containers in the port

and removed a shipping container before it had been controlled by the port authorities. The case, of course, was not isolated, but when the investigative authorities managed to identify the crime, the investigative action contributed to seizing a record eight tonnes of cocaine with a street retail price of EUR 500 million which had been hidden in a container full of bananas from Ecuador.

This attack was carried out using the method of social engineering and a malicious program sent via email. While in this particular case the intrusion was detected and certain countermeasures were applied by the port authorities, they were unable to contain another intrusion where specific hardware (mini-computers hidden inside distribution power cords and external computer data storage) and recording components mounted on a computer keyboard were used.

4.2 Infection of Software Leads to a Complete Shutdown of Port Operations

At the end of June 2017, the Petya virus, which spread through the internet, affected computers in more than 65 countries. The Ukrainian computer virus quickly disrupted various computer systems and did not spare even the largest companies such as the Danish shipwright Maersk, which was crippled by the virus for a few days. Maersk's downturn of several days caused damages of approximately $300 million. Although Petya was not a blackmail virus, it caused enormous damage as it was intended to erase data and disable the operation of various systems.

4.3 Infection of System Software Causes Interference with Port Operations

System software designed to carry out port operations can be destroyed by a malware infection from the web which hacks into the most secured parts of computer memory, including its hardware, in the most cunning of ways. By taking full control of the system, it is possible to intercept all communications of its users over wired (Ethernet) and wireless networks (WiFi, UMTS, GPRS, Bluetooth etc.), and even carry out legally binding actions in their names, such as transfers of funds or entering into credit agreements through e-banking services or, last but not least, impeding port activities and even causing a work accident in the port.

5 Cyber Security Challenges

Based on various studies, it can be concluded that, in addition to physical damage insurance, the main challenges when trying to ensure the cyber security of ports are the following:

- Poor awareness and skills with regard to maritime information and cyber security,
- Lack of financial and other resources (e.g. cybersecurity experts) to ensure information security,
- The technical complexity of the port ecosystem,
- Finding the right balance between business efficiency and cyber security,
- The existence of outdated and vulnerable information systems,
- A lack of a regulatory framework for cybersecurity implementation,
- The interconnection of information technology (IT) and operational technology (OT),
- Security risks in the supply chain (lack of certificates, remote access of the supplier to the port, etc.),
- The heterogeneity of networks/systems,
- The involvement of all stakeholders in the provision of port cybersecurity,
- Cybersecurity does not keep pace with technological advances or developments and the emergence of new challenges related to the digital transformation of ports, etc.

6 Conclusion

We live in a time when the issue of security is an important part of our daily lives. The impact of the tools available to attackers for conducting cyber-attacks is not yet fully understood. This is why ensuring the protection or cybersecurity of maritime critical infrastructure is becoming one of the most important issues in national security and economic stability. Port security and the efficiency of their operations are crucial not only for maritime transport, but also for their strategic role in terms of security at the national, regional and European levels. This is especially true for Slovenia, which only has one maritime cargo port. The fact is that the operation and activities of ports are today becoming increasingly digitized and automated, and as a result more vulnerable to potential cyber threats. However, the consequences of the latter can be avoided or at least mitigated by adequately ensuring advanced security of the port infrastructure, establishing operational procedures, improving the resilience of computer networks/systems protection, increasing user awareness, and last but not least, considering security as part of the strategic management of a port.

7 References

1. Andritsos, F. (2013). *EU port security & growth***.** Proceedings of the 8th Future Security Research Conference, p 267-274 Fraunhofer. Retrieved March 02, 2020, from: http://publica.fraunhofer.de/documents/*H-47052.html, ISBN: 978-3-8396-0604-9*
2. Council of the EU (2018). *Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act")*. Brussels: Council of the EU.
3. *Directive of the European Parliament and of the Council on enhancing port security* (2005). Directive of the European Parliament and of the Council, № 2005/65/EC of 26 October 2005.
4. *Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community* (2002). Directive of the European Parliament and of the Council, № 2002/6/EC of 18 February 2002.
5. *Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC* (2010). Directive of the European Parliament and of the Council, № 2010/65/EU of 20 October 2010.
6. *Directive (EU) of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union* (2016). Directive of the European Parliament and of the Council, № 2016/1148 of 6 July 2016.
7. *Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (2008). EU Council Directive № 2008/114/EC of 8 December 2008.
8. *European Union Maritime Security Strategy* (2014). EU Council № 11205/4 of 24 Jun 2014.
9. *GPS disruption halts ports, endangers ships – US Coast Guard***,** Resilient Navigation and Timing Foundation. Retrieved February 10, 2015, from http://rntfnd.org/2015/02/11/gps-disruption-halts-portsendangers-ships -us-coast-guard/

10. International Maritime Organization (1995/2017). *International Safety Management (ISM) Code*. London: IMO.

11. International Maritime Organization (2017). *FAL Convention – convention on facilitation of International Maritime Traffic, 1965, as amended.* London: IMO.

12. International Maritime Organization (2017). *Guidance on Maritime Cyber Risk Management - MSC-FAL. 1/Circ. 3.* London: IMO.

13. International Maritime Organization (2002). *International Ship and Port Facility Security Code (ISPS)*. London: IMO.

14. International Maritime Organization (1974). *International Convention for the Safety of Life at Sea (SOLAS)*. London: IMO.

15. International Maritime Organization (2002). *International Ship and Port Facility Security Code (ISPS)*. London: IMO.

16. Kramek, J. (2013). *The critical infrastructure gap: U.S. port facilities and cyber vulnerabilities*. Federal Executive Series Policy Papers, Brookings Institution.

17. MORS (2019). *Kritična infrastruktura*. Retrieved March 01, 2020, from: http://mo.arhiv-spletisc.gov.si/ si/delovna_podrocja/kriticna_infrastruktura/

18. Orsosz, M., Chen, J., Maya, I., Salazar, D., Chatterjee, S., Wei, D. (2010). *Protecting our nation's ports with the port security risk analysis and resource allocation system (PortSec 3.0)*, Proceedings IEEE Conference on Technologies for Homeland Security (HST), pp 264-269.

19. Pasternack, A. (2013). *To Move Drugs, Traffickers Are Hacking Shipping Containers*. Motherboard tech by vice. Retrieved March 01, 2020: https://www.vice.com/en_us/article/ bmjgk8/ how-traffickers-hack-shipping-containers-to-move-drugs

20. Roberts, F. (2015). *The little-known challenge of maritime cyber security,* in IISA 2015 – 6th International Conference on Information, Intelligence, Systems and Applications [7388071]. Institute of Electrical and Electronics Engineers Inc.

21. *Uredba o evropski kritični infrastrukturi* (2011). Official Gazette of the Republic of Slovenia № 35/2011 of 13 May 2011.

22. *Regulation (EC) of the European Parliament and of the Council on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) № 3051/95*. Regulation of the European Parliament and of the Council № 336/2006 of 15 February 2006.

23. *Regulation (EU) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Regulation of the European Parliament and of the Council № 2016/679 of 27 April 2016.

24. *Regulation (EC) of the European Parliament and of the Council on enhancing ship and port facility security.* Regulation of the European Parliament and of the Council № 725/2004 of 31 March 2004.

25. *Zakon o kritični infrastrukturi* (2017). Official Gazette of the Republic of Slovenia № 75/2017 of 22 December 2017.

26. *West Coast Port Congestion Could Cost Retailers $36.9 Billion in the Next 24 Months.* Business Wire. Retrieved Feb. 7, 2015, from: http://www.businesswire.com/news/home/ 20150207005007/ en/ West-Coast-Port-Congestion-Cost-Retailers36.9#.VPiNIsbA7c8.

7 If the Face Fits: Is it Possible for Artificial Intelligence to Accurately Predict Threats to Protect Critical Infrastructure?

Graeme Ballard

1 Introduction

In 2002, Tom Cruise starred in a film called Minority Report. The film's central theme was that crime could be predicted by a group of "precogs[1]" and then stopped by law enforcement officers before it occurred. The ethics of both prosecuting and punishing criminals before they had committed a crime was also explored.

While individuals with psychic abilities predicting criminal activity is still very much in the realms of science fiction, this paper examines the question "Can artificial intelligence accurately predict threats to protect critical infrastructure"? The short answer is "yes" – my consortium has been working on this specific project for the last 18 months.

The method by which a machine can be programmed to achieve the identification of threats is far beyond the scope of this article. So, too, is the academic work, from both psychology and sociology, that is required to underpin such a programming. Instead, this paper discusses some of the principles of what is required to achieve a revolutionary, Minority Report-style tool, and the changes in attitude and business models that are required to achieve it. First, there will be a discussion of artificial intelligence and the need to integrate it into security. Second, we will look at how threats are currently predicted using biological cues and statistical analysis. Next follows a discussion on how to improve what we currently do – how to integrate cognitive and conative psychological theory as part of programming an AI, in order to accurately predict threats. The concluding section will consider how business models and our attitudes towards security must change in order for any AI to be successfully implemented in the energy sector.

[1] A fictional term for precognition, where an individual possesses the ability to see the future.

2 Artificial Versus Human Intelligence in the Energy Sector – Critical Infrastructure

2.1 Energy and Society

Economists such as Adam Smith, Karl Marx and Max Weber argued that the development of the nation state is, by definition, a place of conflict. For Weber, the Protestant Reformation in Western Europe produced a vigorous new type of person, whose focus was on work and prosperity – the driving force for the development of Capitalism. Smith and Marx argued that, within this capitalist system, power struggles develop between different classes of people, for example owners of capital and the proletariat; men and women; different races. Figurational sociology developed from these conflict theories. Figurational theorists view society as a whole, as a single playing field of power struggles that can never become fully legitimated or resolved (Dunning, 1999). Security is, therefore, important to the formation and welfare of the nation state, which becomes increasingly complicated as the forces of globalisation increase (Caleta, 2011). The significance of these arguments will be developed later.

Klaus Schwab (2017) argues that we are in the middle of a fourth Industrial Revolution (IR) that is changing the way we are living, working and relating to one another. While the exact number of Industrial Revolutions might be debated, the rapid technological and social innovations that have occurred since the development of the micro-chip have also been accompanied by rapid social upheaval and commensurate increases in threat (Caleta, 2011). Largely due to these technological innovations, modern societies are energy societies, incapable of functioning without access to ever-increasing demands for energy (Groselj, 2011). Furthermore, energy production and supply is, itself, becoming an increasingly complicated issue, thanks to the forces of globalisation (Groselj, 2011) and environmentalism.

Given the central importance of the energy sector to the functioning of modern society, prioritising the protection of that critical infrastructure seems logical. The nuclear industry, in particular, is an interesting case, due to its positive influence with regard to environmental issues (clean energy) and its potential (both real and imagined) for catastrophic impacts if something goes wrong (e.g. Chernobyl and Fukushima). Vrsec (2011) argues that humans (staff) are an important threat within the energy sector that should be included in any threat matrix. This is not simply due to any potential deliberate terrorist act, but also from the potential accidental consequences resulting from human error. The identification of various types of threat among staff in the nuclear industry will be used as exemplars in this paper.

2.2 Artificial Intelligence

True Artificial Intelligence does not (yet) exist. The fundamental problem is there is no single, clear definition of intelligence[2]! Whether in humans, animals or machines, the very concept of intelligence is the subject of much debate. Identifying and measuring it is, therefore, fraught with problems. For some, Artificial Intelligence is simply a branch of computer science that allows computers to make predictions and decisions to solve problems (AI for All, 2020).

2 See https://www.britannica.com/science/human-intelligence-psychology for an explanation of the 4 main theories of intelligence.

What can be said with certainty is that Artificial Intelligence machines are difference engines, capable of making specific types of mathematical calculations, at far higher speeds and volumes than the human brain is capable of doing. Due to relatively recent developments in microchip[3] technology, and with the creative use of standard Boolean algebra, various types of algorithm(s) and multivariate statistical analysis, machines capable of quickly performing large volumes of calculations can now be taught to do tasks that might look like intelligence and might include prediction. This is the essence of Machine Learning (ML) – a more correct term for the current, commonly applied misnomer Artificial Intelligence (AI). These are machines using programmed tools to teach themselves how to identify relationships and correlations, at speeds faster than a human being is able to achieve. It is not really intelligent; it just might look that way.

ML, therefore, is no different from any other kind of analysis – it is just more efficient. Whether from ML or traditional analysis, the results depend on the accuracy and creativity of the researcher/programmer, using the relevant mathematics and statistics to solve the particular problem at hand. In this way, the analysis is still subject to both statistical Type 1 and Type 2 errors, and researcher bias.

In other words, ML has the same potential to yield bad results and/or ever-increasing reams of meaningless data as traditional analysis. Recent examples include issues of accuracy and racism relating to facial recognition software, increasingly used by police forces (BBC, 2019); sexism relating to the human-resource ML deployed at Amazon (The Guardian, 2018); and the general trend towards vast volumes of meaningless data that has become the bane of modern organisations (Baker, 2014). Particularly worrisome is the potential for a machine to appear as if it has calculated a meaningful result but, in reality, it is an error that remains unrecognised by its human overlords. These issues will be developed further, towards the end of the paper.

In the nuclear industry, how can we teach a machine to understand something as irrational and unpredictable as human behaviour, in order to identify and predict potential threats? When faced with such a problem, it is often advantageous to return to first-principles thinking. If we wanted to identify threats from humans within the nuclear industry, how would we do it, using legacy tools?

3 Monitoring Stress with a Wrist Device

As a general rule of thumb, the psychological, sociological and philosophical literature all separate the basis of human behaviour into biological, cognitive and, sometimes, conative components (e.g. Engel et al., 1993; Franken, 1988; Kinnear and Taylor, 1991). The precise definitions and descriptions of these components (and the theories contained within them) is beyond the scope of this paper. What is relevant is that, up to this point in time, research within the security industry has focused mostly, it seems, on biological theories, because these are the easiest to reliably measure. Arousal, in particular, has yielded interesting results, and has been the basis of, for example, lie detector testing, since the mid 20th century.

3 NB The microchip is at its technological limit. Other, more efficient developments in the pipeline include biomorphic circuitry and, the more distant, quantum computing. Such developments might negate the necessity for Boolean algebra and even statistical analysis as we currently understand it. They will, undoubtedly, improve the speed and efficiency of calculations – looking ever-increasingly like intelligence – and make better predictions.

In 1908, Yerkes and Dodson presented the Yerkes-Dodson law of the empirical relationship between arousal and performance (Gjoreski et al., 2017). As shown in Figure 1, according to this law, a human being performs at a near-optimal level under a clearly defined level of stress (which is a useful proxy for arousal). Stress, therefore, is not necessarily a negative process, as is commonly believed, but is a necessary component of optimal performance.

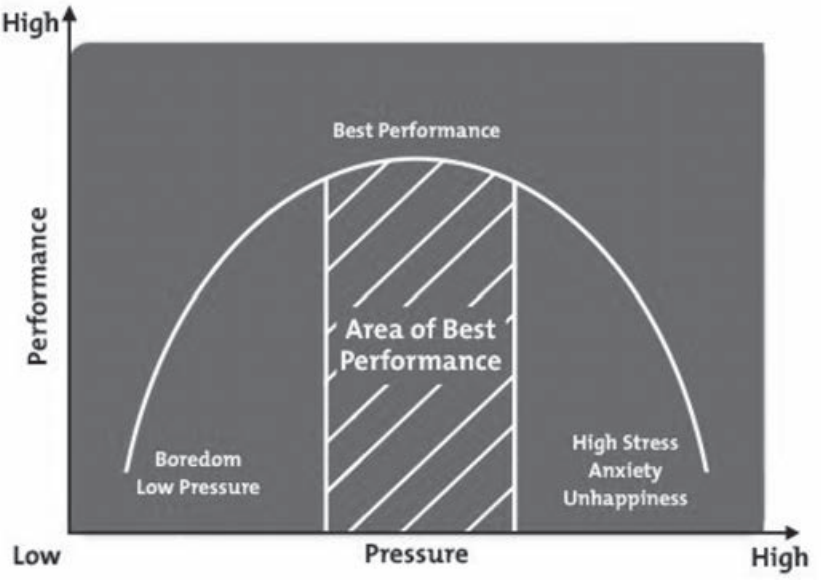


Figure 1: The Inverted U Relationship Between Arousal and Performance (Yerkes and Dodson, 1908).

Recent technological developments have made it possible to measure stress more effectively and less intrusively than ever before. As an example, the work of Gjoreski et al. (2017) made very good progress in this area. Using wearable biosensors, the authors developed a method to "accurately, continuously and unobtrusively, monitor psychological stress in real life" (Gjoreski et al., 2017: p 159).

The results were achieved using a quantitative methodology in both controlled lab conditions and natively in people's homes, and then statistically comparing the results. Using this method, Gjoreski et al. (2017) were able to accurately identify and measure unusual stress levels of people in their homes. They were able to achieve a 96% accuracy, 70% of the time, when contextual data was considered alongside the biological data from the devices. This is accurate enough for immediate and meaningful real-world use.

This protocol, developed by Gjoreski et al., could be used to effectively identify threats in the nuclear industry, if it were applied to staff. The potential threat, in this context, might not simply mean a terrorist event; it has the potential to contribute to identifying and understanding issues of lowered productivity[4] and addressing the well-publicised negative mental health consequences of chronic stress among employees. Issues of lowered productivity (or distraction), and negative mental wellbeing can make individuals more error-prone and, thus, represents a genuine threat within a nuclear facility, as discussed by Vrsec (2011). Of course,

4 Arousal to the same stimulus naturally reduces over time.

it still goes without saying that stress, presented at unusual times, could also be an indicator of an imminent threat in the form of terrorist or other illegal activity.

Whether or not contextual data is considered, Gjoreski et al. (2017) identified a number of weaknesses surrounding research on arousal and stress when using only biological variables.

- Stress, itself, is highly subjective.
- Due to this subjectivity, it is difficult to define the start, duration and intensity of stress.
- Accuracy of monitoring equipment – at the moment the results appear to be equipment-specific.
- Constrained environments – have to "calibrate" the equipment to filter "noise".
- Issue of subjective stress labelling in non-constrained environments.
- In order to explain and, perhaps, overcome these issues, it is important to understand arousal.

3.1 Arousal

There are a couple of important things to note about the nature of arousal. Arousal is not a simple, linear, process but is subject to two other factors: biological rhythms that are unique to the individual; and cognitive interpretation, which is also unique to the individual. In general, when arousal increases, performance increases as well; but this relationship does not continue indefinitely (Hebb, 1955) as seen in Figure 2. This is because human beings are not linear creatures.

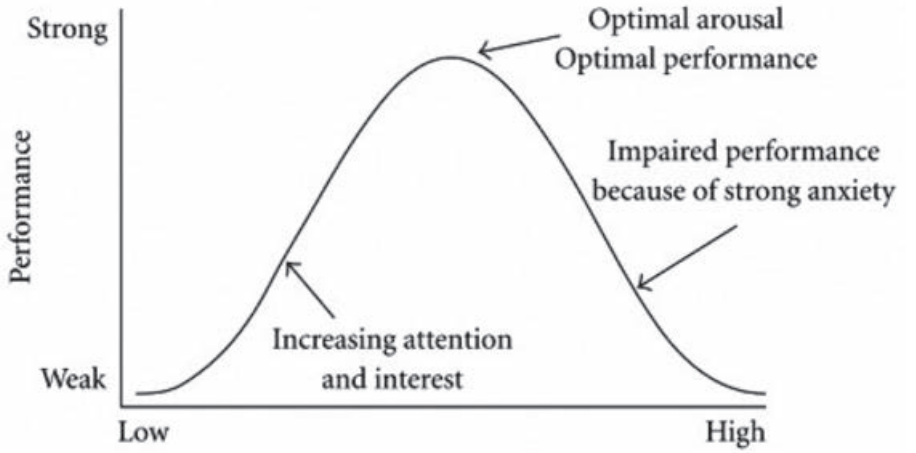


Figure 2: Arousal

3.2 Solomon's Opponent Process

Regardless of how and why an individual is aroused, whenever a person experiences an increase in positive affect – e.g. an emotional state or change in level of arousal – they are likely to experience an increase in negative affect afterwards. Conversely, when a negative affect is initially experienced, an individual will tend to experience a positive affect afterwards. This is because humans are designed in such a way that whenever affect departs from a baseline, an opponent process is triggered to return the person to that baseline, as seen in Figure 3, below.

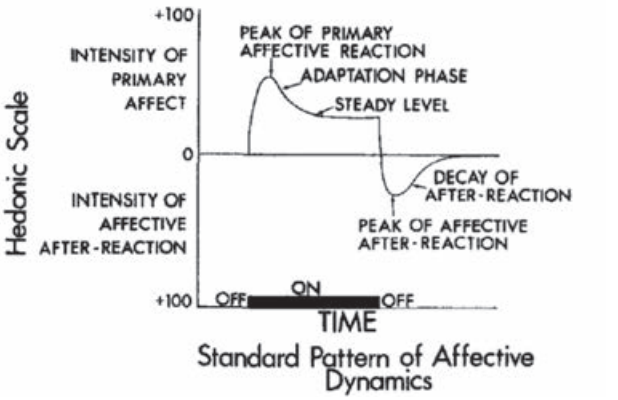


Figure 3: Standard Pattern of Affective Dynamics

Figure 3 illustrates "the standard pattern of affective dynamics, showing the five distinctive features; the Peak of the Primary Affective Reaction; the Adaption Phase; the Steady Level; the Peak of Affective After-Reaction; and finally the Decay of the After-Reaction. The heavy bar represents the time during which the affective arousing stimulus is present. The ordinate represents two hedonic scales, each departing from neutrality; one for the primary affective, the other for the affective after-reaction" (Solomon & Corbit, 1974: p120).

The opponent process is, however, rather sluggish and requires time to exert its full effect. When it does eventually exert full effect, it produces, for a time, the affective state opposite to the one that initially triggered it. Another feature is that the opponent process strengthens with use and weakens with non-use. This helps explain why, for example, with regard to drug use, a person taking a drug for a positive affect will tend to experience ever-increasing negative affects, eventually requiring the drug simply to stop the negative affect. The effect of this process, however, is not limited to drug use, but to all stimuli that create an affective response. The paradox, therefore, is that people who frequently engage in behaviours that initially produce elation and euphoria, will eventually experience more and more negative affect (Solomon & Corbit, 1974).

These issues can be addressed, somewhat, by developing the work of Yerkes and Dodson, Hebb (1955), and considering variables relating to personality, since personality innately influences levels of arousal (Eysenck, 1963, 1967). My consortium has considered such a form of enhanced personalisation as one of the keys to adding contextual value and, by doing so, improving Gjoreski et al.'s work. Enhanced personalisation in the form of consideration of personality could help ameliorate the effects of timing and intensity of stress, and help to better identify whether an individual's level of stress is unusual and/or might represent a health issue for that particular individual. Once again, this data could, probably, also be helpful in the accurate identification of threats from an unusual event, and/or threats from distraction.

A potential problem with this approach, however, is that the addition of personality variables into Gjoreski et al.'s work might not necessarily result in higher accuracy, in spite of the solid and well-tested relationship between personality and arousal. It could equally be the case that, by solely introducing personality variables, researchers might only add further complications to any study, consequently confusing and confounding the results of Gjoreski et al. Such a potential risk was one of the reasons why it was felt, among my consortium partners, that a more ambitious approach was more appropriate.

4 Cognitive Behaviour

Section 2.0 began with the statement that the psychological, sociological and philosophical literature all separate the basis of human behaviour into biological, cognitive and, sometimes, conative components Franken, 1988; Engel et al, 1993). In order to more appropriately (and ambitiously) develop Gjoreski et al.'s biological-based tool, discussed above, my consortium felt that the cognitive and conative components of behaviour should be actively considered – in order to be truly useful in protecting critical infrastructure. Although the exact nature of these concepts is beyond the scope of this article, a basic understanding of how they might operate together, to modify behaviour, is useful. The following example is a tested model from consumer behaviour, relating to the decision-making process regarding travel. Figure 4 shows how multiple psychological factors interact to process information to influence behaviour. A unique model(s) would need to be developed for nuclear power stations, but a suitable version has yet to be adequately identified by my consortium. This example is to illustrate a potential process – what a model might look like.

The components of attitudes (beliefs, feelings and predispositions) form the central portion of the model in Figure 4. Information about an attitude object is presented to the individual, which is processed to form an overall attitude about the object (in this case, travel to a particular destination). These include social factors, such as the attitudes of reference groups or the relative threat of the object to the individual's concept of self[5]. The attitude will then be combined, again, with social factors to form a preference or intention to travel to a certain destination or to use a particular form of transport. This preference, or intention, ultimately leads to behaviour, i.e. purchasing or making travel arrangements.

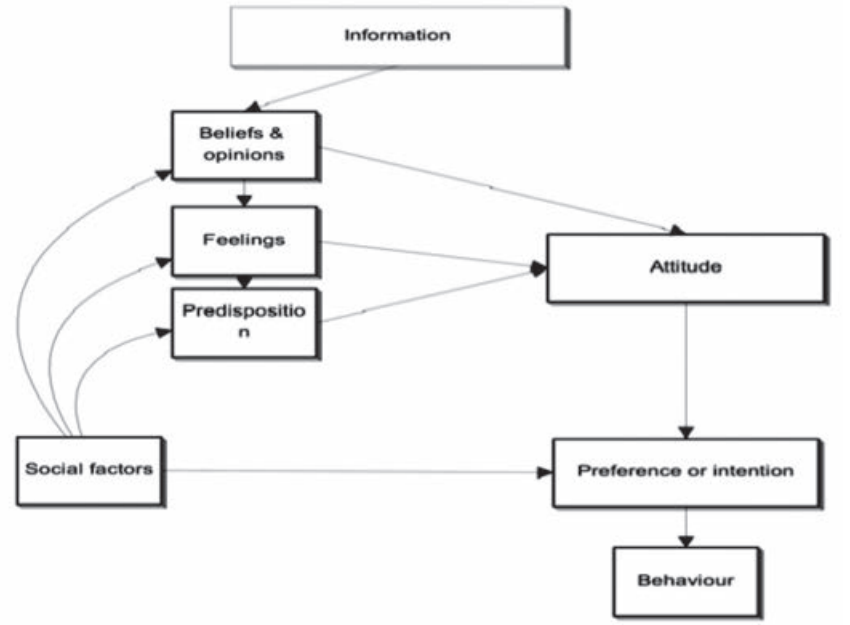


Figure 4: The components of attitudes (beliefs, feelings and predispositions) form the central portion of the model

5 NB It is not clear how much weight this influence has on each component, or on the overall attitude itself, and is likely highly individual in nature.

As is common with the consumer purchase decision-making process, the traveller will evaluate their decision after consumption, which then provides further information to the individual to be used in future potential travel evaluation situations.

Although a marketing example, the principles of decision-making – the integration of social, biological and psychological cues – will be the same for establishing threats within a work environment, such as nuclear power stations. From this example, one can see that, with considerable care and attention, it is relatively easy to programme a machine learning (ML) tool, using either an established psychometric model relating to stress (and/or deviance for that matter) or programming the ML after creating and testing a new, specific, stress-model, and then combine these cognitive results with the biological data. With ample time and budget, such an ML tool would, undoubtedly, result in a significant improvement on the work of Gjoreski et al. The problem with using this approach, however, was alluded to at the very beginning of this paper. The problem is that this approach is based on current assumptions in the psychology and sociology literature. The weakness is not in the theory (although the theory will not be perfect), but in the very fabric of the philosophical approach underpinning the scientific process itself.

4.1 The Inherent Weakness of Quantitative Methods – Methodological Issues When Researching Human Subjects

There are some very specific academic considerations when researching human subjects rather than inanimate objects. Research methods, especially the quantitative methods found in computer science, involve re-modelling a theory into a smaller manageable component (an analogy) and then making up variables with corresponding questions and limiting the answers, in the form of a scale. This allows the scientist/programmer to fit the variables, questions and answers to a scientific theory, in a methodological process termed functional unity (Fletcher, 1974). Statistical techniques are then used to measure how much these variables conform to, or deviate from, the given theory.

The aim of the quantitative researcher, therefore, is to gauge the truth of part of this analogy, rather than to examine the whole issue. Once this is achieved, the research results are published and re-tested by others in a process known as falsification (Hammersley, 1989). In this process, the theory is only rejected once it has been falsified a number of times and in different ways. This process represents a fundamental weakness in research methodologies relating to human subjects (Fletcher, 1974), and is an impediment to any research on human behaviour because the method cannot reflect the true character of the social world (Hammersley, 1989). Until the development of ML, however, it was the only methodology that could be employed in computer science.

The alternative, in the social sciences, is normally to engage in some form of qualitative research methodology, such as participant observation or ethnography (Hammersley, 1989), but this too, has its weaknesses – usually relating to overcoming researcher bias and the unverifiable accuracy of the results. Blumer (1989) and others argue, however, that qualitative methods, employing a process of symbolic interaction and recognising the fundamental idiosyncrasies of human interaction, yield results on human subjects that aid and enhance understanding, rather than simply identifying trends.

The meticulous and creative use of various types of algorithm, combined with multivariate statistical analysis, however, does yield the very real possibility of being able to replicate the

best results from both quantitative and qualitative methods in a ML tool, as long as certain well-established principles are maintained and applied.

4.2 (Much) Wider Contexts

Section 1.1 discussed the relevance of energy production and consumption to the formation and security of the modern nation state, and the inherent conflict therein. It is inevitable that these conflicts and power struggles must be approached and reflected in the analysis, if ML is to be used effectively as a revolutionary, predictive tool. This means we must not only consider the models within the scientific literature – in this case, psychology – but also explore the links between the disciplines themselves: biology, psychology, sociology, and the very history of human beings, as per the Figurational approach (Dunning, 1999). The mechanisms used by the different groups in society for obtaining power, as well as the power conflict itself, are subject to constant change, which affect the outcome of power struggles in society and are relevant in the analysis of threat. Power, in this sense, becomes a social process in and of itself (Dunning, 1999) which can be treated very much like a process within psychological theory, such as arousal.

The implications of this, however, are more complicated than it might at first seem, because it means we must also account for the way we view and understand the world scientifically (Dunning, 1999). It can be argued that scientific facts, as we commonly know and understand them, are actually part of the social process of power management. The hypothetico-deductive reasoning behind science and the scientific facts that emerge, can themselves become viewed as a power-management tool (whether deliberately, accidentally, or incidentally). Such power management might not be a deliberate act, but an unintended consequence of the process of functional unity and falsification required of the quantitative method.

In practical terms, this is one of the explanations of why threat, in and of itself, might be defined differently between countries or regions (e.g. differences in the way health is defined). Furthermore, within regions and countries, what is defined as a threat will change over time (e.g. what constitutes a terrorist threat), and these same societies might temporarily modify or suspend what is viewed as a threat in certain situations (e.g. policy and behaviour in the face of the Covid-19 threat).

Once this idea has been accepted, then it is possible to analyse and critique certain values and beliefs that quietly permeate the whole of society, usually without much thought. For example, there are widely held beliefs that women do not commit sex-offences (Gillespie et al., 2015) and that athletes using drugs are cheats and morally inferior (Van Raalte et al., 1993). These assumptions might not seem unreasonable until it is considered how, when taken as a whole, they genuinely effect the integrity of research, the legal system and the rehabilitation protocols relating to female (and, possibly, male) sex offenders (Williams et al., 2019), or the integrity and success of drug-testing programmes[6] and the potential negative health consequences, related to drug testing itself, in the world of sport (Ballard, 1999). Bad data input always equals bad data output – whether using legacy or ML analytical tools.

Ensuring that only good data is used and maintained in a ML tool will be far more important than it has ever been before, due to the leap in efficiency inherent in ML. This efficiency

6 Although I'm specifically speaking about the sports context here, the definition of success in any drug testing programme, whether workplace or criminal justice system, is highly debatable.

is a double edged sword because any error in the technology will have negative real-world consequences that will emerge far faster, and be far more wide-reaching, than anything legacy analysis could achieve[7]. This is because, in a legacy world of relatively slow scientific analysis, debate and falsification is a slow process, which gives people (both powerful and not) time to adjust to developments and change. This will not be the case with a ML tool. Analysis will be swift and debated only within the machine. It is vitally important, therefore, to ensure ML uses "good" data by considering ALL aspects of "threat", however it might be defined, over time and across geographical and social boundaries. In doing this, the ML will not only be more accurately and reliably utilised to identify threat, but it is more likely that the machine judgement of threat will be trusted by all stakeholders, namely government(s), people with economic self-interest, and the population at large.

In this sense, trust in the accuracy, legitimacy and fairness (whatever this is) resulting from ML is the most important factor in assessing whether or not the execution of an ML tool is a success that adds value to society. Significant changes and developments in business models and the attitudes of governments and others in positions of power (and society at large) are likely to be required in order for ML tools to be trusted enough to be effectively deployed.

5 Changes Required for the Successful Implementation of ML to Identify Threat

Given everything that has been discussed in this paper, there are a number of changes that need to occur for ML to be successfully or, more correctly, meaningfully deployed.

5.1 The Assumptions when Programming ML

When researching human subjects, it is vital to consider the human idiosyncrasies noted by Blumer (1989), along with the (much) wider contexts in which all behaviour occurs – including scientific analysis itself. Three fundamental assumptions must be at the core of ML programming – the same assumptions for researching all human subjects (e.g. Denzin, 1989; Blumer, 1989; Dunning, 1999):

- Reality is a social product.
- Humans can guide their own futures and that of others.
- Humans are social beings; they must interact with each other, and gain meaning and insight in so doing.

Such assumptions can no longer be considered merely as academic niceties, of no value in the real world. When dealing with ML, such considerations are the new real world.

5.2 Attitudes Towards Data, Privacy and Security

In the new real world, attitudes towards data, privacy and security must, probably and necessarily, change – not only as a necessity for programming the ML, but as a result of its

7 As an example of what could happen, I cite current attempts to shoe-horn legacy business models and approaches into social media technology. The superior new technology creates negative outcomes in models that used to work well with legacy technology.

implementation. Change has always been a continuous process but, after engaging ML, the process of change will occur at a faster pace. Political and economic systems must adapt to this – preferably proactively rather than reactively[8]. As I hope will be clear from the discussion so far, the relationship between ML and human processes will be symbiotic – each will influence the other. Under these conditions, the ML tool itself must be considered as highly active and will need to be constantly modified, curated and updated in order to remain relevant and accurate – not just technologically, but also in terms of data management and its continued ability to identify threats in a world that is constantly changing.

By definition, therefore, data-sharing is a necessity that will make a positive contribution to the identification of threats and those tasked with maintaining security. It must become the norm – both in attitude and in practice. The more frictionless movement of data that can be achieved, the more accurate and trusted any ML tool will be. Data must be acquired and moved from as varied and wide a source(s) as possible. This will mean not only sharing data between nuclear power plants within the same company, but data between competing companies; perhaps also with different industries and, almost certainly, across geographical and political boundaries.

In order to facilitate such frictionless data-sharing, it is imperative that changes to both legal and commercial practices must be found. This will likely require a shift in the psychological attitude of both our politicians and our business leaders, and also significant (and potentially disruptive) changes to business models, accounting practices and the security services themselves. This must all be achieved without itself creating a security risk, and achieved within the law, ensuring that what Lepine (2014) describes as the social contract remains intact.

6 Conclusion

The use of ML to identify threats to protect critical infrastructure within the energy sector is a tantalising prospect and a project that my consortium partners have been actively undertaking for the last 18 months. There is little question that the correct and careful implementation of such a technology will add value to the security of nuclear (or other) energy production. The ultimate success of any implementation, however, is dependent on six factors:

- Finding good consortium partners who truly understand the idiosyncrasies and complications of researching human subjects.
- Finding the appropriate amount of funding to be able to account for the idiosyncrasies and complications of researching human subjects.
- If points one and two can be addressed, the next factor of success is the gathering of good data and ensuring certain methodological issues are addressed when designing the tool. These human methodological issues are no longer mere academic niceties, but are essential to the accurate and meaningful implementation of the technology.
- Trust in the technology. The technology must be human-centric. It must add value in the widest possible terms. For example, ML has the potential to not merely identify threats in terms of preventing catastrophe, it has a role to play in human resource management, ensuring the wellbeing of workers in terms of their physical and psychological health. These factors should be considered not simply because of their relevance in preventing a disaster, but in wider acceptance of the results from the tool.

8 Once more, the lessons from social media v legacy media should be learned.

- Attitudes towards data, privacy and security must change; not merely to make ML work, but also to help engender trust, minimise the potential disruption caused by the results of the technology, and ensure the technology continues to grow and adapt to an ever-changing environment.
- Prioritising worker health and achieving frictionless data-sharing could be disruptive in the short term. Attitudes of governments and business leaders must be proactively managed in order to facilitate the necessary adaptations in business models required to achieve these potential benefits with minimal disruption.

7 References

1. AI for All (2020) from http://ai-4-all.org/about/what-is-ai/
2. Baker, P. (2014). Why Big Data Hasn't Reinvented Advertising…Yet. FierceBigData.com.
3. Ballard, G. S. D. (1999). Pump Fiction: How Elite New Zealand Bodybuilders View The Anabolic Steroid Debate. The Journal of Performance Enhancing Drugs, 2 (4), 21-25.
4. BBC (2019). Facial Recognition Fails on Race, Government Study Says. From https://www.bbc.co.uk/news/technology-50865437
5. Blumer, H. (1989). Society and Symbolic Interaction. In Hammersley, M., The Dilemma of the Qualitative Method. London: Routledge.
6. Caleta, D. (2011). A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership. In D. Caleta, P. Shemella (Eds.), Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection. Ljubljana, Slovenia: Institute of Corporative Security Studies, and Monterey, USA: Center for Civil-Military Relations.
7. Denzin, N. K. (1989). The Research Act: A Theoretical Introduction to Sociological Methods. Englewood Cliffs, N.J.: Prentice Hall.
8. Dunning, E. (1999). Sport Matters: Sociological Studies of Sport, Violence and Civilisation. London: Routledge.
9. Engel, J.F., Blackwell, R.D., Miniard, P.W. (1993). Consumer Behaviour (7th ed). Fort Worth: The Dryden Press.
10. Eysenck, H.J. (1963). Personality and Drug Effects. In R.E. Franken (1988). Human Motivation. California: Brooks/Cole publishing.
11. Eysenck, H.J. (1967). The Biological Basis of Personality, in R.E. Franken (1988). Human Motivation. California: Brooks/Cole publishing.
12. Franken, R.E. (1988). Human Motivation. California: Brooks/Cole publishing.
13. Fletcher, C. (1974). Beneath the Surface: An Account of Three Styles of Sociological Research. London: Routledge and Keegan Paul.
14. Gillespie, S. M., Williams, R., Elliott, I. A., Eldridge, H. J., Ashfield, S., Beech, R. (2015). Characteristics of Females Who Sexually Offend: A Comparison of Solo and Co-Offenders. Sexual Abuse, 27 (3), 284-301.
15. Gjoreski, M., Lustrek, M., Gams, M., Gjoteski, H. (2017): Monitoring Stress with a Wrist Device Using Context. Journal of Biomedical Infomatics. Vol 17, 159-170.

16. Groselj, K. (2011). Critical Infrastructure Protection and the Energy Sector. In D. Caleta, P. Shemella (Eds.), Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection. Ljubljana, Slovenia: Institute of Corporative Security Studies, and Monterey, USA: Center for Civil-Military Relations.

17. Hammersley, M. (1989). The Dilemma of the Qualitative Method. London: Routledge

18. Hebb, D.O. (1955). Drive and the CNS (conceptual nervous system) in R.E. Franken (1988), Human Motivation. California: Brooks/Cole publishing.

19. Kinnear, T.C., Taylor, J.R. (1991). Marketing Research: An Applied Approach. (4th Ed). New York: McGraw-Hill inc.

20. Lepine, P. (2014). Intelligence Gathering in Democracies: Breaking the Social Contract? In D. Caleta, P. Shemella (Eds.), Intelligence and Combating Terrorism: New Paradigm and Future Challenges. Ljubljana, Slovenia: Institute of Corporative Security Studies, and Monterey, USA: Center for Civil-Military Relations, Naval Post-Graduate School.

21. Mayo, E., Jarvis, L. (1981). The Psychology of Leisure Travel. Boston: CBI Publishing.

22. Schwab, K. (2016). The Fourth Industrial Revolution. Geneva: World Economic Forum.

23. Solomon, R.L., Corbit, J.D. (1974). An Opponent Process Theory of Motivation: Temporal Dynamics of Affect. Psychological Review, 81 (2), 119-145.

24. The Guardian (2018). Amazon Ditched AI Recruiting Tool that Favoured Men for Technical Jobs. From https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine

25. Van Raalte, J.L., Cusimano, K.A., Brewer, B.W. (1993). Perceptions of Anabolic Steroid Users. Journal of Applied Social Psychology, 15 (23), 1214-1225.

26. Vrsec, M. (2011). Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) Infrastructure for the Functioning of a State, Economy and Civil Society. In D. Caleta, P. Shemella (Eds.), Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection. Ljubljana, Slovenia: Institute of Corporative Security Studies, and Monterey, USA: Center for Civil-Military Relations.

27. Williams, R., Gillespie, S. M., Elliott, I. A., Eldreidge, H. J. (2019). Characteristics of Female Solo and Female Co-Offenders and Male Solo Sexual Offenders Against Children. Sexual Abuse, 3 (2), 151-172.

Acknowledgement:
I would like to thank my business partner, Bozidar Zaloznik, for his assistance in the content work in this conference paper.

Index

D

E

F

G

H

I

S

T

U

V

W

X

Y

Z

Summary of Contents

Section I: Extremism, Radicalization and Cyber Threats as an Important Security Factors for Countering Terrorism Processes

Re-assessing Online Jihadi Extremism: Reasoning for a Marketing Approach to Counter-Radicalization

Paul Lieber

While there is increased recognition of the potency of online communication for the proliferation of jihadi violent extremism across Europe, existing approaches are falling woefully short. Specifically, these approaches are wedded to particular paradigms and assessments that inherently favour data organization over audience understanding. As a result, the vast majority of resources expended towards addressing European jihadi violent extremism see increased spending, but little impact. This chapter details the strengths and weaknesses of current approaches, while offering three alternatives to reasoning about this problem, nested in marketing research.

Extremism and Radicalization in the European Environment – Security Challenges of Return Foreign Fighters

Denis Čaleta, Sara Perković

This analysis will consider whether foreign fighters pose a real danger to European security, knowing that the potential threat is always possible. The threat posed by returning foreign fighters should not be underestimated. Terrorist attacks carried out by returning foreign fighters in different European countries are proof of that. We have researched the attacks that have been carried out by returning foreign fighters, and in this chapter we try to analyse the challenges that European security policymakers face in order to deal with extremism and the radicalism processes connected to returning foreign fighters. We consider how Germany,

Bosnia and Herzegovina, and Kosovo are dealing with the return of foreign fighters and what measures have they taken; are they more focused on a restricted legislation approach, or is their focus on de-radicalization and reintegration programmes?

Russian Cyber Operations: The Relationship between the State and Cybercriminals

Mark Grzegorzewski

In the age of Great Power Competition, the United States needs to better understand all of Russia's capabilities. The Russian state is a master of covert and clandestine operations, especially in cyberspace, so the United States needs to be able to understand all the ways in which the Russian state employs its cyber capabilities. This paper uses Tim Maurer's "cyber mercenary" thesis as a jumping-off point to argue that there is in fact a fourth typology that we need to understand, which is labelled "commensalism". Only after understanding this fourth typology can we see that the Russian state has broken down the artificial wall between crime and national security to engage in a hybrid war against the United States..

Radicalization as a Cause of Terrorism – The Case of Bosnia and Herzegovina

Mile Šikman

In the most general sense, radicalization is regarded as one of the causes of terrorism. However, in order to accept this view, several prerequisites must be met. First, radicalization must be understood as a process of adopting a view that violence is a justifiable way of achieving goals. In this sense, terrorist radicalization is discussed and distinguished from other forms of radicalization. Secondly, radicalization must be aimed at achieving the goals of a terrorist organization, including terrorist-related behaviours (recruitment for terrorism purposes, terrorist training, and so on). Thirdly, in accordance with the multifactorial approach to explaining every crime, including terrorism, other factors (individual and external) leading to the behaviour referred to as terrorism should also be taken into account. This paper applies the theoretical concept of radicalization to practical cases of terrorism in Bosnia and Herzegovina (BiH). The aim of this paper is to examine the extent to which terrorist radicalization has contributed to terrorism in BiH, including BiH citizens who have left for Syria and Iraq to join the Islamic State terrorist group.

Addressing Challenges from Cyber Terrorism in Kosovo

Kadri Arifi

Global interdependence; rapid technological, industrial, scientific and transport development; free movement of people, services and goods; new opportunities in cyberspace throughout the world and the use of these opportunities by terrorist groups have given a more serious and challenging dimension to threats of terrorism. Countries with better developed economies and more modern industrial capacities are more likely to be exposed to cyberattacks or terrorist acts. However, the same can also apply to less developed countries, because the use of the internet there has increased in critical infrastructure sectors such as energy, water, health, transport and communication. These systems improve the quality and speed of the services provided, thereby helping organizations to work more productively and contributing in an improvement in living standards. Nevertheless, in the absence of cybersecurity they are also exposed to various risks, which lie in the inevitable ICT violation and can cause service shortages or even abuse of these services, causing potential damage (loss) to human life, economic loss to a great extent, collapse of public order, terrorist acts and threats to national security.
The efforts of Kosovo's institutions in the fight against violent extremism and terrorism have increased significantly and consistently. As a result of all the measures taken by the Kosovo institutions, both in terms of prevention and in strengthening international cooperation, as well as criminal prosecution, the threats of violent extremism and terrorism have been significantly reduced. However, the phenomenon of extremism and terrorism remains an ongoing challenge for Kosovo's security institutions. Considering that currently the spread of radical and extremist ideologies is almost entirely focused on the internet and social networks, there is an imposed need to strengthen cyber security and the capacity to protect critical infrastructure from cyber terrorism. In this respect, the lack of a strategy and mechanisms for cyber defence can be seen as one of the major challenges to Kosovo's efforts to combat cyber terrorism.

Section II: Cyber Terrorism and Security Implication for Critical Infrastructure Protection

Hyper Threats to Critical Infrastructures in the Region of South-Eastern Europe: A Wake-up Call for South-Eastern European Leadership

Metodi Hadji-Janev

The contemporary security reality is complex and unpredictable. Thanks to technological development, intensified globalization and a major shift in international politics, state and non-state actors are able to pose asymmetric, cyber and hybrid-based threats to South-Eastern European democracies. The ongoing artificial intelligence competition at the global level is expected to give new momentum to the geopolitical and security context. The ability of these systems to collect and process mega-data in almost no time and execute functions beyond human capacities' limitation in the security context elevates asymmetric, cyber and hybrid-based threats to a whole new "hyper threat" level. These threats are real and will profoundly change, among other things, the approach to critical infrastructure protection/critical information infrastructure protection. Therefore, the South-Eastern European leadership needs to seriously consider and confront the hyper based threats that are just around the corner.

Cyberterrorism Threats to Critical Infrastructure: Coordination and Cooperation from Brussels to South-Eastern Europe and back

Robert Mikac, Krešimir Mamić, Iva Žutić

This paper analyzes the response towards cyberterrorism threats to critical infrastructure. To this goal, the paper examines a strategic and normative framework for the protection of critical infrastructure at the European Union level and in the Republic of Croatia, as a representative country of South-Eastern Europe, as well as their operational level of implementation of critical infrastructure protection. As some cyber threats are indistinguishable from each other, the paper gives an overview of cyber threats to critical infrastructure, and explores the threat of cyberterrorism to critical infrastructure in the EU and the Republic of Croatia. The paper focuses on inspecting public policies and measures taken by the EU and the Republic of Croatia to protect critical infrastructure from cyberterrorism at both levels (EU and Croatia), and their implementation. The paper analyzes how much these public policies are operationalized in practice, providing recommendations with regard to stronger cooperation and coordination in the region.

A Critical Infrastructure Protection Perspective on Counter-Terrorism in South-Eastern Europe

Alexandru Georgescu, Adrian Victor Vevera, Carmen Elena Cîrnu

This article argues that counter-terrorism policy makers in South-Eastern Europe and especially the Western Balkans, should pursue a Critical Infrastructure Protection perspective as being useful in a number of ways. It provides a way to map societal weak points that could be exploited, a ready-made toolbox to address vulnerabilities, mechanisms for international cooperation, and best practices to be transferred and assimilated. It is also an inherently useful roadmap for the allocation of scarce security resources to increase resilience to terrorist activities. At the same time, the EU Member States in South-Eastern Europe already feature National Critical Infrastructure Protection Programmes and inclusion in the European Programme, which could prove to be a useful starting point to work with the non-EU countries in the region, including through the transfer of experience and best practice. This article also presents a series of proposals which may improve the security situation in the Western Balkans with regard to vulnerability to terrorist activity and intent.

Historical and Legal Aspects of Cyber Attacks on Critical Infrastructure

Andrej Iliev, Ferdinand Odzakov

The development of cyber attacks follows three major historical periods: first follows the technological advances of information technology during the 1980's until the end of the Cold War in 1990, second is from the end of the Cold War to the terrorist attacks in United States 2001 and the third is onwards. Each historical period followed a specific doctrine and strategy of dealing with national security threats from cyberspace. The world's super-powers and states, introduced appropriate strategies and national policies to deal with the consequences of this type of warfare.

The term "cyberspace" and "cyber attack" were first presented from American author William Gibson in 1982. In the following years, this word turned out to be conspicuously related to online PC systems. According to NATO, people are part of cyberspace. NATO defines that cyberspace is more than just the internet, and includes not only hardware, software and information systems, but also peoples and their social interaction on these networks. The first cyber warfare weapon was Stuxnet, whose objective was to physically annihilate a military target. Stuxnet contaminated more than 60,000 PCs around the world, mostly in Iran.

While international cooperation is essential, in the near future each nation should develop its own national foundation, national cyber security strategy, authorities and capabilities. Every nation state should require effective coordination and cooperation between governmental entities at the national and sub-national levels, as well as in the private sector and civil society. The main focus of this paper is to present the historical development of cyber attacks on critical infrastructure, and accordingly to propose best legal concepts, doctrines and strategies for dealing with cyber attacks on critical infrastructure.

Cyber Threats to Maritime Critical Infrastructure

Andrej Androjna, Elen Twrdy

The increasing speed of the development of information and communication technologies (ICT) and the constant connection to the internet bring new cyber threats, thus increasing the chances of cyber-attacks targeting maritime critical infrastructure. In terms of improving the efficiency of port operations, their vulnerability (e.g. consequences in the event of a system failure) is increasing with the interconnection and integration of many maritime and logistics systems. The impact of the tools available to attackers for cyber-attacks are not yet fully understood. This is precisely why the protection, or cyber security, of maritime critical infrastructure is becoming one of the major issues of national security and economic stability. Port security and the efficiency of port operations are crucial not only for maritime transport but also for their strategic role in terms of security at the national, regional and European level. This article presents new challenges, threats and strategies in overcoming barriers in the context of ensuring the cyber security of maritime critical infrastructure.

If the Face Fits: Is it Possible for Artificial Intelligence to Accurately Predict Threats to Protect Critical Infrastructure?

Graeme Ballard

Artificial Intelligence, or more correctly, machine learning, can potentially be used to identify and predict threats in order to protect critical infrastructure. Building on previous work, which only included the biological components of behavior, this paper describes how a machine learning tool could potentially be programmed using biological, cognitive and conative components of behavior. The relevance and importance of the unique issues surrounding the research and understanding of human subjects is discussed, along with how these issues will need to be actively considered and overcome if a successful machine learning tool is to be successfully achieved, and its judgments accepted, by stake-holder groups and the public at large.

Biographical Notes about Editors and Contributors

Editors

Denis Čaleta[1] holds Ph. D. from Faculty of state and European studies, Slovenia in 2007. He is associate professor at Faculty of state and European studies and Faculty of Entrepreneurship/GEA College where he's a Head of Department for Management of Corporate Security. He is also President of the Board in Institute for Corporative security studies (ICS), a Head of the resource group in the ICS and President of Slovenian Association for Corporative Security. He's author of many scientific articles and books related to Critical Infrastructure Protection, Counter Terrorism and other security issues. He has participated as an active participant in more than 80 international and national conferences and research projects.

He is also President of the Slovenian Association of Corporate Security and currently serves as the Chairman of the international association "SE Europe Corporate Security Association" (SECSA).

He worked as a Slovenian representative in the framework of NATO in the field of intelligence standardization matters in "Joint Intelligence Working Group at the period 2002-2008. He served as an Adviser for Counter Terrorism to the CHOD of Slovenian Armed Forces at the period 2002-2010. He was also member of the Government Coordination Group to coordinate the preparations for critical infrastructure protection for more than 10 years and was representative of the Slovenian Armed Forces in the working body for transnational threats inside the National Security Council (NSC) primarily concern for Counter terrorism activities. He is national representative in EU RANNET (Radicalization Awareness Network).

He still works for Slovenian Armed Forces as a Military Specialist XIV. Class (OF5).

[1] Editor of this monograph is also co-author of chapter in this book. As he is presented in a section About the Editors they do not reappear in About the Authors section.

James F. Powers Jr. currently serves as a Senior Fellow for the US Special Operations Command's *Joint Special Operations University*, located on MacDill Air Force Base, Tampa, Florida. His specific research/teaching areas include, *inter alia*, analyzing & defining violent extremism & terrorism; root causes of discontent; combating terrorism; countering violent extremism; information & intelligence-sharing challenges; the protections, responsibilities and challenges of sovereignty; identification & protection of critical infrastructure; inter-ministerial collaboration & cooperation challenges; national strategic appraisal and strategy development; civil-military operations; critical thinking; legal aspects associated with combating violent extremism; leveraging alliances & coalitions to combat transnational criminal organizations; and homeland security-related topics. As a Senior Fellow, Powers' duties currently include supporting USSOCOM Capstone doctrine and strategic initiatives, strategic objectives, programs and outreach activities through research and analysis, subject matter expertise, exercise support, symposia orchestration & participation and other adult learning methods. In support of the Department of Defense's *Combating Terrorism & Irregular Warfare Fellowship Program*, Powers serves as a seminar facilitator in both CONUS and OCONUS for both US and foreign special operations forces, law enforcement, intelligence and other ministry officials.

Authors

Andrej Androjna, PhD. has been involved in maritime security-related issues for three decades. As a Navy Commander, he has served in various positions and held functions of Staff and Command in Slovenia, abroad and on operations. He is now Head of the Maritime Studies Department at the Faculty of Maritime Studies and Transport, University of Ljubljana.

He has worked across diplomatic, strategic, operational and tactical levels in NATO (Supreme Headquarters Allied Powers Europe (SHAPE), NATO Headquarters Northwood, NATO Headquarters Skopje, KFOR, ISAF) and the EU, where he was thoroughly involved in NATO defense policy issues and the EU Common Security and Defense Policy (CSDP).

His published research covers international and domestic maritime policy and maritime security and safety, while his principal fields of interest include safety of navigation, safety at sea, human resource management, bridge team management and maritime cyber security.

Kadri Arifi, Colonel, PhD, Department of Personnel and Administration, Kosovo Police MHQ. During his professional career he worked in numerous fields of police works- Public Security, Road traffic Police, Criminal Intelligence, Organized Crime and corruption, Counterterrorism and Countering Drug and Human Been Trafficking. He is former Head of Crime Department, Kosovo Police. He attended different training programs in Europe and USA and participated in many international seminars and conferences regarding security issues, terrorism, organized crime, anticorruption and emergency management.

Kadri Arifi holds a PHD in Public Law. He is a lecturer at University AAB in Pristina and he is serving as project advisor to the Association of Women Police of Kosovo (AWKP).

Graeme Ballard is founder and CEO of Devolution Media Group of companies (2003-present). He was also actor, dancer, producer credits (1999-2006). Psychologist and Behaviour Support Worker at Specialist Education Services (1999-2000).

He is Assistant Lecturer and joint developer of New Zealand's first real-time, interactive, distance learning web site at Lincoln University (1996-1998).

Referenced publication he want to point out is: Ballard, G.S.D.B. (1998). Pump Fiction: How Elite New Zealand Bodybuilders View the Anabolic Steroid Debate. *International Journal of Performance Enhancing Drugs, 1999, 2 (4), 21-25.*

Carmen Elena Cîrnu, is Scientific Researcher II, Head of the Cyber Security and Critical Infrastructure R&D Department and Vice President of the Scientific Council at the National Institute for Research and Development in Informatics – ICI Bucharest, where she is involved in the development of research and development projects in the field of cybersecurity, cyber diplomacy, critical infrastructure protection and the interoperability of e-government systems. She graduated from the University of Bucharest in 2003, and obtained her PhD in 2011. An Aspen Institute Fellow and former Guest Researcher at the Global Security Research Institute Japan, she has held various roles in the field of research management, as well as at senior advisory level collaborating with universities and central public administration institutions over the years. She is the author or co-author of numerous articles, books, studies, and research reports, and project manager for a significant number of national and international research projects in the field.

Alexandru Georgescu, is an Expert with the Department for Cybersecurity and Critical Infrastructure Protection of the National Institute for Research and Development in Informatics. He studied Economics, then Geopolitics, and has obtained a PhD in Risk Engineering for Critical Infrastructure Systems. He is actively involved in advancing Critical Infrastructure Protection and Resilience issues through cooperation at the international level, and has worked on international projects for the European Space Agency, among others. He is currently a moderator for the Critical Energy Infrastructure Protection Working Group of the European Defence Agency's Consultation Forum on Sustainable Energy in the Defence and Security Sectors. He was a Visiting Fellow with the Shanghai Institutes for International Studies. He is also affiliated to the European Centre for Excellence for Blockchain, with the Romanian Association for Space Technology and Industry, the EURISC Foundation and Eurodefense. He has turned his PhD thesis into a book on Critical Space Infrastructures – Risk, Resilience and Complexity, published by Springer in 2019.

Mark Grzegorzewski, PhD. is a Resident Senior Fellow in the Department of Strategic Studies at Joint Special Operations University where he is currently focused on cyberspace operations and artificial intelligence. He has a recent article in *The Special Operations Journal* on "Demystifying Artificial Intelligence through DoD Education," and has a chapter titled "Why Silicon Valley is a Poorly Suited Model for SOF" in the upcoming *JSOU Press* "Big Data for Generals" monograph. Dr. Grzegorzewski holds a Ph.D., M.A., and B.A. in Political Science from the University of South Florida, along with a graduate certificate in Globalization Studies.

Metodi Hadji-Janev, Brigadier General, (Ph.D.) is a TRADOC commander in the Armed forces of the Republic of North Macedonia. He is an associate professor at the Military Academy "General Mihailo Apostolski"-Skopje, a unit of University "Goce Delcev" in Stip, Macedonia, and an Adjunct Faculty Member at Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S.A. D-r Hadji-Janev's current scholarship focuses on legal aspects of countering asymmetric, cyber, and hybrid-based threats, with emphasis on critical information infrastructure and critical infrastructure protection.

Andrej Iliev, PhD is born in 1978 in Belgrade, Republic of Serbia. He finished military academy in Republic of North Macedonia in 2001. In 2005 he finished his MA studies and in 2009 his PhD studies in area of modern international military history. He is lieutenant colonel and associate professor in Department of social science in Military academy "Gen. Mihailo Apostolski" in Skopje.

D-Dr Andrej Iliev holds several subjects in I, II and III cycles of studies in Military academy such as: Military history, Evolution of warfare, Modern warfare, Systems for collective security and defense, Globalization and security, NBC protection and other subjects dedicated to his area of research. He has published 6 books and more than a 75 articles in international conferences and journals. Some of the journals are registered in international scientific bases: EBSCO and Scopus. He took a part in several international projects such NATO SPS and RADLI with Jefferson institute.

Paul Lieber, PhD. is COLSA Corporation's Chief Scientist (Data & Social Science), where he specializes in communication influence. A Board Member of the Information Professionals Association, he previously served as the Command Writer for two USSOCOM Commanders, likewise Strategic Communication Advisor to Special Operations Command-Australia. Within academic environs, Dr. Lieber was full-time Graduate faculty at Joint Special Operations University, Emerson College, University of South Carolina, and the University of Canberra, respectively. He holds a Ph.D. in Mass Communication and Public Affairs and a Masters of Mass Communication from Louisiana State University, and a B.S. in Broadcast Journalism from Syracuse University.

Krešimir Mamić Head of Counter Terrorism Service of Ministry of Interior of the Republic of Croatia with more than 15 years of experience in police, specialized in Counter Terrorism issues.

Robert Mikac is Assistant Professor at the Faculty of Political Science of the University of Zagreb in the area of Social Sciences, Field of Political Science, Subfield International Relations and National Security. He is the author and co-author of six books and more than forty scientific articles. Prior to his academic career, he served in various positions within the Croatian security sector from the operational to the strategic level in the country and internationally. Among other things, he served in the NATO ISAF mission in Afghanistan. For merit in Afghanistan he was awarded with the NATO Medal and the Order of Merit of the Italian Republic.

Ferdinand Odzakov, PhD was born in 1969 in Gnjilane, Kosovo. He graduated from the Institut for Defense and Protection (Now: Institut for Security, Defense and Peace Studies) within Faculty of Philosophy in Skopje, in April 1994. In 2010 he obtained master's degree in the field of defense. He obtained doctor's degree in the field of law in 2013.

Since February 2018 he is visiting Associate Professor at the European University-Republic of North Macedonia in Skopje. Ferdinand Odzakov works at the Ministry of Defense of the Republic of North Macedonia, for more than 24 years. Since 2007 to 2015 he was Head of Military Service for Security and Intelligence in the Ministry of Defense of the Republic of North Macedonia.

His current position is Head of Human Resources Department in MoD. Ferdinand Odjakov was participant on different courses & seminars in USA, Germany and Turkey.

Sara Perković is currently employed at Nanobit d.o.o. after four years of working in the Thai Consulate General in Zagreb. She was born in Zagreb, on January 2nd, 1988. She has a bachelor's degree in Communication studies and has finished postgraduate studies in International relations and Diplomacy in the Faculty of Government and European Studies in Kranj, Slovenia.

Mile Šikman, Associate professor, PhD in Law, is the head of Police Education Administration within the Republic of Srpska's Ministry of the Interior. He is a professor of Criminology and Organized Crime at the Faculty of Security Science and Law Faculty of the University of Banja Luka. So far, he has had three textbooks, three monographs and several other papers published. He has also published over 140 scientific and expert studies and has taken participation in many international and national conferences. He was also a part of several scientific and research projects. He has been given a status of educator in the Center for Education of Judges and Prosecutors of the Republic of Srpska. He participated in the development and implementation of the strategy called "Community Policing in BiH" (2008-2011), and the strategy "Prevention of Juvenile Delinquency in BiH" (2011-2014).

Elen Twrdy has a PhD in Transport Technology at University of Ljubljana. She obtained an MSc in 1995 from the University of Rijeka, Croatia, and her PhD from the University of Ljubljana in 2003. She was a Dean of the Faculty of Maritime Studies and Transportation (University of Ljubljana) during the period 2007-2019. Currently she is Head of Department of Transport Technology.

She is a full Professor at the Faculty of Maritime Studies and Transport at the University in Ljubljana at the first, second and third levels of study. She has written various academic and research papers from the field of transport technology and transport logistics, with a special research area in terminals, ports and maritime transport, and maritime logistics. Her bibliography lists more than 100 papers published in scientific journals and presented at conferences.

Adrian Victor Vevera, is the General Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics, as well as a Senior Researcher II General Director. A Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Vevera has extensive experience in the field of national security, fulfilling various positions over time, in numerous managerial and counselling posts in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.

Iva Žutić graduated in History and Comparative literature in 2007 at the Faculty of Philosophy University of Zagreb, and finished university specialist postgraduate study programme 'Leadership' in 2009. at the Faculty of Economy University of Zagreb. She started career in the private sector in 2008, and since 2010 has been employed as an advisor in the Agency for Mobility and EU programmes. Since January 2011, she has been employed in the Croatian Parliament, first as an advisor, then as the Secretary of the Deputy Club of Croatian People's Party - Liberal Democrats. From July 2014 to July 2019, she worked at the European Parliament in Brussels, Belgium, as an advisor for the European Union's foreign, security and defence policy to Jozo Radoš, Member of the European Parliament.

Rising to the global security challenges calls for coordinated and effective responses. Terrorism, the radicalization of individuals and groups, and the risks posed by the cyber environment involve serious threats to the continued operation of critical infrastructure. The introduction of new technologies further increases the complexity of the environment in which critical infrastructure operates. This book gives some of the answers we need for the future in order to be even more effective in preventing these socially deviant acts. Through its activities, the Republic of Slovenia adds its part of energy, knowledge and experience to the international mosaic designed to ensure national and international security. It will be difficult to overcome all the accumulated challenges in a short period of time, so the awareness of the importance of long-term and continual efforts is crucial for achieving the expected success. Our commitment to preserving all the democratic and technological gains of our age will also have a significant impact on the further development of effective measures directed towards ensuring the security and stability of our society.

Matej Tonin MA
Minister of Defence of the Republic of Slovenia

Terrorism has claimed innocent lives for thousands of years. We saw it evolve to greater levels of violence and lethality in the 21st century, and it will undoubtedly remain a threat to peace and freedom for the foreseeable future. As they have in the past, the enemies of civilization continue to expand their methods to disrupt our way of life, seeking targets on which we all depend such as our financial systems and information and communications technology. Our age is also characterized by a growing reliance on automation. Cybersecurity is central to security and resilience of critical infrastructure. Nations throughout Europe and the Western Balkans have made significant investments to protect critical systems and ensure our militaries and governments maintain an advantage in the cyber domain. We must remain vigilant. Our adversaries seek new asymmetric ways to exploit cyber vulnerabilities and attack critical information and communications systems. This Regional Defense Fellowship Program book is an important examination of the issues all nations face.

Lynda C. Blanchard
U.S. Ambassador to Slovenia

Modern security processes present significant challenges. In the field of protection of critical infrastructure, these challenges are increasingly related to the risks of the cyber environment. Adding to this framework the human potential, which has been neglected in the recent period, specifically because of the development of new technologies in the area of artificial intelligence, two important segments stand out; they are addressed in this book. The radicalization of individuals or wider social groups, and the associated cyber risks in the modern information society, can significantly affect the smooth and uninterrupted operation of those procedural and technological capabilities that fall under critical infrastructure. These are of key importance for the functioning of individual sectors and for the proper functioning of the wider community. Success in counteracting these complex security phenomena relating to the protection of critical infrastructure can be ensured through appropriate cooperation of all the involved entities within the public and private environments.

Blaž Košorok
State Secretary Ministry of Infrastructure of the Republic of Slovenia