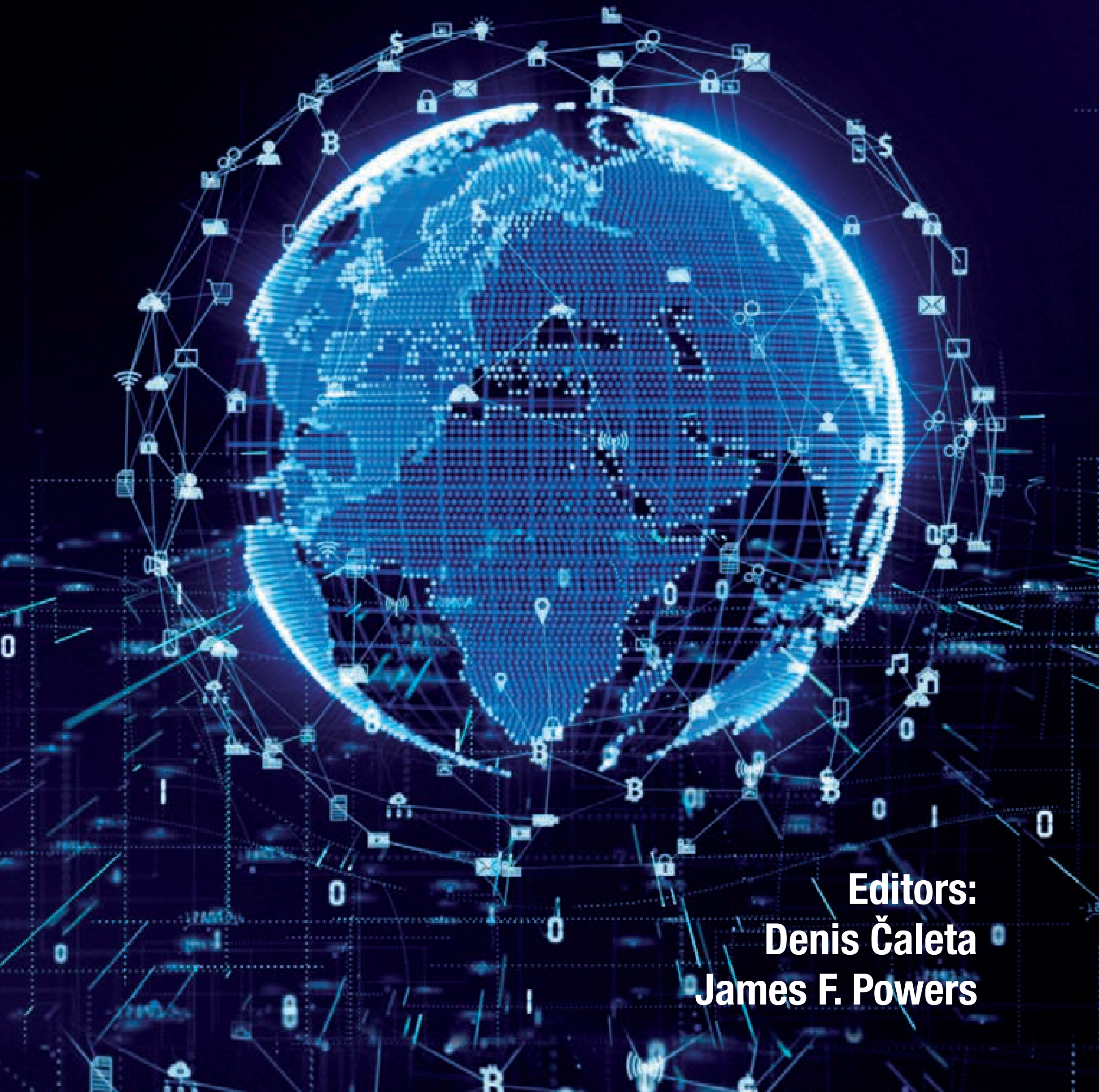
Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection



Editors:
Denis Čaleta
James F. Powers

Publishing of this publication was funded by the Regional Defense 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 increasingly 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 operations. 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.

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).

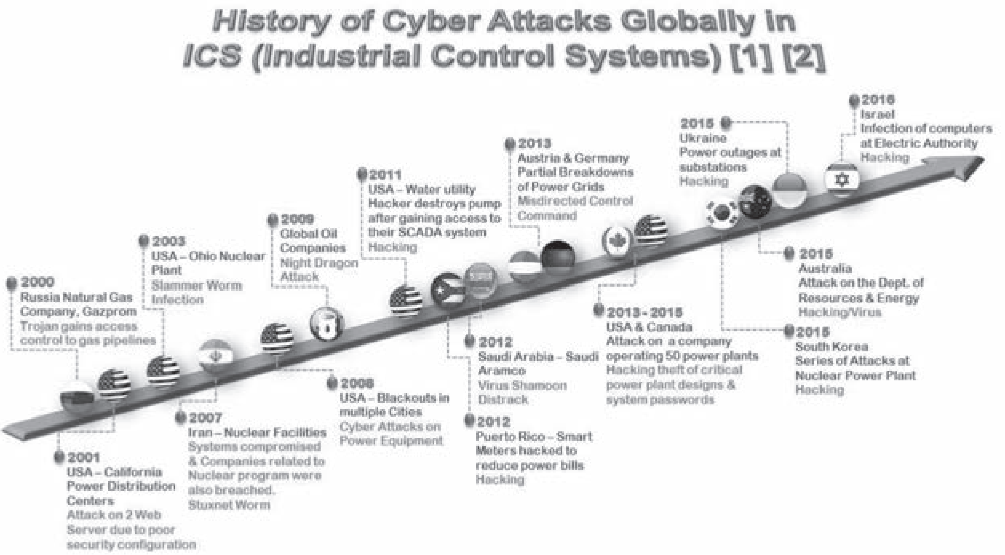

History of Cyber Attacks Globally in
ICS (Industrial Control Systems) [1] [2]
2000
Russia Natural Gas Company, Gazprom
Trojan gains access control to gas pipelines
2001
USA – California Power Distribution Centers
Attack on 2 Web Server due to poor security configuration
2003
USA – Ohio Nuclear Plant
Slammer Worm Infection
2007
Iran – Nuclear Facilities
Systems compromised & Companies related to Nuclear program were also breached.
Stuxnet Worm
2008
USA – Blackouts in multiple Cities
Cyber Attacks on Power Equipment
2009
Global Oil Companies
Night Dragon Attack
2011
USA – Water utility
Hacker destroys pump after gaining access to their SCADA system
Hacking
2012
Saudi Arabia – Saudi Aramco
Virus Shamoon Distrack
2012
Puerto Rico – Smart Meters hacked to reduce power bills
Hacking
2013
Austria & Germany
Partial Breakdowns of Power Grids
Misdirected Control Command
2013 - 2015
USA & Canada
Attack on a company operating 50 power plants
Hacking theft of critical power plant designs & system passwords
2015
Ukraine
Power outages at substations
Hacking
2015
Australia
Attack on the Dept. of Resources & Energy
Hacking/Virus
2015
South Korea
Series of Attacks at Nuclear Power Plant
Hacking
2016
Israel
Infection of computers at Electric Authority
Hacking

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 Co-operative 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.

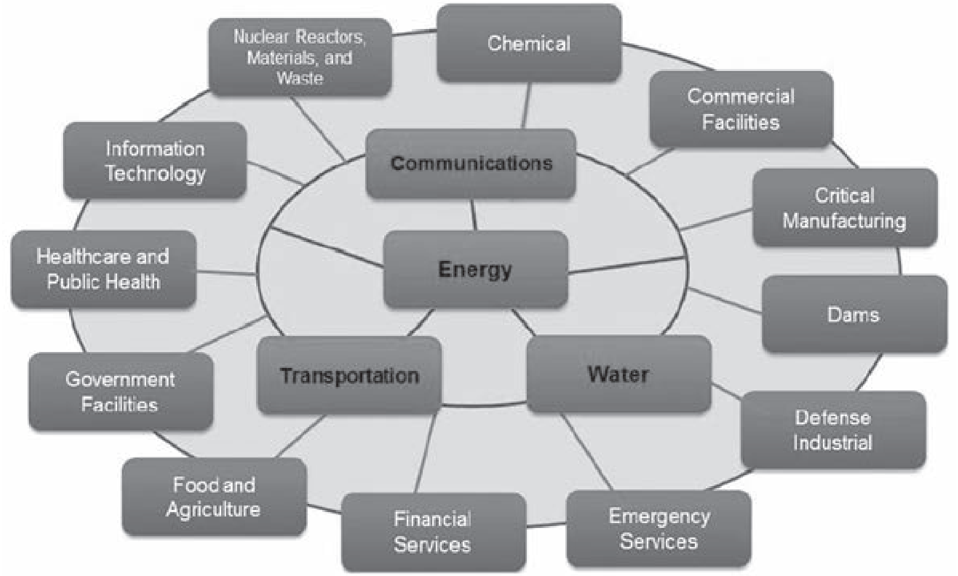


Figure 2: Critical Infrastructure Interdependencies[2]

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/

Index

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