Critical Infrastructure Security – the ICT Dimension

Grzegorz Abgarowicz, Ryszard Antkiewicz, Piotr Ciepiela, Michał Dyk, Dominika Dziwisz, Zbigniew Fałek, Piotr Gajek, Rafał Kasprzyk, Włodzimierz Kotłowski, Mirosław Maj, Andrzej Najgebauer, Dariusz Pierzchała, Aleksander Poniewierski, Maciej Pyznar, Mirosław Ryba, Krzysztof Rzecki, Joanna Świątkowska, Zbigniew Tarapata, Agnieszka Wiercińska-Krużewska

Main Partner

EY
Building a better
working world

Strategic Partner

RCB
Rządowe Centrum
Bezpieczeństwa

The Kosciuszko Institute

Critical Infrastructure Security – the ICT Dimension

Grzegorz Abgarowicz, Ryszard Antkiewicz, Piotr Ciepiela, Michał Dyk, Dominika Dziwisz, Zbigniew Fałek, Piotr Gajek, Rafał Kasprzyk, Włodzimierz Kotłowski, Mirosław Maj, Andrzej Najgebauer, Dariusz Pierzchała, Aleksander Poniewierski, Maciej Pyznar, Mirosław Ryba, Krzysztof Rzecki, Joanna Świątkowska, Zbigniew Tarapata, Agnieszka Wiercińska-Krużewska

The Kosciuszko Institute

If you appreciate the value of the presented publication, we kindly encourage you to financially support our future publishing initiatives.

Critical Infrastructure Security – the ICT Dimension

Grzegorz Abgarowicz, Ryszard Antkiewicz, Piotr Ciepiela, Michał Dyk, Dominika Dziwisz, Zbigniew Fałek, Piotr Gajek, Rafał Kasprzyk, Włodzimierz Kotłowski, Mirosław Maj, Andrzej Najgebauer, Dariusz Pierzchała, Aleksander Poniewierski, Maciej Pyznar, Mirosław Ryba, Krzysztof Rzecki, Zbigniew Tarapata, Agnieszka Wiercińska-Krużewska

Editor: Joanna Świątkowska

Editorial assistant: Anna Hojcak

The Kosciuszko Institute's team analysing factors influencing security and formulating recommendations on the basis of the chapters' content: Joanna Świątkowska, Zbigniew Fałek.

Translation: Justyna Kruk, Krzysztof Gajda (*Introduction* and *Recommendations*)

Graphic design: Małgorzata Kopecka

In Images 7 and 11, the following Noun Project icons have been used: Arrow by Roman J. Sokolov, Skull and Crossbones by Andrew Cameron, Factory by Patrick Trouvé, Key by Márcio Duarte, Settings by Luis Rodrigues, Security by mohit arora, Route by Carlos Valério, Server Security by Roman Kovbasyuk, Laptop by Simple Icons, Analysis by Christopher Holm-Hansen, Network by Matthew Hawdon, Flow Chart by Jhun Capaya, Server by Jaime Carrion, Gears by Hysen Drogu, Computer by Simple Icons, Server by Alf.

Publication date: August 2014

The Kosciuszko Institute
ul. Lenartowicza 7/4
31-138 Kraków, Poland
e-mail: ik@ik.org.pl
mob.: +48 12 632 97 24
www.ik.org.pl

ISBN: 978-83-63712-22-8

Table of contents

The views expressed in this publication are those of the authors and do not necessarily reflect any views held by the Kosciuszko Institute and the publication partners. They are published as a contribution to public debate.

Authors are responsible for their own opinions and contributions and the authors do not necessarily support all of the opinions made by others in the report.

Introduction

Joanna Świątkowska, Zbigniew Fałek
– the Kosciuszko Institute

Critical infrastructure (CI) is a key component of national security, stability and economic growth. It also determines the functioning of societies and individuals. Even though infrastructure of special significance for man and the communities he creates has always existed, it only gained in importance as civilizations developed. Consequently, it has become more and more vital to ensure its safety, especially over recent years.

A turning point in the debate over CI protection was marked by the terrorist attacks which took place in the USA on September 11th 2001 and then in London and Madrid in 2004. The attacks showed, first, what terrible consequences can be brought about by targeting the most pivotal infrastructure elements; second, how much these elements are interrelated[1]; and finally that the entire state system may be put in danger not only by state- but also non-state actors. Faced with this reality, individual states and international organisations (e.g. the European Union) intensified their actions with the aim to protect CI.

Currently, however, we can observe yet another trend of crucial importance for ensuring CI security – the increasing role and gravity of security in cyberspace as the basis for the functioning and security of CI. The present report focuses on exactly this topic.

ICT solutions related to CI can be discussed in two different ways. First, ICT networks in Poland constitute one of the country's CI systems. Second, ICT is part of different CI systems supporting them and often ensuring their proper functioning. In other words, ICT solutions may be CI in themselves or act as components of other CI elements.

What is the danger?

The fact that CI is increasingly dependent for its functioning on ICT solutions coupled with the changes taking place in this domain poses new challenges related to ensuring security. Potential dangers can be caused by technical failures and human error, but also intentional, hostile activities undertaken in cyberspace. There are at least several reasons making this last category of threats more and more menacing.

[1] See B. Hammerli, A. Renda, *Protecting Critical Infrastructure in the EU*. CEPS Task Force Report, 2010, p. 12.

CI may be disrupted or destroyed by attacking its ICT elements. Cyberspace attacks are, among other things, relatively cheap to prepare and carry out but have potential to inflict great damage on the target. Their additional "advantage" is that it is difficult to detect the perpetrator and prove his guilt[2] which means that he is relatively safe in the sense that he can avoid reprisal and responsibility in all its different aspects. Potential severity of damage, the ease of carrying out the attacks and shifting responsibility mean that cyber attacks against CI may become the key weapon at the disposal of states and non-state aggressors.

According to "The Cyber Index. International Security Trends and Realities" prepared under the auspices of the UN, there is a sharp increase in the number of states which set up special official agencies dedicated to cyberspace activity (also offensive) as part of their armed forces[3]. All of this shows that cyberspace may become a major theatre of conflict. Cyber attacks against CI may destabilise the functioning of a state in a situation of political tension or be used as an important element in a military campaign during an open conflict.

Potential attacks may be prepared already at the time of peace. Every so often, the media report of cyber espionage activities targeting entities operating within systems commonly considered to be CI[4]. Even though such activities are mostly carried out for financial reasons, they do make it possible to acquire knowledge of and access to systems which may become targets in future. There are also other methods of "paving the way" for potential aggression. It is enough to realise that the ICT products (hardware, software, etc.) we use are produced all over the world. As a result, it is not difficult to embed hostile elements which, activated at the right moment, may impair the functioning of the entire system.

Today, potential sources of danger are no longer only nation states. In spite of the fact that the scenario whereby non-state actors[5] perpetrate mass-scale cyber attacks against CI with far-reaching, nation-wide consequences may not seem very likely[6], the danger is higher in the case of individual infrastructure elements.

Finally, in addition to potential intentional threats related to the employment of digital tools, it is critical to ensure protection from human error, technical failures or even the natural environment.

Objectives and structure of the report

Acknowledging the fundamental importance of CI for national security, the Kosciusko Institute decided to devote the present report to the problem of its protection focusing primarily on

[2] The problem of attribution.

[3] Centre for Strategic and International Studies, Institute for Peace Research and Security Policy, *The Cyber Index. International Security Trends and Realities,* UNIDIR, 2013, p. 3.

[4] For a list of systems covered by critical infrastructure in selected countries see for example: Haemmerli, A. Renda, *CEPS Task Force Report. Protecting Critical Infrastructure in the EU*, 2010, http://www.ceps.eu/book/protecting-critical-infrastructure-eu, [accessed: 05/03/2014].

[5] Single aggressors, cyber terrorists and criminal organisations, but not supported by states in this context.

[6] Due to the lack of advanced knowledge necessary to carry out an attack of this type as well as other resources (broadly understood).

cyber security of CI due to its growing role and significance. Our ambition is that the report contribute to the on-going debate over CI protection especially in the context of cyber criminality.

The main objective of the report is to provide entities directly responsible for CI protection with recommendations improving security. The recommendations have been developed following an analysis of factors influencing both CI protection in its general aspect as well as ICT security of CI. The factors were selected from individual chapters in the report and constitute their most important element.

The structure of the report reflects the objective presented above and the tasks set for the authors. The report is divided into two parts. The first contains general, systemic reflections related to CI and ensuring its security. It puts great emphasis on the problem of identifying CI (a necessary pre-condition for its protection), legal aspects of CI security as well as cooperation between private and public actors. Hence, this part of the report is addressed mainly to decision makers and entities responsible for national security in its entirety.

The second part is devoted specifically to ICT aspects. It identifies the most pivotal factors related to cybersecurity of CI as well as good practices and strategies making for the most effective actions. Many recommendations contain suggestions of systemic changes whereas the others are addressed[7] to CI owners and operators and are naturally more detailed.

Part One opens with chapter written by Maciej Pyznar and Grzegorz Abgarowicz, PhD, from the Government Centre for Security. Not only does it introduce the reader to fundamental facts on CI, but it also shows the most important, selected elements of the CI protection system from the perspective of the state. The focal part of the chapter is devoted to reflections on the CI identification process.

The second chapter was prepared by the law firm Wierciński-Kwieciński-Baher. It analyses the legal aspects of CI both on the national and the international level. The analysis focuses in particular on financing CI protection activities, public procurement issues and the problems of establishing cooperation between the public and private sectors.

Chapters Three and Four in Part One, written by the experts from the Kosciusko Institute, Joanna Świątkowska and Dominika Dziwisz, PhD, should be treated as complementary. They are both devoted to the problem of public-private cooperation and the factors influencing its effectiveness. Currently, most of CI is either owned or managed privately. As effective cooperation between the state and the owner or operator of CI is a pre-condition for its efficient protection, the topic is discussed at length in the first part of the report.

The second part opens with a chapter by Mirosław Ryba, PhD, from EY showing the role ICT solutions play in the context of the functioning and security of CI. The chapter highlights the use of IT and OT systems.

[7] Or directly concern.

Chapter Six, also prepared by an EY expert, Aleksander Poniewierski, PhD, describes major changes which took place in the functioning of ICT solutions employed in the area of CI. The changes happened on the economic, technological and organizational level and have a direct impact on the challenges related to ensuring CI security. It is necessary to realise and understand them in order to take efficient measures.

Chapter Seven, written by Włodzimierz Kotłowski from MATIC, shows how ICT solutions are used to protect CI effectively.

Chapter Eight by Piotr Ciepiela form EY is devoted to the security of OT, a crucial component in the entire system of CI cybersecurity. The chapter not only presents the most important standards of OT (and, to a lesser degree, IT) security, but also suggests other solutions ensuring and improving security.

Cyber security of CI also requires a well organised incident reaction process. Chapter Nine by Mirosław Maj, the President of the Safe Cyberspace Foundation, contains good practices in this area as well as a short analysis of incidents threatening the ICT security of CI.

Chapter Ten presents the authors' original concept of an IT toolkit improving the efficiency of detecting, countering and neutralising the effects of cyber threats. The toolkit was developed by a team led by Professor Najgebauer from the Military University of Technology and may be broadly used in ways going beyond the purely military domain in such areas as crisis management on different levels of central and local administration.

The last chapter prepared by Krzysztof Rzecki, PhD, from the Cracow University of Technology contains an analysis of tertiary education curricula in the area of CI's ICT network system protection.

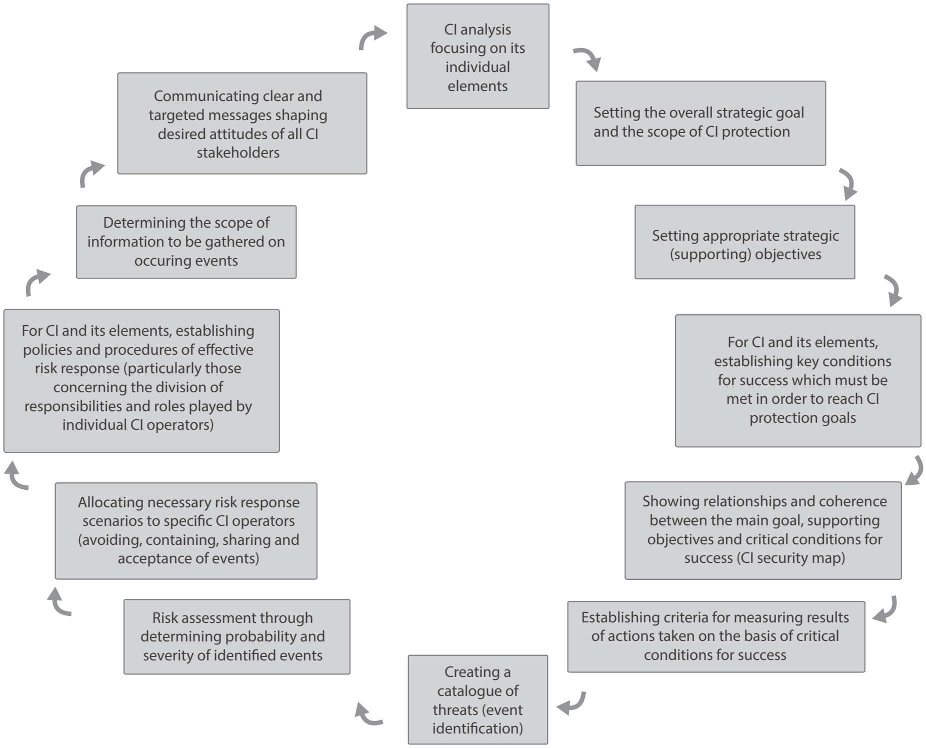
The report is concluded by recommendations.

What follows (Figure 1) is a process chart presenting the most important elements related to ensuring CI security. The report touches upon most of the suggested elements, but has no ambition of being an exhaustive discussion of all CI security problems. This is primarily because the subjects of CI in general and the ICT aspect of its functioning in particular are very broad.

Having analysed the factors influencing CI security, not only could we prepare basic recommendations contained in this report, but also identify those elements which require further study. As we are well aware that there are a lot of important issues which it was impossible to put into a single document, we hope to continue our work and research.

Finally, since the entire report has been drafted on the basis of unclassified and generally available data, the reader should be aware that it does not provide a full account of all information which may bear upon CI security and may omit some factors which are specific for the resources used.

Figure 1a. The process of ensuring critical infrastructure security – the most important elements.
Source: own compilation


CI analysis focusing on its individual elements
Setting the overall strategic goal and the scope of CI protection
Setting appropriate strategic (supporting) objectives
For CI and its elements, establishing key conditions for success which must be met in order to reach CI protection goals
Showing relationships and coherence between the main goal, supporting objectives and critical conditions for success (CI security map)
Establishing criteria for measuring results of actions taken on the basis of critical conditions for success
Creating a catalogue of threats (event identification)
Risk assessment through determining probability and severity of identified events
Allocating necessary risk response scenarios to specific CI operators (avoiding, containing, sharing and acceptance of events)
For CI and its elements, establishing policies and procedures of effective risk response (particularly those concerning the division of responsibilities and roles played by individual CI operators)
Determining the scope of information to be gathered on occuring events
Communicating clear and targeted messages shaping desired attitudes of all CI stakeholders

part I

1. The role of critical infrastructure in the functioning of the state

Maciej Pyznar, Grzegorz Abgarowicz
– the Government Centre for Security

The infrastructure development and its growth in significance

Human needs have always determined advances in technology. The process of taming nature through technology intervention with the surroundings has accompanied mankind nearly from the outset.

The development of agriculture stemmed from the need to provide food; the development of industry was supposed to make human life easier while medical advances helped keep life-threatening illnesses at bay.

It is human nature that determines the desire and need to create and constantly modify the environment.

In his "Little Book About Man," Roman Ingarden wrote: *what makes us human is that in a sense we "live beyond our means," beyond everything we need to sustain our basic physiological life (...) we create "things" that any physiological life considers luxurious (....). What makes us human is that we surpass biological conditions we were born into and we use them as the basis for creating a new different world*.[1]

As a result of human activity, the layers of culture, technology, and social solutions are applied on Ingarden's duality: human–nature. Those "things" are the state and infrastructure alike. Since social or cultural concepts are inscribed in and limited by human nature, this duality transforms into a triad: man–nature–technology.

Having been accustomed to the presence of infrastructure in his life, man fails to notice that a widespread access to it is a relatively recent phenomenon which began with the industrial and technological revolutions at the turn of the 19th and 20th centuries.

This revolution initiated changes in the entire social structure, being mostly determined by the expansion of urban areas. With population growth in urban areas, the needs of the

[1] R. Ingarden, *Książeczka o człowieku* [Little Book About Man], Wydawnictwo Literackie Kraków, Kraków 1987, p. 37.

people residing in them started growing rapidly. Those requirements stemmed not only from the desire to satisfy individual needs of residents, but also from the demands of the collective population with regard to protection against crime or diseases, two-way communication or transport.

Despite a heavy burden of negative historical experiences, the course of Poland's technological advancement was similar to that of other countries.

In order to illustrate the phenomenon of technological development, it is worth tracing the evolution of at least some of its elements. In 1929, Poland had 57 active 5 MW power plants with a combined output of 636 MW.[2] Their combined power generation totalled 2,355 GWh.

As of 30 September 2013, the total installed capacity of all Polish power plants amounted to 38490.1 MW[3] while power generation in 2011 was 70 times higher and totalled 163,118 GWh.[4]

When analysing the data, we need to remember that prior to World War II, power plants in Poland did not constitute an interconnected system and there was no nationwide power network.[5] The power systems as we know them today were developed after World War II, i.e. only 70 years ago.

At the beginning of the 19th century, a glass of water could either quench thirst or kill. Currently perceived as an obvious element of everyday life, safe drinking water was scarcely accessible while fatal water-borne diseases, such as cholera, typhoid or dysentery, posed a constant and real threat.[6] The first clean water was distributed to the residents of Warsaw on 3 July 1886. In 2012, Poland had 8,748 water and sewage companies supplying water to over 37 millions of people.[7]

[2] *Mały rocznik statystyczny 1930* [1930 Small Statistical Yearbook], table 5, "Elektrownie w Polsce" [Power Plants in Poland], p. 33, http://statlibr.stat.gov.pl/exlibris/aleph/a18_1/apache_ media/4U9MMALMHKN1ENV6KTGHPGE9HDUFM8.pdf, [accessed: 08/04/2014]. The largest main activity producers around 1938 included Powiśle Power Plant (83 MW), Pruszków Power Plant (31.5 MW), Łaziska Power Plant (105 MW), Będzin Power Plant (23.5 MW), Zabrze Power Plant (70.3 MW), Szombierki Power Plant (51.2 MW), Łódź Power Plant (101 MW), Garbary Power Plant in Poznan (42 MW), *Historia polskiej energetyki* [The History of Polish Energy Industry], http://www.wnp.pl/artykuly/historia-polskiej-energetyki,5327.html, [accessed: 08/04/2014]. For the sake of comparison, the nameplate capacity of Bełchatów power plant is 5,298 MW.

[3] CIRE.pl, http://www.rynek-energii-elektrycznej.cire.pl/st,33,207,tr,75,0,0,0,0,0,podstawowe-dane.html, [accessed: 10/04/2014].

[4] Ibidem.

[5] *Historia polskiej energetyki* [The History of Polish Energy Industry], http://www.wnp.pl/artykuly/historia-polskiej-energetyki,5327.html, [accessed: 08/04/2014].

[6] *Greatest Engineering Achievements of the 20th Century*, http://www.greatachievements.org/?id=3610, [accessed: 08/04/2014]. In order to demonstrate how recent a development the ability to supply clean water is, we recommend analysing achievements of mankind presented on the timeline.

[7] Chief Sanitary Inspectorate, "Stan sanitarny kraju w 2012 r." [Sanitary conditions in Poland in 2012], table 22. "Struktura przedsiębiorstw wodociągowo-kanalizacyjnych w 2012 r." [The structure of water and sewage companies in 2012], p. 76. The situation looks interesting in the case of sewage disposal and treatment. According to *2013 Small Statistical Yearbook of Poland* (p. 49), in 2012, wastewater treatment plants provided service to only 69% of the country's population (92% in urban areas and in villages, where about 39% of the country's population reside, as little as 33%).

In 1927, Robert Bosch GmbH launched the production of a fuel injection system for a combustion-ignition engine[8], constructed by Rudolf Diesel in 1893, which allowed for its wide use in motor-driven vehicles and road transport. In the same year, Poland had only 45,500 km of hard-surface roads[9] on which diesel-engined lorries could drive. The hard-surface road network in Poland increased to 280,000 km in 2011[10] to allow for a transport of 1,545 million tonnes of goods in 2012.[11]

Between 1927 and 2012, the railway network grew from 17,146 km to 20,094 km.[12] It is a fair observation to make that, given the period of eighty-five years, the increase of 2,948 km seems small. It needs to be noted, however, that more than half of the railway lines have been electrified[13] and used to transport over 230 million tonnes of goods in 2012 (in 1927, it was 73.7 million tonnes[14]).

In 1928, there were 126,000 telephone subscribers in Poland who in total made 672 million calls.[15] In 1929, in the whole of Poland, there were 157,000 telephone sets[16], which means that back then only about 0.5% of the population owned a telephone set.[17] Conversely, in 2012, nearly 7.4 million subscribers (almost 20% of the population[18]) used land lines while the combined call volume reached 13 billion minutes.[19]

It goes without saying that pre-war Poland and the then contemporary world did not know mobile telephony. In 2012, the combined volume of SIM cards registered by operators in their databases was over 53.9 million[20] (140% of the population) whereas the total time of outgoing calls in 2012 amounted to over 69 billion minutes.[21]

It was not until the second half of the 20th century that the world first heard about a new means of communications – the Internet. In today's Poland, there are over 11.6 million

[8] F. DeLuca, *History of fuel injection*, http://www.disa.it/pdf/01HystoryOfDieselFuelInj.pdf, [accessed: 08/04/2014].

[9] *Mały rocznik statystyczny 1930 r.* [*1930 Small Statistical Yearbook*], table 8, "Drogi Bite w Polsce w latach 1925 – 1928" [Hard-surface roads in Poland in 1925–1928], p. 55.

[10] *Mały rocznik statystyczny Polski 2013* [*2013 Small Statistical Yearbook of Poland*], table 1 (237), "Sieć Komunikacyjna" [Transportation Network], p. 379.

[11] Ibidem.

[12] *Mały rocznik statystyczny Polski 2013* [*2013 Small Statistical Yearbook of Poland*], table 1 (237), "Sieć Komunikacyjna" [Transportation Network], p. 379 and M*ały rocznik statystyczny 1930 r.* [*1930 Small Statistical Yearbook*], table 1, "Długość linii i tabor w latach 1922–1928" [Railway track length and rolling stock in 1922–1928], p. 52.

[13] *Mały rocznik statystyczny Polski 2013* [*2013 Small Statistical Yearbook of Poland*], table 1 (237), "Sieć Komunikacyjna" [Transportation Network], p. 379. It is also worth bearing in mind that railway electrification in Poland only took place after World War II.

[14] *Mały rocznik statystyczny 1930 r.* [*1930 Small Statistical Yearbook*], table 3, "Przewóz pasażerów i towarów w latach 1922 – 1928" [Transport of passengers and goods in 1922–1928], p. 52.

[15] Ibidem, table 24, "Telefony w Polsce w latach 1924 – 1928" [Telephones in Poland in 1924–1928], p. 61.

[16] Ibidem, table 27, "Stan liczbowy telefonów w niektórych państwach w 1929 r."[The volume of telephones in some countries in 1929], p. 62.

[17] Poland's population on the 1st January 1930 was 30.7 million. *Mały rocznik statystyczny 1930 r.* [*1930 Small Statistical Yearbook*], table 6, "Ludność Polski w latach 1921 i 1930" [The population of Poland in 1921 and 1930], p. 4.

[18] Poland's population on the 31st March 2011 was 38,512. *Mały rocznik statystyczny Polski 2013* [*2013 Small Statistical Yearbook of Poland*], table 1 (62), Ludność na podstawie spisów [Population on the basis of censuses], p. 116.

[19] *Raport o stanie rynku telekomunikacyjnego w Polsce w 2012 roku* [*Report on the telecommunications market in Poland in 2012*], President of the Office of Electronic Communications, Warsaw, June 2013, pp. 48–49.

[20] Ibidem, p. 23.

[21] Ibidem, p. 27.

broadband Internet subscribers[22], which places the Internet service saturation per household at 83.5%.[23] We also cannot forget about other services that emerged together with the Internet, e.g. VoIP (Voice over IP). Over 1.1 million users in total used this service (for a fee) in 2012.[24]

When analysing the quantitative and qualitative development of infrastructure on the example of Poland, two determinants need to be taken into account.

First, the service supply infrastructure is remote geographically wise.[25] It is owned by enterprises established specifically for this purpose and end users have very little impact on how it works. This was influenced by at least three factors:

- The absence of suitable technologies for individual application: no technology existed in the past that would enable individual households to become independent of the infrastructure (the fact that people did not take advantage of the infrastructure in rural areas has to be disregarded); likewise, the funding of technological development was out of the range of an ordinary citizen. In contemporary times, this trend is being reversed and we are increasingly in a possession of such technologies, e.g. electricity generating photovoltaic cells, on-site wastewater treatment systems, ionizers for water purification, etc.

- The cost of technological advancement: the construction and maintenance of infrastructure is expensive; therefore, the financing of it was taken upon by the state, local authorities, or private investors. Only these entities could bear the cost of investment into power plants, wastewater treatment plants or roads;

- The need to provide a large number of consumers with the access to infrastructure: in the past, the only means to meet this demand was the construction of a centralised infrastructure. This stems from the fact that due to this centralisation, charges for access to the services provided through the infrastructure are relatively low and thus widely accessible despite the high costs of building and maintaining the infrastructure.

Second, the process in which man is becoming increasingly detached from nature and its unpredictable power through technological development expressing the expansion of human independence and his needs, has paradoxically introduced another threat – that of "on-technology dependence". Nevertheless, the potential lack of access to services is not the only consequence of human activity in this domain. The very fact that this infrastructure exists carries with it further risks. Due to the diffusion of innovations[26], these threats are also becoming fundamental risks for the contemporary world, especially since the process of assimilating technological novelties can no longer be counted in decades, but in months. The

[22] Ibidem, p. 7.

[23] Ibidem, p. 4.

[24] Ibidem, p. 63.

[25] For example, there are only 20 main activity producers in Poland with a nameplate capacity of over 80%, *Elektrownie w Polsce* [*Power plants in Poland*], http://www.rynek-energii-elektrycznej.cire.pl/st,33,200,tr,67,0,0,0,0,0,elektrownie-w-polsce.html and *Podstawowe dane* [*Basic data*], http://www. rynek-energii-elektrycznej.cire.pl/st,33,207,tr,75,0,0,0,0,0,podstawowe-dane.html [accessed: 25/05/2014].

[26] More in: A. Pomykalski, *Innowacje* [*Innovations*], Wydawnictwo Politechniki Łódzkiej, Łódź 2001.

emerging new technologies quicken the pace in which the reality changes, making it impossible for man to prepare for their consequences. Such a state of affairs is an offshoot of both the rapidity of changes themselves and the unpredictability of their consequences. Being a result of searching for ever new means to satisfy human needs, this technological development created not only new and previously unheard of threats but also new, secondary needs.This peculiar spiral of development has become such a natural phenomenon that it is hard to imagine man functioning in isolation from infrastructure as well as the benefits and risks it entails.

As a consequence, it is the state that needs to take upon itself the responsibility for not so much the functioning of infrastructure as the continuous supplies of services it offers and the effects of threats it poses for human health, life and the natural environment. When realising its basic functions, the state tends to concentrate on these issues. Out of six domains related to the internal activity of the state, half of its functions directly pertain to the problem of security and are closely connected to infrastructure. These elements include: safeguarding public order and safety, citizens' property and health protection as well as actions aimed at ensuring the internal security of the state. The implementation of the remaining ones, i.e. securing the system of ownership existing in the state, maintaining and developing international relations with other states, or actions facilitating the flow of information and inter-human relations[27], is indirectly dependent on technical infrastructure and the legal system created and guaranteed by the state.

It is a fair observation to make that the functioning of the society and the state is contingent upon infrastructure while the level of its advancement affects both the efficiency and the effectiveness of tasks that the state performs. As a consequence, technological development creates a system of interdependences and interrelations between the state and infrastructure.

On the one hand, the state, acting for the benefit of security and public order, must secure itself against infrastructure-induced threats, but at the same time protect it in order to continue carrying out its infrastructure-reliant functions. On the other hand, pursuing the goal of ensuring a continuous supply of services, vast and extensive infrastructure systems tend to transfer some of their responsibility for it to the state.

Today, it is very hard to question the hypothesis that the ability of the state to perform its duties (all of its functions) is closely dependent on both the level of technological development and the quality of service provided by individual infrastructure sectors. The awareness of these dependencies and their consequences has led to isolating its most vital components from the entire infrastructure system – critical infrastructure (CI). Hence the emphasis that has been put on creating systems protecting this infrastructure for several of the previous decades.

[27] J. Oniszczuk, *Współczesne państwo w teorii i praktyce. Wybrane elementy* [*Modern state in theory and practice. Selected elements*], Warsaw: Oficyna Wydawnicza SGH, Warsaw 2008, p. 401.

What is critical infrastructure and how to identify it?

Touching upon the role CI plays in relation to the state, with the latter being perceived as a social institution that guarantees the security of its members (citizens), it is impossible not to allude to the concept of needs. One of the factors determining whether infrastructure is flagged as a critical component of the state system is recognising it as a basic instrument responsible for providing services that fulfil the needs of the state and its citizens alike.

In the literature on the subject, we can find at least several taxonomies of human needs. Abraham Maslow outlined a hierarchy of needs by grouping them into 5 levels (physiological, safety, love/belonging, esteem, and self-actualization).[28] Erik Allardt divided human needs into three spheres related to having, loving and being.[29] In turn, Andrzej Luszniewicz distinguished 7 groups of material and cultural needs: food, shelter (housing, clothes, shoes), health care, education, recreation (leisure time and its use), social protection, and material security.[30] Conversely, in the studies led by Aleksander Zeliaś, a taxonomy of 9 needs was used, including healthcare and welfare, job market and safe working conditions, adequate salary and income, appropriate housing conditions, and public safety. In addition, other needs were indicated such as education, recreation, culture and free time, communications, and protection against the effects of environmental degradation.[31]

The overview of the above taxonomies allows for a conclusion to be drawn that services provided by means of infrastructure can satisfy nearly every need imaginable, thus validating the role of CI. This perspective does not, however, warrant its criticality. In connection with the above, it is worth considering another approach which is defined by distinguishing a set of fundamental values among which human life undoubtedly takes prominence. Essentially, human life can be threatened in six ways (6WTD – 6 ways to die)[32]: overheating (too hot), hypothermia (too cold), hunger, thirst, illness, and injury.

In this approach, the role of CI is to protect the public from life and health threats as defined by 6WTD. Following this model, infrastructure can be grouped into:[33]

1. Infrastructure that provides shelter and secures its effective functioning; it is most often understood as heating and power plants
2. Infrastructure that accompanies and secures the supply chain, e.g. road and waterworks infrastructures, refineries

[28] M. Panek, *Podstawowe kategorie i klasyfikacje w badaniach poziomu i jakości życia* [*Basic categories and taxonomies in studies of standard and quality of living*], http://kolegia.sgh.waw.pl/pl/KAE/struktura/ISiD/ struktura/ZSS/zaklad/sklad/Documents/Statystyka_Tomasz_Panek/Statystyka_spoleczna/Podstawowe_kategorie_i_klasyfikacje_w_ badaniu_poziomu_ijakosci_zycia.doc, [accessed: 08/04/ 2014].

[29] Ibidem.

[30] M. Dąbrowa, *Badanie poziomu życia – metodologia konstrukcji wybranych wskaźników* [*Study in standard of living—methodology of structure of selected indicators*] – zeszyty naukowe MWSE w Tarnowie 2011, No 1(17), http://zn.mwse.edu.pl/dabrowa-maria-badanie-poziomu-zycia-metodologia-konstrukcji-wybranych-wskaznikow/, [accessed: 08/04/2014].

[31] Ibidem.

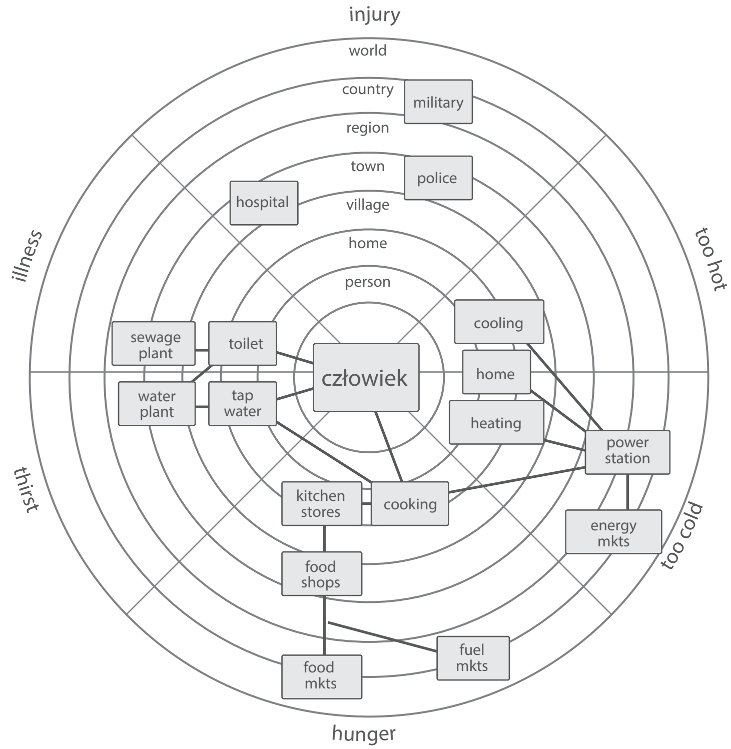
[32] M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe* – http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf. More information about research and projects in which Vinay Gupta is engaged can be found on this website: http://vinay. howtolivewiki.com/blog/about, [accessed: 08/04/ 2014].

[33] Ibidem.

3. Infrastructure that ensures access to basic safety services, allowing for the supply of services, e.g. telephone switchboards, power plants, refineries, databases.

It needs to be noted that protection against 6WTD occurs at numerous layers, which is best illustrated by the picture below.

Figure 2. The map of critical infrastructure and its layers. Source: M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe.*



If we look at the map presented above, we will notice that it does not cover CI, which is not directly linked to providing protection against 6WTD. Therefore, it appears advisable to supplement the 6WTD concept with the infrastructure indispensable for the implementation of basic functions of the state indicated earlier in order to map the state significant infrastructure completely.

By delineating mutual relations between CI, the public and the state, it is possible to make an attempt to define what CI really is. In Poland this concept shall be understood as *systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and* *enterprises*.[34] Comparing the above statement with other definitions of CI used in other countries, we discover they are akin to one another. Similarly to Poland, CI is understood in most cases as infrastructure (e.g. facilities, services, systems, networks) whose destruction or incapacitation would have serious effects for the citizens and the state. These impacts pertain to different categories, e.g. key social functions, economic well-being of citizens, national security, or the functional performance of the state.[35]

The advantage of formulating a definition of CI, besides conferring a common meaning to the term, is the possibility to include in it national objectives and operational priorities.[36] In their paper, "Critical Infrastructure: Where we Stand Today?", Cécilia Gallais and Eric Filiol[37] emphasise two components that are commonly missing from the definitions of CI, namely the human aspect and references to the political and social environment of CI. According to the authors, none of the definitions mentions people as integral part of CI although they are indispensable for the functioning of any infrastructure regardless of the fact whether their criticality is acknowledged or not. Moreover, none of the definitions takes into account the CI environment, e.g. its dependency on external components (sub-contractors, suppliers, data centres, etc.), which according to the authors, results from a very narrow-minded view of CI as a completely isolated structure. In order to fill the gaps, Gallais and Filiol propound their own, broader definition. It states that CI can be companies, institutions, or organisations at the regional, national, and international level whose disruption, damage, or destruction would have a serious impact on the health, safety, and economic well-being of citizens or the effective functioning of governments and other infrastructures that depend on it. It also includes humans whose corruption, preclusion, or death could result in the disruption of critical infrastructure. In addition, it also encompasses:

- installations (access, buildings, sites, etc.)
- equipment (computer, printer, hard drive, etc.)
- physical and natural resources
- physical (electrical, water, etc.) and virtual networks (Intranet, the Internet, etc.)
- physical and virtual data (confidential data, such as access codes and passwords, procedures, organizational chart, etc.)
- Information and Communication technology facilities
- services
- processes
- assets, including image
- systems or their parts
- another infrastructure to which connections exists (e.g. service or products suppliers)

[34] Art.3 (2) of the Act of 26 April 2007 on Crisis Management (Journal of Laws of 2013, Item 1166). The list of critical infrastructure systems, which in the case of Poland are integral to the definition of CI, has been purposefully omitted.

[35] More in: *Report OECD [Report by OECD]: Protection of 'critical infrastructure' and the role of investment policies relating to national security*, Table 1. National Definitions of Critical Infrastructure, p. 4.

[36] It needs to be noted that despite the clear advantages mentioned above, only some countries decided to take this step. Critical infrastructure protection is being implemented through the protection of assumed values, e.g. key social functions. This group comprises the following countries France, Sweden, Estonia, and Italy.

[37] C. Gallais, E. Filiol, *Critical Infrastructure: Where we Stand Today?* http://www.tevalis.fr/images/ArticleICCWS2014.pdf, [accessed: 08/04/ 2014].

which if disrupted, damaged, stolen, or destroyed would adversely affect the health, safety and well-being of employees and threaten the effective functioning of CI. In truth, any element that comprises CI could potentially disrupt its functioning, damage or even destroy it. These elements can also be found in the political and cultural environment of the infrastructure.[38]

It appears, however, that applying such a broad definition of CI is unnecessary. Apart from the fact that practical reasons would prove its application difficult, it needs to be noted that the shortcomings pointed out by Gallais and Filiol, although missing from the commonly used and compressed definitions, are applicable to every organised system of CI protection. To give an example, in Poland's National Critical Infrastructure Protection Programme, the identification of CI environment and the resulting dependencies and interdependencies is part of the risk assessment[39] while the human element is mentioned in all types of CI protection activities.[40] Nevertheless, the considerations presented by the authors of "Critical Infrastructure: Where we Stand Today" can be useful when identifying CI.

Regardless of the fact whether a country has developed its own concept of CI or not, the basic and all-important process is the identification of critical infrastructure. It raises a number of serious challenges. The first one involves developing a common, harmonised methodology that can be utilised to determine infrastructure's individual components. Another challenge is to distinguish those infrastructure components that are critical nationally from infrastructures that are key at the local and regional levels, but do not require central intervention. In addition, the process brings about grave consequences related to the protection of information gathered thereby and often including not only the list of critical infrastructures, but also sensitive critical infrastructure protection data.[41]

In the process of identifying CI, two basic approaches can be observed.[42] The "bottom-up" approach involves applying criteria to the entire national infrastructure in order to assess its criticality. Conversely, the "top-down" approach, which is more widespread in the world, assumes the application of pre-defined, basic list of critical sectors (systems or services).[43] The list of critical sectors is strongly linked to the establishing of mutual relationships between CI, the society and the state – in other words, the role that was allocated to critical infrastructure in the state. The analysis of selected examples allows for a conclusion to be drawn that the list of critical sectors (systems or services) in individual countries looks very similar.

[38] Ibidem, p. 11.

[39] See *The National Critical Infrastructure Protection Programme – main body*, p.30.

[40] See Annex 2 of *The National Critical Infrastructure...*, op.cit.– *Standards ensuring smooth functioning of critical infrastructure – good practices and recommendations.*

[41] Lord Jopling (special rapporteur), *Special report to NATO Parliamentary Assembly: The protection of critical infrastructures.*

[42] *Good practices manual for CIP policies for policy makers in Europe* – the publication is part of the project RECIPE (Recommended Elements of Critical Infrastructure Protection for policy makers in Europe).

[43] Ibidem, p. 16. The definition of critical infrastructure or other executive documents may comprise the list of critical sectors and sub-sectors.

Table 1. The breakdown of CI by sector in the French Republic. Source: Own compilation based on the *Decree of 2 June 2006 on establishing a list of sectors of vital importance and appointing the coordinating ministers of the said sectors (Décret du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale)*.

Sector	Minister–Coordinator
Government administration	Minister of the Interior
Judicial system	Minister of Justice
State military activity	Minister of Defence
Food	Minister of Agriculture
Electronic communications and information transmission	Minister competent for electronic communications
Energy	Minister of Industry
Space research	Minister competent for research
Finance	Minister of the Economy and Finances
Water management	Minister of Ecology
Industry	Minister of Industry
Health	Minister of Health
Transportation	Minister of Transport

Table 2. The breakdown of CI by sector in the United States of America. Source: Own compilation based on the *Homeland Security Presidential Directive-7 of December 17, 2003 on Critical Infrastructure Identification, Prioritization, and Protection.*

Sector	Competent agency
Chemical industry Business facilities Lock gates Emergency services Nuclear	Department of Homeland Security
Defense industry	Department of Defense
Agriculture and food	Department of Agriculture Department of Health and Social Services (for food other than poultry, meat, and egg products)
Telecommunications and information technologies	Bureau of ICT Protection and Telecommunications
Energy	Department of Energy
Banking and finance	Department of the Treasury
Water (including wastewater discharge)	Environmental Protection Agency
National heritage	Department of the Interior
Postal services	Transportation Security Administration
Health	Department of Health and Social Services
Transportation	Transportation Security Administration United States Coast Guard (maritime transport)
Government facilities	Immigration and Customs Enforcement Federal Protective Service

Table 3. The breakdown of CI by sector in the Kingdom of the Netherlands. Source: Own compilation based on the report published in 2005 by the Ministry of the Interior and Kingdom Relations entitled *Protection of Critical Infrastructure.*

Sector	Competent Minister
Energy	Minister of Economic Affairs
Telecommunications and information technologies	
Drinking water supply	Minister of Housing, Spatial Planning and the Environment
Chemical and nuclear industry	
Food	Minister of Agriculture and Food Quality
Health	Minister for Health and Sport
Finance	Minister of Finance
Public order and safety	Minister for the Interior Minister of Defence Minister of Foreign Affairs
Public administration	
Legal order	Minister of Justice
Dams and surface water management	Minister of Transport, Public Works and Water Management
Transportation	

Table 4. The breakdown of CI by sector in the United Kingdom of Great Britain and Northern Ireland. Source: Own compilation based on *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, 2010.*

Sector	Competent authority
Energy	Minister of Energy and Climate Change
Communications	Minister of Business, Innovation and Skills Minister of Culture, Media and Sport
Water	Minister of Environment, Food and Rural Affairs
Food	Minister of Environment, Food and Rural Affairs Food Standards Agency
Health	Minister of Health and Sport
Finance	Chancellor of the Exchequer
Emergency services and health protection	Home Secretary Secretary of State for Health Secretary of State for Communities and Local Government
Public administration	Cabinet Office Secretary of State for Communities and Local Government
Transportation	Minister of Transport

In addition, as part of the "top-down" approach, the authors of the guidebook "Good practices manual for CIP policies for policy makers in Europe" offer three methods for differentiating CI from other infrastructures. Firstly, the service-based method uses criteria for specifying the level of service required, e.g. number of Megawatts delivered. Secondly, the operator-based approach focuses on identifying critical operators who subsequently determine which specific assets (services) are part of CI. Thirdly, the asset-based approach uses elements of both methods described above.[44]

[44] *Good practices manual…*, op. cit., p. 16.

What is common to the "bottom-up" and "top-down" approaches is the use of criteria. The attempt to determine CI solely on the basis of confronting it with its definition, especially taking into account a universal character of those definitions, would be laden with too high uncertainty as to the final outcome. Therefore, the most frequently applied are the cross-cutting criteria that refer to the consequences of either destruction or disruption of the functioning of a given facility, service or operator. These criteria usually correspond to the definition of CI[45] and the state's engagement domains indicated therein as well as the state's reaction capabilities to the consequences of destruction or disruption of CI.

Other types of measures applied are sectoral criteria which serve, as it was mentioned earlier, to determine the level of demand for a given service or to specify the thresholds for the preliminary selection of infrastructure in a given sector, thus lowering the number of potential CIs in the long term. Both cross-cutting and sectoral criteria can be illustrated quantitatively (numerically) or qualitatively (descriptively). The advantage of quantitative criteria is their objectivity while their biggest disadvantage is little flexibility, which, in effect, can lead to overlooking sub-threshold, yet critical, assets in the selection phase. Conversely, the advantage of qualitative (descriptive) criteria is greater sensitivity to seemingly negligible details that are impossible to quantify. Their main drawback, however, lies in the description tending to leave too much room for interpretation, thus making it impossible for the participants of the identification process to reach an agreement over the infrastructure assessment.

In practice, to compensate for potential errors in the identification of CI, a combination of both types of criteria and ways to present them is used. This, however, fails to resolve one of the most serious problems in the identification process, i.e. a lack of access to credible information to compare the value of an assumed parameter with a threshold. This refers predominantly to cross-cutting criteria, presented both quantitatively and qualitatively. In practice, if no data on historical events are available, the verification whether criteria are met is based, out of necessity, on estimates that are more or less erroneous. What we often cannot determine, however, is how erroneous these estimates are.

In Poland, a "top-down" approach was used to identify CI, focusing on services provided by systems of infrastructures cited in the definition of CI.[46] Where possible, both sectoral and cross-cutting quantitative criteria as well as a definition of CI were applied. As set out in the NCIPP, the procedure for identifying CI involves:[47]

1. In phase one – systemic criteria relevant for a given CI system should be applied to the system's infrastructure in order to make the initial selection of objects, installations, facilities and services that could be potentially considered as CI in a given system

[45] In the case of countries which do not use definitions, the cross-cutting criteria refer to assumed values that are subject to protection.

[46] Article 3(2) of the Act of 26 April on Crisis Management mentions the following critical systems: energy, fuel and energy resources supply, communication, Information and Communication Technology networks, financial, food and water supply, health care, transportation, emergency services, systems ensuring the continuity of public administration activities; systems for production, storage and use of chemical and radioactive substances including pipelines transporting dangerous substances.

[47] *The National Critical Infrastructure*…, op. cit. pp. 11–12.

2. In phase two – a definition included in the Article 3(2) of the Act on Crisis Management should be applied to the infrastructure identified in phase one in order to investigate whether an object, facility, installation or service is critical for the security of the state and its citizens, and whether it aims to ensure a smooth functioning of public administration bodies, including public institutions and companies

3. In phase three – in order to assess potential consequences of destruction or incapacitation of potential CI, cross-cutting criteria should be applied to the infrastructure identified in phase one and two. It is required, however, that the potential CI must meet at least two cross-cutting criteria.

It needs to be noted that despite concentrating on services provided by infrastructure, it is mostly specific, physical objects that have made it to the uniform list of assets, installations, facilities and services comprising CI. Facilities that are managed by specific owners and have a definite location allow a still young system of CI protection to be easily implemented. Given Polish conditions, a postulated (and exercised) practice of some countries (e.g. France) of indicating entire systems (e.g. power system) or even processes as CI currently appears to be too sophisticated. The system (process) understood as e.g. a supply chain, can be implemented in numerous locations and have multiple owners. It would generate specific problems, also of legal nature. The issue of dependencies and co-dependencies is similarly problematic. Currently, it is much easier to determine them for the specific physical resource rather than for the system or process. It is quite plausible, however, that together with the development of the CI protection system and the maturity of its participants, a change will occur in this area.

Having defined and identified CI, the next step is to ensure its protection. There are at least two methods of protecting CI: procedural and structural. The procedural approach involves establishing a system to protect these facilities. This solution can take two forms: a mandatory or voluntary participation in the protection system. The structural method assumes the lowering of criticality of infrastructure. This effect can be achieved by either further enlarging infrastructure in order to lead to a situation of purposeful superfluity (redundancy) or by bringing closer, geographically-wise, a selected infrastructure to citizens.[48] The concept of "bringing closer" the infrastructure assumes that an individual citizen or smaller groups of citizens have access to infrastructure that allows them to be independent of services being provided by a more distant infrastructure. Hence, from the point of view of the state, some services could become less critical as this group of citizen would become more resilient and independent of CI. This model increases the possibility for a potential response of the civil service to a disruption of a closer infrastructure as well as creates a situation in which the number of citizens affected at any time is radically lower. The examples of such infrastructure could be individual renewable energy sources (solar, wind) or on-site wastewater treatment systems. The concept assumes that local and district infrastructures are built to serve a smaller number of residents at a time in towns and densely populated areas.[49] In both infrastructure protection models, the challenge lies in

[48] M. Bennett, V. Gupta, op. cit.

[49] It was once suggested that a biogas plant should be built in every Polish town. This idea, regardless of its political aspects, fits in perfectly with the above-mentioned concept and should be considered as an interesting voice in the discussion about the means to enhance the resilience of both the state and its citizens to crisis situations. We also disregard the fact that in a mutually connected infrastructure system, a change in only one of them is likely to shift the threshold of "criticality" in another system.

finding an answer to the question of who should be implementing specific solutions and at the same time take on the financial burden. Does the responsibility for ensuring civil protection against the consequences brought about by the disrupted CI lie within entities that either own or manage the infrastructure, or is it the responsibility of the state?

In Poland, a draft bill on crisis management was produced by drawing on experiences and examples of countries in which the building of the infrastructure protection system that was key to the security of the citizens and the functioning of the state had begun earlier, namely the United States of America, the United Kingdom of Great Britain and Northern Ireland, the Kingdom of the Netherlands, the French Republic and the Federal Republic of Germany. The common characteristics of the CI protection system in the above-mentioned countries include:

- criteria-based identification of CI and appointing its owner or operator as the entity responsible for its protection
- division into sectors (products or services) that are critical for the functioning of the state, society and economy
- identification of administrative bodies responsible for the coordination of activities in a given sector
- the necessity to develop facility protection plans by either a CI owner or manager
- the cooperation between CI owners, operators and competent authorities responsible for both the coordination of activities in a given sector and civil protection and crisis management.

Taking into account Poland's specific character and legal culture, a regulatory solution has been chosen that puts particular emphasis on the procedural method and a mandatory participation in the CI protection system. In other words, provisions of the Act on Crisis Management literally indicate an obligation to protect CI by its owners as well as sole and dependent proprietors, to draw up protection plans and to appoint a person responsible for contacting administration. Conversely, the regulation of 30 April 2010 on Critical Infrastructure Protection Plans[50] specifies in detail the contents of plans as well as the procedure and schedule for their negotiation and authorisation (this mechanism allows administrative bodies to have a real influence on the contents of plans and a specific CI facility security system). This solution is based on a French model[51] which assumes

- appointing a CI operator and its obligation to protect it
- the obligation to draw up the Operator Security Plan
- sanctions for CI operators who fail to execute the imposed obligations
- the obligation imposed on the public administration to draw up an External Security Plan (originally, the Act on Crisis Management imposed an obligation to draw up the National Critical Infrastructure Protection Plan (NCIPP) as well as Provincial Critical Infrastructure Protection Plans (PCIPP))
- specifying which sectors are considered critical due to their key importance to social and economic processes

[50] Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Law, No. 83, item 542).

[51] More about the French system and the systems used in other European countries in: *Study: Stock-Taking Of Existing Critical Infrastructure Protection Activities*, http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_stock_taking.pdf, [accessed: 08/04/2014].

However, in contrast to the solution implemented in France and the Act of 22 August 1997 *on the protection of people and property*[52], no sanctions have been envisaged for failure to fulfil obligations specified. The effectiveness of this solution appears to be unsatisfactory. A repressive character of this approach has its side-effects – namely, a deep reluctance of executors towards tasks imposed and, as a consequence, attempts undertaken by them to either evade the execution of imposed obligations or perform them at minimal cost. On the other hand, it forces the administration to build structures whose aim is to conduct control activity and proceedings in case of breaches of obligations. It denotes a necessity to employ highly-qualified workers, which poses a serious challenge in the area related to protection, and incurs significant financial outlay. The assumption that underpinned the approach was that the increase of the effectiveness of CI protection could only be achieved through operators activity being supported by the capacity and potential of public administration. At the same time, it was based on a belief that motivation[53] to sustain business continuity is a more effective tool than sanctions to achieve a high level of protection.[54] CI operators are equipped with the best knowledge and tools to diminish threats that affect their activity. They are also capable of making the shrewdest choice of strategy to minimise the effects of these threats. This approach does not envisage sanctions for failure to fulfil the obligations specified in the Act. The absence of sanctions is not tantamount to the absence of responsibility. Owners, sole and dependent proprietors who consciously fail to fulfil their obligation to protect CI expose their employees and other people to a direct risk of losing their lives or suffering from severe health consequences, which may result from a disrupted functioning of CI and be subject to punishment of imprisonment for up to 3 years (Article 160, paragraph 1 of the Penal Code).

In 2009, amendment to the Act on Crisis Management was made on the basis of experiences gathered in the period when the Act had been in force. In essence, the CI protection model has not changed significantly; however, the emphasis has been shifted towards the CI owners (managers). The obligation to develop NCIPP and PCIPP has been abolished; instead, a requirement to develop National Critical Infrastructure Protection Programme – a document that consolidates the efforts for CI protection helping both CI operators and administration, has been introduced. Moreover, having adopted the principle of joint responsibility and the

[52] The Act of 22 August 1997 on the protection of people and property (Journal of Laws of 2005, No. 145, item 1221 with further amendments).

[53] Motivation is a process that elicits, channels and sustains specific human behaviour amongst other,alternative forms of behaviour in order to achieve certain goals. One of the theories of work motivation developed by Douglas McGregor (Massachusetts Institute of Technology) assumes the existence of two contrasting sets of theories: X and Y. Theory X assumes that an average human being inherently dislikes work and will avoid it if they can. They will work only to satisfy their material needs. According to Theory Y, people are mostly creative, with great imagination and ingenuity. In appropriate conditions, such people are not only responsible but they also expect that they will be given a responsibility for performing a task or doing work. According to McGregor, external motivating conditions such as reward and punishment, lower intrinsic motivation. It is due to a change in the perception and placement of reasons for action (outside rather than inside of a subject) as well as a weakened sense of authorship associated with it and a limited personal impact on the situation.

[54] Disclosed incidents of security breaches seem to corroborate the fact that the occurrence of sanctions does not warrant effectiveness of the system that is supposed to protect key assets: Bełchatów, 3 July 2007: Greenpeace activists trespassed on the premises of the power plant and climbed a cooling tower on which they painted "Stop CO2"; Konin, 3 December 2008: environmental activists trespassed on the premises of the power plant, climbed a tower and started protesting against greenhouse gas emissions; France, 5 December 2011: Greenpeace activists burst into four nuclear power plants. In Nogent-sur-Seine, it took them only 15 minutes to get to the nuclear reactor. This diagnosis appears to be corroborated by the reports being submitted to the Government Centre for Security by plenipotentiaries for critical infrastructure protection, appointed as part of implementation of the Act of 18 March 2010 on Specific Rights Vested in the Minister in Charge of State Treasury the exercise of such powers in certain capital companies or capital groups conducting business activities in electric power, crude oil and gas fuel sectors (Journal of Laws No. 65, item 404).

effectiveness of cooperation[55], in the amended Act the obligations resulting from the requirements of CI protection have been divided anew between the public administration and CI operators. The duties of operators include:

1. CI protection by means of preparing and implementing, in line with the foreseen threats, critical infrastructure protection plans as well as maintaining own emergency systems that ensure the security and sustain the functioning of this infrastructure until it is fully restored (Article 6(5) of the Act) as well as

2. appointing a person responsible for maintaining contacts with entities competent for the CI protection (Article 6(5a) of the Act).

Conversely, the administration is obliged to include tasks associated with CI protection in the crisis management plans at every administrative level; in the case of levels below national, those tasks can be included in the plans on condition that CI is located in the area covered in the plans[56]. In addition, as part of the civil protection against the consequences associated with critical infrastructure failures, it ensures there is a system of support for operators that aims to shorten the time required to restore services (tasks, functions) being delivered by CI.

When analysing solutions adopted in Poland[57], one can make an observation that they have answered at least several earlier questions. Does this mean, however, that the adopted model has proven successful? Currently, it is impossible to provide an unequivocal answer to the posed question as there is still too little credible data at our disposal. The experiences of the Government Centre for Security are promising, but the real test will be the quality evaluation of CI protection plans that have just started pouring in for authorisation.

Summary

Today, it is impossible to imagine our life without the surrounding infrastructure and solutions it carries with it. Bringing technical novelties practically on a daily basis, the pace of technological development has ceased to surprise us while the resulting popularity and usefulness of services have made us addicted to them. However, the questions that man has to answer in the 21st century are not whether these changes are reasonable, but how to survive in the technology-saturated world? How to enjoy the achievements of modern times and at the same time not fall prey to them?[58] Becoming aware of new threats, man increasingly turns to the state with expectations to reduce the risk of their occurrence. Due to the immensity of infrastructure, its cross-border and ubiquitous character, it is states and international organizations that are predisposed to take on themselves this responsibility. One of the tools that allows us, at least partially, to control the threats is CI. Reducing the risk of a situation where services

[55] More in: *The National Critical Infrastructure…*, op. cit.

[56] Article 5, Paragraph 2(3) (k) and (l) of the Act on Crisis Management.

[57] More in: Act of 26 April 2007 on Crisis Management (Journal of Laws of 2013, item 1166) along with executive orders and the *National Critical Infrastructure Protection Programme.*

[58] According to Bennett and Gupta, the disruption of a centralised infrastructure may have far more greater consequences than primary threats.

supplied become dysfunctional was possible due to drawing attention to sensitive elements in the human environment as well as determining their specific traits, which, in consequence, led to creating dedicated solutions.

Every solution has its limitations. Also those adopted in Poland. Despite a very recent implementation of the Act on Crisis Management, Poland has a complementary and widespread CI protection system. Deliberations presented in this chapter show unambiguously that much has been done already, but there is still a lot of work ahead of us.

In the case of Poland, supplementing the definition of CI so that it leave no room for doubt whether it encompasses virtual (information) infrastructure, e.g. collection of information from databases, is also worth considering. In the definition that is currently in force, the system and mutually bound functional objects contained therein, including constructions, facilities, installations and services are not unequivocally indicated.

Therefore, we need to pursue the abandoning of sectoral criteria as postulated in the National Critical Infrastructure Protection Programme, thus bringing it closer to the "bottom-up" approach. Taking into account the difficulties in applying this approach, the local administrative units and CI operators should be encouraged to engage in the identification of CI as part of the currently binding procedure. It would allow for minimising the possibility of ignoring CI that fails to meet the criteria.

In order to obtain information and historical data about the effects of infrastructure disruption that have occurred, it would be recommendable to tighten the cooperation between local administrative units, CI operators and other entities (e.g. market regulators), organisations (e.g. non-governmental), services and guards, which would allow the criteria to be more adequately calibrated, thus making them more suited to real conditions.

If the currently applied, voluntary approach to cooperation turns out to be ineffective, a more formalised solution based on the compulsory collaboration with the Government Centre for Security should be considered.

2. Legal determinants of critical infrastructure protection

Agnieszka Wiercińska-Krużewska, Piotr Gajek
– WKB Wierciński, Kwieciński, Baehr

Legislation regarding critical infrastructure (CI) protection has been embedded in numerous legal acts of a statutory and sub-statutory rank, encompassing various areas related to the functioning of the state[1]. Although these acts do not apply directly to CI, the analysis of the terminology used, including terms referring to facilities, demonstrates that the meaning they convey is often similar if not identical[2]. This applies to such fields of activity as telecommunications, fuel and power production and trade, performance of defence-related tasks by entrepreneurs, strategic reserve accumulation, the rights vested in the minister in charge of State Treasury or the protection of persons and property[3]. The above cited examples corroborate the fact that the formal and legal conditions for CI protection existed before 26 April 2007 when the Act on Crisis Management[4] (the Act) was enforced.

The Act introduced the concept of CI and comprehensively regulated the issue of CI protection. As set out in the Act, CI shall be understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises (Article 3(2) of the Act). In total, CI comprises 11 systems (facilities and installations) that are indispensable for sustaining the basic functioning of the economy and the state, namely

- energy, energy resources and fuel supply
- communication

[1] The following legal acts can be quoted as examples: the Act of 22 August 1997 *on the protection of persons and property*; the Act of 23 August 2001 *on the organisation of tasks for the defence of the state being executed by entrepreneurs*; the Act of 16 July 2004 *Telecommunications Law*; the Act of 10 April 1997 *Energy Law*; the Act of 9 June 2011 *Geological and Mining Law*; the Act of 3 July 2002 *Aviation Law*; the Act of 29 October 2010 *on strategic reserves*; the Act of 18 March 2010 *on specific rights vested in the Minister in charge of State Treasury* and the exercise of such powers in certain capital companies or capital groups conducting business activities in electric power, crude oil and gas fuel sectors; regulation of the Council of Ministers of 24 June 2003 *concerning facilities of particular importance to the defence and security of the state and their particular protection*. Since a detailed discussion of the above identified legal acts goes beyond the scope of the present study, it presents the legal conditions resulting in particular from the Act of 26 April 2007 *on Crisis Managemen*t.

[2] W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona Infrastruktury krytycznej* [Critical Infrastructure Protection], National Defence University of Warsaw, Warsaw 2012, p. 37.

[3] K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce* [Selected legal instruments for protecting critical infrastructure in Poland], Bezpieczeństwo Narodowe 2011, no 3, pp.181-197.

[4] The Act of 26 April 2007 on *Crisis Management* (Journal of Laws of 2013, item 1166).

- Information and Communication Technology networks
- financial systems
- food supply
- water supply
- healthcare
- transportation
- rescue
- systems ensuring the continuity of public administration activities
- systems for production, storage and use of chemical and radioactive substances including pipelines transporting dangerous substances.

CI protection should be understood as activities aiming to ensure the functionality, continuity and integrity of CI in order to effectively counteract threats, risks and weaknesses as well as to curtail and neutralise their effects; it also assumes taking a swift action to reconstruct the infrastructure in the event of a failure, attack or any other event that disturbs its normal functioning.

In order to implement the assumptions underlying the Act, the entity in possession of CI should actively seek to maintain it in a proper condition, protect it against damage and people who could compromise the safety of the state. These entities should also make investments to continuously enhance CI and its state.

Activities of CI owners should be centrally coordinated not only when a threat occurs, but also when duties related to CI maintenance ensuring the performance of tasks by the state in crisis situations are executed.

Since CI protection is one of the state's priorities, the state should introduce mechanisms allowing for

- monitoring and updating the list of CI's components
- establishing mutual relationships between the components of CI
- establishing mutual relationships between the CI administrators
- launching initiatives for CI protection
- running educational campaigns to raise awareness of the role of CI in ensuring the security of the state
- supporting CI owners by participating in costs of CI construction, maintenance and protection.

The absence of the above-said mechanisms in place may lead to poor knowledge about the importance of CI for the security of the state, chaos when coordinating activities, reluctance of private entities to cover the CI-related costs.

Only developing a suitable support system for entities participating in CI maintenance warrants the creation of an effective system of sanctions. The support elements provided to these entities should include:

- a formal platform for exchanging experiences and knowledge about CI protection
- a public-private partnership
- special-purpose funds

- facilitating the use of legal acts, e.g. the use of the Public Procurement Act
- activities aimed at supporting the self-regulation of enterprises in possession of CI with regard to the flow of information and incurring financial outlay on CI protection and maintenance.

The Supreme Audit Office (Najwyższa Izba Kontroli, NIK) has, on several occasions, audited various government bodies and their performance of duties imposed by the Act (latest audit results by NIK dated 20 June 2013). Audits conducted by NIK have demonstrated a number of irregularities concerning the implementation of the statutory tasks since the enforcement of the Act and its amendment in particular. NIK concluded that CI protection is to a large extent based on *ad hoc* activities. According to NIK, the creation of the effective CI protection system will take time to complete taking into account the necessity to update crisis management plans regarding the implementation of CI-related tasks at the ministerial and provincial levels as well as the need to develop protection plans of individual CI facilities by the operators.

The conclusion drawn by NIK is valid, but the cause for it appears to lie elsewhere than the lack of regulation and basis to carry out further work. The necessary framework was created in 2013 with the emergence of the "National Critical Infrastructure Protection Programme."

The European Union Level

The European programme for critical infrastructure protection / Directive

The 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* (Directive)[5] is the backbone of the European Programme for Critical Infrastructure Protection (EPCIP). This document for the first time introduces definitions of CI to EU law, European Critical Infrastructure (ECI), CI protection, and the concept of the ECI owner (operator). The main purpose of this legal act is to establish the means to identify and designate ECI as well as define fundamental duties imposed on the Member States (and indirectly on CI owners) with regard to ECI protection.

In the Directive, it is already clearly emphasised that *"the primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures" and "given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach needs to encourage full private sector involvement."* At the same time, the Directive points to the ICT sector as a future priority in the area of CI protection. The European Commission itself devotes plenty of attention to the above indicated sector[6], which is reflected in the documents it issues, including

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on Critical*

[5] OJ of the EU of 23 December 2008, L 345/75.

[6] T. Szewczyk, *Europejski program ochrony infrastruktury krytycznej* [The European programme for critical infrastructure protection], Przegląd Bezpieczeństwa Wewnętrznego 6/12, pp.157–168.

Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"[7](Communication)

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on Critical Information Infrastructure Protection* "Achievements and next steps: towards global cyber-security"[8] and
- proposal for a Directive of the European Parliament and of the Council *concerning measures to ensure a high common level of network and information security across the Union*.[9]

It is necessary to indicate that neither the Directive nor any of the remaining documents mentioned above contain any direct regulations regarding legal instruments that Member States could use to encourage private sector entities to participate actively in CI protection initiatives.

ENISA – a public-private partnership

In parallel to EPCIP, activities are carried out in line with the plans included in the Communication where it was emphasised once again that although the ultimate responsibility for defining the CII (Critical Information Infrastructure) policy lies with Member States, its implementation relies essentially on the engagement of the private sector which either owns or controls a large number of CIIs. On the other hand, markets do not always sufficiently incentivise the private sector to invest in the protection of CIIs at the level that would match the expectations of governments.[10]

In the Communication, it is said that *"to address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a European level, European PPPs have not materialised so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA*[11]*, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground."*[12]

In order to support models promoting cooperation based on PPP, ENISA has issued a guide on the effectiveness of good practices in this area (the Guide). The Guide demonstrates that

- state authorities lack sufficient financial resources that are indispensable for providing effective CI protection
- ensuring such protection requires mechanisms to be created to allow for engaging the private sector.[13]

[7] COM (2009) 149 final, 30/03/2009.

[8] COM (2011) 163 final, 31/03/2011.

[9] COM (2013) 48 final, 07/02/2013.

[10] COM (2009) 149 final, 30/03/2009, section 3.4.2.

[11] European Union Agency for Network and Information Security.

[12] COM (2009) 149 final, 30/03/2009, section 3.4.2.

[13] ENISA, *Cooperative Model for Effective Public Private Partnerships Good Practice Guide*, 2011, p. 18.

It is precisely this document which for the first time has indicated premises that can be perceived as an indirect incentive to promote active collaboration between private and public sectors for the protection of CI (as part of the public-private cooperation) which involves

- the reduction of the risk of exposing CIIs to damages which generate costs for CI operators and owners
- the reduction of administrative costs necessary to perform duties related to ensuring adequate standards of CII protection
- ensuring access to specialist knowledge on CII protection
- significant impact on giving a final shape on the CI protection policy of Member States, including the formulation of duties imposed in this respect on entities operating in the private sector (CI operators and owners).

The above premises should be treated as general assumptions that intend to support Member States in implementing more concrete solutions that promote PPP nationally.

The National Level

The Act on Crisis Management

The Directive should have been implemented in the national legal orders until 12 January 2011. Poland has implemented the Directive by means of the Amendment to the Act of 26 April 2007 *on Crisis Management*[14], which constitutes a principal legal act concerning CI protection. As it was mentioned in the introduction, independently of the Act, the Polish legislator has also included special provisions that indirectly regard the protection of CI in other legal acts regulating specific sectors of the economy, such as telecommunications[15] and aviation[16].

In the area of CI protection, the Act specifies tasks that include the collaboration between the public administration and the owners and operators of sole and dependent CI objects, installations, and facilities. The Act requires the CI owners and operators of sole and dependent CI objects, installations and facilities to protect them through the preparation and implementation, proportionally to projected threats, of CI protection plans as well as the maintenance of their own backup systems ensuring security and sustaining the functioning of this infrastructure until full reconstruction. On the other hand, the government (the Council of Ministers) was required to adopt "The National Critical Infrastructure Protection Programme" (NCIPP, Programme). The Programme was adopted on 26 March 2013.

At the same time, it needs to be noted that similarly to legal acts at EU-level law, Polish legislation does not introduce any concrete regulations that could be directly classified as instruments incentivising the private sector to systematic enhancement of the standards of CI protection, which may impair the maintenance and development of CI. Also in this case, such instruments can potentially be found in "lean" documents.

[14] The Act of 29 October 2010 on *Amendment to the Act on Crisis Management* (Journal of Laws of 2010, No. 240, item 1600).

[15] The Act of 16 July 2004 *Telecommunications Law* (Journal of Laws of 2004, No. 171, item 1800).

[16] The Act of 03 July 2002 *Aviation Law* (Journal of Laws of 2002, No. 130, item 1112).

The National Critical Infrastructure Protection Programme (NCIPP)

In the Programme, it is highlighted that the majority of CI is operated by private entrepreneurs, independent of the public administration. The Programme provides the framework for the collaboration of the public administration and CI operators in order to ensure the operational continuity of CI, thus protecting the economic and social foundations of our country. The Programme sets out mechanisms for the development of partnership relations between public administration and CI operators in the area of CI protection.[17] Considering the above and the obligation imposed on the CI operators by the Act, the Programme also targets these entities, in particular their boards of directors. Every new CI operator automatically becomes a target recipient of the Programme. CI operators participate in activities that protect CIs described in the Programme.

The Programme underscores that one of the key elements ensuring smooth and comprehensive protection of CI is the cooperation between the private and public sectors[18] as well as the intrasectoral collaboration with the particular emphasis being put on the cooperation between the representatives of individual systems within the private sector. An important element of this collaboration involves developing transparent principles and procedures to be used by the state authorities and services as well as the owners and operators of sole and dependent CI objects, installations and facilities.[19] It needs to be emphasised, however, that the PPP[20], within the meaning of the Programme (the scope of CI protection), specifies only the type of collaboration between public administration units and private entities that may involve e.g. the exchange of information that can potentially affect the achievement of NCIPPs objectives. This partnership, however, does not provide for entering into any agreement on the basis of which a private partner would be paid to execute a project to the benefit of the public body.[21]

It is therefore justified to clearly distinguish the naming convention used to describe both forms of cooperation, i.e. the public-private cooperation as set out in NCIPP, and the collaboration in the form of PPP and within the meaning of the Act on Public-Private Partnership[22] (the PPP Act). It appears that apart from the cooperation set out in the NCIPP and understood as an information exchange process, the PPP within the meaning of the PPP Act could significantly supplement the system of CI protection. Further down this article, the public-private partnership within the meaning of NCIPP will be referred to as “PPC” whereas the public-private partnership within the meaning of the Public-Private Partnership Act will be referred to as “PPP”. Taking into account the fact that the discussion about the PPP exceeds the scope of the present publication, it will not be subject to detailed analysis in this article.

[17] *The National Critical Infrastructure…*, op. cit. p. 6.

[18] More on the prospects of the public-private cooperation in Poland can be found in Chapter 3: *Effective public-private cooperation - success factors*.

[19] Government Centre for Security, http://rcb.gov.pl/?page_id=257, [accessed: 12/06/2014].

[20] It is about a public-private partnership denoted in the National Critical Infrastructure..., op.cit. p. 33. (cooperation).

[21] *The National Critical Infrastructure…*, op. cit. p. 33.

[22] The Act of 19 December 2008 *on Public-Private Partnership* (Journal of Laws of 2009, No. 19, item 100).

It appears, however, that the participation in the Programme should already be considered as a form of an incentive for private sector entities to actively engage in cooperation for CI protection. In particular, the entities would be strongly encouraged to actively engage in the activities of the specialist PPC forum established for the purposes of the Programme.[23] The key objectives of such a forum would include

- the creation of a platform that facilitates the exchange of opinions and collaboration on sensitive issues regarding CI protection
- submitting and developing new legislative solutions regarding CI protection
- the exchange of opinions and observations between interested parties at an early stage of CI legislative work
- the organisation of workshops, seminars and conferences devoted to CI protection
- the creation of a database of professionals specialising in CI protection in various systems: financial, communications, ICT networks, the supply of energy, energy resources and fuels, etc.

It appears that in such a scope, the PPC forum, created under the Programme, will to a large extent replicate the fundamental assumptions defined in the Guide. As a consequence, it will also become a vital instrument to motivate private sector entities to undertake activities aiming to enhance standards for CI protection. The work done within the forum will contribute to the creation of a database of professionals specialising in issues related to CI in various systems: financial, communications, ICT networks, the supply of energy, energy resources and fuels, etc. Such experts will cooperate with the government, e.g. during work undertaken on the EU forum in order to discuss EU legislative proposals with the private sector. The establishing of a specialist database will accelerate the consultation process and at the same time it will allow the members of the public administration to take advantage of the experience and expertise when their knowledge is insufficient.[24]

Hence, the entities participating in the forum will be able to

- conduct an active dialogue on shaping the principles of CI protection
- exert an influence on the shaping of final solutions implemented in the above area, and
- consult experts on an ongoing basis.

It appears that the PPC forum could contribute to

- developing clear and transparent rules and procedures for action as well as the exchange of information between state authorities and private partners
- developing uniform and compatible methods of collecting and processing information on CI threats
- developing and implementing procedures to counteract CI threats when they occur
- identifying the means and mechanisms of CI protection and reconstruction
- developing optimal methods for ensuring the protection of data received from private entities; maintaining backup systems
- developing procedures to prevent disturbances in the functioning of CI as well as to prepare CI for crisis situations that may adversely affect it.

[23] More on the management methodology, organisational structure, financing and communication within such fora can be found in Chapter 4: *The methodology of governing collaboration forums for critical infrastructure protection*

[24] Government Centre for Security, http://rcb.gov.pl/?page_id=257, [accessed: 12/06/2014].

In order to perform the above presented tasks and achieve expedient results, it is necessary to undertake a number of educational, planning, coordinating and legislative activities. In the first instance, it is the Government Centre for Security that should undertake these activities. In conjunction with the fact that the NCIPP was only developed in March 2013, which was criticised for instance by the Supreme Audit Office, it is difficult to estimate if these activities will be undertaken expeditiously. In accordance with the information made public by the Government Centre for Security, the list of infrastructure elements has been created and is being updated. However, since access to it is heavily restricted, it is difficult to estimate its completeness. Currently, the very fact of establishing the Programme and creating the list of CIs allows for further work to begin that would regulate in detail the mechanisms of effective CI management and protection.

Financing CI protection activities in Poland

The Programme emphasises that activities related to the protection of CI are funded with the own resources of the Programme participants and planned in their budgets (in the case of CI operators it is regulated under Article 6 of the Act). Both the Programme and the Act do not directly indicate that CI owners and operators can seek the refinancing of costs incurred for CI from the state budget or the EU.[25]

Amongst the instruments used to indirectly finance activities related to CI protection, the Programme mentions a 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"[26] – CIPS. The aim of the CIPS was to provide financial support from the EU budget of activities undertaken, inter alia, in the area of CI protection such as

- stimulating, promoting and supporting risk assessments of CI in order to upgrade security systems
- stimulating, promoting and supporting the development of methodologies for the protection of CI, particularly the risk assessment methodologies
- promoting and supporting the development of security standards as well as the exchange of know-how and experiences regarding the protection of people and CI
- promoting and supporting the Community-wide coordination and cooperation on the protection of CI.

At the same time, the entities from the private sector could also become the beneficiaries of CI protection projects under CIPS by applying for suitable funding of initiatives that are consistent with the fundamental objectives of the programme. The CIPS programme was established in the period from 1 January 2007 to 31 December 2013; currently, it is supposed to be partially replaced with the Internal Security Fund, a financial instrument designed to support law enforcement cooperation and crisis management as well as to prevent and combat crime (ISF).[27]

[25] This issue was already highlighted in 2006 in the Study of the Ministry of Infrastructure; cf. R. Piwowarczyk, *Ochrona Infrastruktury Krytycznej* [Critical Infrastructure Protection].

[26] OJ of the EU of 24/02/2007, L 58/1.

[27] Currently, the work is under way on the Regulation of the European Parliament and of the Council aiming to set up a financial instrument

Amongst the potential indirect sources of financing for CI projects, the CI operators may apply from national operational programmes which use the EU funds[28] (the new Financial Perspectives 2014-2020 or the EU level financial instrument "Connecting Europe Facility" (CEF)).[29] In terms of objectives related to telecommunications network infrastructure, the CEF mentions, inter alia, the supporting of critical telecommunications infrastructures.

It needs to be noted that apart from information exchange on threats and a broadly understood public-private cooperation, a key question remains on how to ensure the private sector takes action to protect the CI it owns which exceeds the basic measures involving exclusively the protection of its own resources. A valid question that is being raised is who should be responsible for the security of CI if the private sector is insufficiently motivated to invest in CI security while the state does not undertake any initiatives in this area.[30]

What is being emphasised is that shareholders have little financial incentives to invest in the security of CIs that exceeds their stake in a given organisation; hence, private entities support investments in CI security only to the extent they find necessary and profitable. It seems therefore that the market itself does not provide sufficient incentives to effectively protect CIs.[31] For instance, it is said that the necessity to reduce costs and ensure security in the energy industry may lead to contradictory objectives in the public policy and insufficient incentives for private entities to invest in increased infrastructure protection.[32] Conversely, given the threats we face today, relying exclusively on best practices and internal regulation introduced by individual sectors (self-regulation) may turn out to be insufficient.[33]

Introducing certain requirements in given sectors by private entities is a practice that allows for increasing industry standards. Self-regulation is a means that enables minimum legal requirements to be exceeded, but it can also strengthen the understanding and conformity with the currently binding provisions. In a competitive environment, intrasectoral cooperation proves a strong incentive for enterprises to continually improve and raise standards in order to gain their market share. Introducing certain requirements by private entities voluntarily enables the state to avoid imposing obligations and responsibilities on them.

The above can also refer to the context of CI protection and security; therefore, private and sector-specific entities that are in possession of CI should be encouraged to introduce self-regulation in this regard.

Attention should be given to the need for developing additional, stronger incentives for a more active engagement of the private sector in the protection of CI. Potential instruments that the state can utilize to this end have been mentioned in Chapter 3 of the present report: tax

within the framework of the Internal Security Fund to support police cooperation, prevent and combat crime, and crisis management.

[28] From the Cohesion Fund and the European Regional Development Fund in particular.

[29] *Connecting Europe Facility*, http://ec.europa.eu/digital-agenda/en/connecting-europe-facility, [accessed: 12/06/2014].

[30] P. Auerswald, L.M. Branscomb, Todd, M. La Porte, E. Michel-Kerjan, *The Challenge of Protecting Critical Infrastructure, Risk Management and Decision Process Center*, Wharton University of Pennsylvania, Working Paper # 05-11, October 2005, p. 4.

[31] S. Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, Matthew B Ridgway Center for International Security Studies, Pittsburgh, United States, 2005, p. 15.

[32] CEPS, Task Force Report, *Protecting critical infrastructure in the EU*, Brussels 2010, p. 73.

[33] Ibidem, p. 15.

incentives, subsidies (grants), insurance discounts, certification of companies, and preferential loans. Incentives for undertaking "bottom-up" activities by private entities from individual sectors should also be introduced (self-regulation) in order to develop and observe certain standards and solutions for CI protection and security.

It appears that the effectiveness of the CI protection system would be considerably enhanced if it comprised the above-mentioned elements, i.e. a broadly understood public-private cooperation (PPC) including information exchange, self-regulation of individual sectors, and fiscal or parafiscal incentives.

The direction of changes concerning the CI protection requirements

The approach to CI protection so far has been predominantly based on a voluntary cooperation between the private and public sectors. In the new EU-level legal regulations, a shift towards a regulatory approach can be observed. It is particularly true of the proposal for a Directive of the European Parliament and of the Council *concerning measures to ensure a high common level of network and information security across the Union*[34] (the NIS Directive). The aim of the proposed directive is to ensure a high common level of network and information security. The work on creating a final version of this legal act is still in progress.

In the proposal of the NIS Directive, the European Commission adopted a regulatory (sanction-based) approach recognising that the voluntary approach followed so far had resulted in diversified preparedness and limited collaboration. It was concluded that the current situation in the EU, reflecting the purely voluntary approach, does not provide sufficient protection against network and information security incidents and risks across the EU.

According to the Commission, it is highly unlikely that all Member States should achieve nationally a comparable level of capabilities and preparedness indispensable for enhancing security, cooperation and the exchange of sensitive information at the EU level, by relying on voluntary activities of the Member States and private entities.

As part of the regulatory option proposed in the NIS Directive, the competent national authorities and CERTs are supposed to constitute an element of a collaborative network at the EU level. Within this network, national authorities and CERTs would exchange information and collaborate in order to combat threats and incidents affecting the security of networks and information in accordance with the European cyber incident contingency plan and the European cooperation plan that would need to be agreed upon by Member States. The Commission intends to put an obligation on all Member States to have in place a minimum level of national capabilities (setting up Computer Emergency Response Teams (CERTs), establishing competent authorities for NIS, and adopting national contingency plans for cyber incidents and national cybersecurity strategies).

In the explanatory memorandum to the NIS Directive, it was pointed out that *"the players managing critical infrastructure or providing services essential to the functioning of our societies are*

[34] COM (2013) 48 final, 2013/0027 (COD) 7.2.2013.

not under appropriate obligations to adopt risk management measures and exchange information with relevant authorities. On the one hand, therefore, businesses lack effective incentives to conduct serious risk management, involving risk assessment and taking appropriate steps to ensure NIS."[35]

For this reason, enterprises (with the exception of micro-enterprises) in the specific critical sectors, such as banking, energy (electricity and gas), transportation, health care, the infrastructure of key Internet services, and public administrations, will be required to assess the risks they face and adopt appropriate and proportionate measures to respond to real threats. Moreover, these entities would be required to report to competent authorities those incidents that seriously compromise the operation of their networks and information systems, thus having a significant impact on the continuity of services and supply of goods which depend on network and information systems.[36]

The above approach is manifested in the proposed changes to the contents of Articles 14 and 15 of the NIS Directive (after amendments of the European Parliament[37]). In accordance with Article 14, paragraphs 1–3:

„1. Member States shall ensure that market operators take appropriate and proportionate technical and organisational measures to detect and effectively manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting the security of their network and information systems on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

2. Member States shall ensure that market operators notify without undue delay to the competent authority or to the single point of contact incidents having a significant impact on the continuity of the core services they provide.

a) In the event of gross negligence in security and safety, commercial software producers shall be held liable despite user agreements containing absence of liabilities clauses.

3. The requirements under paragraphs 1 and 2 apply to all market operators (and software producers) providing services within the European Union."

In turn, according to Article 15 (3) of the Proposal for a NIS Directive, "Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations."

[35] *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union*, SWD(2013) 31 final 7.2.2013, p. 3.

[36] Commission staff working document, *Executive Summary of the Impact Assessment, Accompanying the document: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union*, SWD(2013) 31 final 7.2.2013, pp. 4–6.

[37] Report of the EP of 12 February 2014 on the *Proposal for the Directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union* (COM (2013) 48 – C70035/2013–2013/0027(COD)).

The above cited proposals reaffirm the position of EU administrative bodies that *"tentative, voluntary measures do not work and there needs to be strong regulatory obligations on MS to ensure harmonisation, governance and enforcement of European NIS"*[38]; in addition, due to a proposed regulatory option "[...] *the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably."*[39]

Although the above cited directive concerns only a specific area within CI, i.e. CI related to the network and information security, it cannot be ruled out that the regulatory (sanction-based) approach will also be applied to the protection of CI in other areas in the future. Adopting a "top-down" (regulatory) approach, the EU authorities concluded that a purely voluntary "bottom-up" approach was insufficient to achieve the assumed objectives.

The question remains whether such methods of "incentivising" private entities actually encourage them to act more actively in the area of CI protection or makes them act minimalistically, namely perform duties imposed by the law to the extent that allows them to avoid sanctions and at the same time discourage them to undertake *self-regulation* activities.

The issue of public procurement in the context of CI protection

The provisions of the Act of 29 January 2004 on *Public Procurement Law* (Journal of Laws of 2013, item 907 with further amendments, hereinafter "PPL") do not directly address issues concerning the occurrences of disruptions in the functioning of CIs.[40] It does not mean, however, that PPL does not contain decisions appropriate to extraordinary situations including failures, attacks, and other events that can result in disruptions affecting the functioning, continuity and integrity of CI.

From the point of view of disturbances in the functioning of CI and in the context of the public procurement system, the key issue is the possibility to efficiently award contracts of intervention of an interim nature that allow for a formalised and time-consuming procedure to be circumvented. From the data published by the President of the Public Procurement Office, it transpires that in 2012 (data for 2013 have not been published yet), the average duration of the public procurement procedure (counted from the date of publication of the contract notice) conducted as the open tendering procedure and restricted tendering amounted to

- *in the case of proceedings conducted in compliance with a national procedure (with value below the EU thresholds):*
    - 31 days for open tendering
    - 60 days for restricted tendering

[38] The opinion of the European Economic and Social Committee on the *Proposal for the Directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union*, COM (2103) 48 final – 2013/0027 (COD), 22 May 2013.

[39] Commission staff working document. *Executive Summary of the impact assessment*, Accompanying the document *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union*, SWD (2013) 31 final 7.2.2013, p. 8.

[40] As a side note, it needs to be noted that the Act on Crisis Management does not refer to PPL provisions either.

- *in the case of proceedings conducted in compliance with a EU procedure (with value exceeding the EU thresholds):*
    - 86 days for open tendering
    - 112 days for restricted tendering.

It is quite obvious that if a contracting entity is forced to use a time-consuming tender procedure, attempts to prevent disruptions in the functioning of CI can be futile. Therefore, PPL contains solutions which, after a relevant situation has arisen and having regard to the circumstances invoked, entitle the contracting authority to award a contract in a manner that allows the statutory time limits required under the procurement procedure to be shortened or use the non-competitive procedure. Depending on how urgent an event is and what demand it creates as a result, these solutions help prevent extraordinary situations.

The Table below presents an overview of statutory prerequisites that enable the contracting authority to take advantage of preference warranted by PPL (under individual procedures).

Table 5. Overview of statutory prerequisites that enable the contracting authority to take advantage of preference warranted by PPL (under individual procedures). Source: own compilation.

	PREREQUISITES
RESTRICTED PROCEDURE/ NEGOTIATED PROCEDURE WITH PRIOR PUBLICATION OF A CONTRACT NOTICE – FAST-TRACK PROCEDURE	urgent need to award a contract
NEGOTIATED PROCEDURE WITHOUT PRIOR PUBLICATION OF A CONTRACT NOTICE	need for prompt execution of the contract need for prompt execution of a contract does not result from events brought about by the contracting entity inabilityto foresee the necessity to award a contract time limits indispensable for conducting a tender procedure or a negotiated procedure with prior publication cannot be observed
SINGLE-SOURCE PROCUREMENT	exceptional situation exceptional situation does not result from events brought about by the contracting entity inability to foresee the occurrence of the exceptional situation time limits provided for other procedures cannot be observed

If the requirements that enable using one of the above procedures have been met, then

- in the event of the restricted procedure/negotiated procedure with prior publication – shorter time limits for the submission of requests to participate in a restricted tendering procedure can be established, but not shorter than 10 or 15 days depending on the form in which the contract notice is dispatched to the Publications Office of the European Union, compared to 30 or 37 days provided in the standard procedure and time limits for submitting offers (minimum 10 days compared to at least 40 days provided in the standard procedure)
- in the event of negotiated procedure without prior publication – negotiations can be conducted with selected economic operators
- in the event of the single-source procurement procedure – negotiations can be conducted only with one economic operator.

It is interesting to note that if a contract is classified as utility, i.e. executed by an entity designated in Article 3, paragraph 1 (4) of PPL and exercising the activities referred to in Article 132 of PPL, the PPL provisions are applicable only if the value of the contract is equal or exceeds the EU thresholds which currently amount to EUR 414,000 for deliveries/services and EUR 5,186,000 for construction works. However, if the value of utilities was estimated to be lower, the contracting authority is not obliged to use the provisions of PPL.

To conclude, the above quoted procedures (negotiated procedure without prior publication and single-source procurement in particular) may turn out to be extremely useful if a disturbance of CI occurred. It should be noted, however, that non-competitive procedures are exceptional in nature, and the presumptions justifying their use cannot be interpreted freely. In the case of the contracting authority taking advantage of non-competitive procedures, it is inevitable that the competitiveness principle, fundamental for the public procurement system, will always be violated. The contracting authority must be certain that the well-being it protects (life, health, property) objectively requires to be given priority before competitiveness due to its significance.[41] It is also necessary to remember that the use of one of the above procedures is justified only in response to a specific threat that has become a reality. There will be no grounds, however, to award a contract under either the negotiated procedure without prior publication or a single-source procurement procedure if the contracting authority, wishing to prevent undefined future phenomenon, executes contract which could be awarded under the competitive procedure.

Exemption from applying PPL provisions

Regardless of the procedures described above, it needs to be noted that in the event of an occurrence that disturbs the functioning of CI, it is potentially possible to use a premise entitling to withdraw from applying the PPL provisions *in view of significant national security interest or protection of public security* (Article 4(5) of PPL).

In accordance with the interpretation of the President of the Public Procurement Office, the aim of the legislator was, inter alia, to protect internal security. It is a fair observation to make that a causal relationship must exist between the withdrawal from applying the PPL provisions and a significant national security interest. The explication of the exact meaning of *significant national security interest may,* however, be quite problematic. Following the position of President of the PPO, a contract that is of significant national security interest is particularly one that concerns such values as sovereignty, international position, independence, territorial integrity, and defence of the state. Should the disruption of the functioning of the CI exert an influence on the above-said values, it is reasonable to consider the use of PPL to be waived. Although PPL does not mention this, it appears, however, that the disruption must be of real and not only potential nature.

[41] W. Dzierżanowski, *Ochrona konkurencji w prawie zamówień publicznych* [Protection of competition in the Public Procurement Law], Wolters Kluwer Polska Sp. z o.o., 2012, p. 156

Appeal procedure

The use of the appeal procedure in proceedings conducted in relation to the disruption of the functioning of CI may raise certain controversies. It needs to be emphasised that in principle the contracting authority, having lodged an appeal, cannot conclude an agreement until the National Appeals Chamber has delivered a judgement or an order closing the appeal procedures. The appeal procedure can therefore significantly extend the duration of proceedings leading to the conclusion of an agreement, which in the case of incidents threatening the functioning of CI, that by nature are urgent, may negatively affect actions undertaken by the contracting authority. PPL, however, provides a mechanism that prevents negative effects from happening during the suspension period resulting from the appeal lodged. Hence, the contracting authority is entitled to apply to the National Appeals Chamber for revocation of the prohibition to conclude an agreement. The National Appeals Chamber may in turn accede to the foregoing unless the failure to conclude a contract could cause negative effects for the public interest which exceed the benefits of safeguarding all interests likely to be harmed as a result of actions taken by the contracting authority under procurement procedures. It appears that in the case of CI-related threats, the justification of the application in question should not pose any problems (as practice demonstrates, there is a strong likelihood that the National Appeals Chamber will in fact take into account such a request). At the same time, it needs to be highlighted that the lodging of the appeal with the National Appeals Chamber is only possible if the public procurement procedure (regardless of the procedure selected by the contracting authority) is conducted under the PPL regime. Therefore, if a given procedure, either due to the value of a contract or the exemption mentioned in the Article 4(5) of PPL, is conducted without availing itself of PPL, the procedure before the National Appeals Chamber cannot be conducted and the appeal is rejected.

PPL does not provide for any mechanisms (other than those indicated above) which would facilitate (accelerate) the procurement procedure in relation to the maintenance (construction) of CI in non-crisis situations. The extraordinary procedures provided for in PPL have been derived straight from the EU directive. Therefore, introducing additional simplifications for contracting authorities without changing the directive, appears highly unlikely at this stage. The latest EU regulations replicate the system laid down in previous directives when it comes to tackling extraordinary situations, which also demonstrates that in view of the EU legislator, the current solutions should be deemed sufficient. What could be potentially considered is to introduce to special Acts exemptions from using PPL in certain defined situations. Such solutions already exist in Poland (e.g. the Act *regarding investments in the liquefied natural gas regasification terminal in Świnoujście* allows contracts to be executed in accordance with Article 4, paragraph 5 of PPL (de facto without availing themselves of PPL) if significant national security interest so requires.

Summary

National legislation imposes concrete obligations on CI owners and operators which, in practice, can incur substantial financial outlays. At the same time, in accordance with the provisions of the Act, CI owners and operators correspondingly bear the costs of performing their duties.

It appears, however, that these entities should be able to apply for financing of at least partial expenditure incurred in order to maintain CI. Amongst the potential sources of financing for CI projects, the CI operators may apply from national operational programmes which use the EU funds and the financial instrument CEF which among its objectives related to telecommunications network infrastructure mentions, inter alia, the supporting of critical telecommunications infrastructures.

Basic incentives for CI operators to encourage them to actively cooperate with state authorities in the area of CI protection should be found not so much in the binding provisions of law, but in the consequences of their collaboration with the public administration, such as

- gaining access to specialist knowledge
- identification of best practices and standards for CI protection
- participation in the shaping of and affecting the state's policy with regard to CI protection and at the same time affecting the final shape of responsibilities related to CI protection.

It appears that the foregoing could contribute to reducing the costs of CI operators in certain areas; nevertheless, a significant incentive for a more active participation of CI operators, besides purely statutory obligations, could be at least partial refinancing of costs incurred by CI operators, resulting explicitly from the binding provisions of law.

However, legal acts that are currently in force put a far greater emphasis on the need to protect CI and the obligation to engage private sector entities in the process rather than on specific instruments (financial, PPP) that could incentivise these entities to actively participate in the CI protection system.

The PPL provisions provide for mechanisms that facilitate the shortening or even elimination of competitive procedures in extraordinary situations or in situations with respect to specific utilities. However, with regard to CI maintenance and protection, the legislator does not provide for facilitation in the acquisition of goods and services.

3. Effective public-private cooperation – success factors

Joanna Świątkowska – the Kosciuszko Institute

Nowadays, a significant part of critical infrastructure (CI) is in the hands of private entities. Thus, in numerous cases, the state does not exert an exclusive influence on the security and continuity of CI. In order to maximise the effectiveness of infrastructure protection, the mechanisms of cooperation between public and private entities need to be provided. The purpose of this chapter is to indicate elements that strengthen the effectiveness of such cooperation, to demonstrate potential difficulties and to recommend solutions to overcome them. Chapter 4 complements this article by presenting good practices on CI forum governance methodologies.

Baseline conditions for effective cooperation

Mutual awareness and conviction that the responsibility for the security of the state and the common good should be shared is a prerequisite for effective cooperation between public and private entities and, as a consequence, is a vital component of CI security. On the one hand, the state should treat private entities as key actors and partners whose engagement is imperative for achieving the assumed objective. On the other hand, private entities themselves should be aware of the important role they play in the process of ensuring security for both the state and its individual citizens. The responsibility is incumbent on them and they need to be ready to embrace it. Being fully aware of these circumstances is a condition that determines the integrity of necessary actions undertaken to ensure CI security.

The public-private cooperation is frequently a "buzzword" used in the majority of debates on CI protection. However, it is not always clear what meaning it conveys.[1] In this article, public-private cooperation is predominantly used in the sense of initiatives aimed at a broadly understood information sharing (between private entities themselves and between private and public entities being supported by the state authorities) as well as the implementation of

[1] In the context of public-private cooperation, it is common to find references to public-private partnerships. If PPP, in accordance with the Act (Act of 19 December 2008 on Public-Private Partnership) is understood as a joint undertaking (defined in very formal terms), then in the spirit of adopted recommendations, it fails to be the most effective form of collaboration. One of the reasons is that PPPs are more project-orientated whereas security must be viewed as a process.

solutions recommended by the state (expressed in the form of standards) by private entities which considerably enhance the level of security. Information sharing should be understood as a process of collecting, analysing and exchanging information most often related to threats, the vulnerability of infrastructure, good practices, and recommendations, etc.

In spite of focusing the deliberations on the process of information sharing, the recommendations presented in this chapter may be applicable to other forms of cooperation, e.g. joint exercises during which procedures as well as safeguards and other crucial security elements are tested.

Effective cooperation – factors and potential challenges

One of the biggest challenges facing effective public-private cooperation is a difference in the understanding of objectives and priorities by the two parties. Public entities focus their activities on providing the highest level of security for the state and its citizens. Today, it is assumed that prosperity and development are contingent upon it. In turn, private entities are mainly profit-oriented, driven by improving financial performance. Yet, providing security requires material outlays such as investments, remuneration for work, the implementation of safety measures, control, monitoring, etc. Costly investments in security are therefore an additional load that private entities have to bear. This type of expenditure may not necessarily be in line with their financial strategy. Therefore, there is a risk that these entities will either minimize the expenditure on security, or purposefully count in the risk of potential loss, or simply hope that a problematic situation never arises.

Hence, the key to solving this problem and at the same time the main task facing the state is to make private entities as well as CI owners and users aware that they are incumbent with a much greater responsibility than the one which is exclusively about financial performance. Raising ethical or emotional arguments has little chance of success and is burdened with a high risk; therefore, it is worth concentrating on elucidating the economic consequences of negligence in the area of security.

A good practice is trying to persuade high-level company representatives (preferably at board level) to invest in security. What is important is to show them potential risks significantly affecting security which can be minimized with the use of acceptable resources.

An often inadequate level of protection associated with cybersecurity can be a good example. Raising awareness among the representatives of the board, who are often unaware of threats, about how widespread and costly problem cyber threats generate improves the chances of success.[2] It is useful to demonstrate the frequency with which problems occur and the extent of damages to finances, reputation, and the loss of credibility that occur as a consequence.

[2] Good practices on the methodology of the above-mentioned raising awareness process are derived, among others, from Dutch experiences. First of all, the process of raising awareness is most effective if it takes place during conversations held between the company and the representatives of public entities or their associates. During such a meeting, the company's representatives may be encouraged to take a short knowledge test that shows on the one hand if the board of directors has knowledge and awareness of safeguards applied in their company, and on the other hand, it allows for verifying whether these safeguards are being truly implemented. Asking simple questions created on the basis of a standardised questionnaire can also bring good results.

Confrontation with the prospect of potential consequences, together with an indication that an investment in security can in fact protect the company from heavy losses and secure their financial performance, proves an effective instrument. In this context, a particular emphasis should be put on promoting the advantages of the preventive approach to security instead of adopting a reactive attitude.

Another strategy is to aim similar activities at the company's shareholders. The underlying assumption is that the knowledge they acquire will either prompt them to compel the board to take action, or to express the necessity to invest in security.

Apart from the different perception of objectives, the effectiveness of public-private cooperation is contingent upon resolving other potential issues. These include building mutual trust between the collaborating parties as well as convincing them of the purposefulness and value-added of the undertaken partnership. The processes involving information exchange provide a good example. When it comes to trust[3], the engaged entities need to be certain that sharing information is "safe." The entities must be given guarantees that information will never fall into the wrong hands, be disclosed without their consent, harm their image, or otherwise adversely affect the confidence of their customers. By analogy, the entities cannot fear retribution as a result of disclosing any data. Security must be ensured at a contract level, mutual obligations, and in the form of technical measures that secure information sharing channels. Apart from trust, the entities involved need to be certain that the participation in information sharing initiatives makes sense and brings a desired effect.[4] Otherwise engagement will be perceived as an unproductive waste of time. Effective communication must be a two-way process and feedback received by private entities needs to translate into benefits that increase security in real terms. Only the sense of purposefulness of actions will make the entities engage in these activities more solidly.

Finally, the discussion of an effective form of public-private cooperation gives rise to a heated dispute between advocates and opponents of applying voluntary and mandatory forms of cooperation. The first strategy draws upon the willingness of entities to participate in certain initiatives and the belief in their value. According to the other option, it is possible to make private sector representatives engage in given processes and, for instance, implement security-related solutions (specific standards) under threat of broadly understood sanctions.[5]

The opponents of the mandatory approach argue that "enforced" forms of cooperation undermine trust, making entities perform tasks only to avoid punishment. With the sole aim of completing the tasks, the entities engage minimally in the activities they perform, which often makes these activities highly ineffective. An example of such a danger is a routinely applied approach described by "compliance" where individual entities obtain a set of standards and requirements they have to comply with. They do not focus on actual threats or dangers (risk based approach); instead, they solely, and often indiscriminately, "tick off" activities they have to take in order to comply with a standard. In this scenario, the conformity with the guidelines is erroneously considered as an aim in itself.

[3] Good practices in this respect are closely related to the methodology of running and managing a forum, and as such will be presented in Chapter 4.

[4] More about it can be found in Chapter 4.

[5] It is highly disputable if such a form can actually be termed cooperation.

Successful forms of voluntary collaboration are presented as a counterargument for mandatory activity. Operating in the USA and Great Britain, Self Storage Associations are perfect examples of such cooperation.[6] The main aim of these organisations is to establish common, voluntary standards. The overriding value lies in the fact that the development of these standards is a joint effort drawing upon practical knowledge and experiences of individual entities. Being convinced of their value, the entities themselves start using and implementing them.

Conversely, the advocates of the compulsory cooperation invoke an argument that market-based solutions are insufficiently strong to persuade entities to ensure security; in fact, they actually promote risk-taking. Numerous real-life examples of negligence in security reinforce the view that a more "invasive" form of influence exerted by the state is justifiable. It needs to be noted, however, that the risk resulting from employing a trust-based approach only is enormous considering the significance and important role of CI for the security of the state.

In addition, experts such as James Lewis from C.SIS argue that the introduction of just a few very simple solutions may dramatically strengthen security. In this context, it is worth considering the introduction of regulation that will impose their implementation.[7]

To recapitulate the considerations of the mandatory and voluntary approaches, it appears impossible to assess unequivocally which of them is more legitimate. It is one of the most challenging aspects of effective public-private cooperation, also because it touches upon worldview issues. This publication recommends using a case-by-case method to assess the situation and select an appropriate strategy. Applying tailored and not only "one-size-fits-all" solutions can eventually bring a desired effect. Alternatively, a "mixed" approach allows mandatory mechanisms to be selected and applied in the most crucial sectors[8] where the risk is the highest.

Regardless of the option selected in the end, it is worth ensuring that basic principles such as purposefulness of action and an action-result relationship are properly demonstrated and fulfilled.[9] Above all, however, any forms of collaboration should be combined with mechanisms introduced by the state that stimulate interest in cooperation as well as affect the efficiency and engagement of the participants.

Incentives affecting the effectiveness of public-private cooperation

There is a wide array of instruments that the state can use to encourage private entities to cooperate and conscientiously perform security-related tasks (e.g. implement specific standards). A list of selected tools has been presented below:

[6] See http://www.azselfstorage.org/, http://www.ssauk.com/.

[7] Although the author refers to solutions strictly associated with ICT systems, it is worth considering his reasoning regarding this particular example and the context of general solutions for the entire CI system. See J. A. Lewis, *Raising the Bar for Cybersecurity*, 12 February 2013. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, [accessed: 13/04/2013].

[8] S. Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf, [accessed: 13/04/2013].

[9] Which, in the voluntarily approach and the absence of sanctions, is imperative.

Tax incentives: dedicated to entities participating in initiatives related to, inter alia, information sharing or applying security solutions that comply with specific standards.[10]

Grants: introducing a system of grants for research and innovation in the area of security. One of the examples is a USD 51 million grant awarded by the Environmental Protection Agency to water utilities for performing vulnerability assessments and developing emergency response plans.[11] The system of grants can work in two ways. First, as an opportunity per se to apply for financial resources to be spent on activities directly involving security. Second, they can indirectly affect the increase in the level of protection. Undertaking specific security-related activities, such as the implementation of standards, can, in effect, be a necessary requirement that allows companies to participate in grant competitions that are of interest to them. Therefore, in order for the companies to be able to apply for funding and, in addition, raise funds for real actions, they will need to implement certain solutions and take part in initiatives (active participation in information sharing forums may be one of the requirements). The foregoing mechanisms, alternative to grants, can take the form of a condition upon which companies are allowed to participate in tenders or state-funded training programmes enhancing specific skills.

Establishing insurance market[12] for security-driven activities: in essence, companies which undertake actions that increase security (e.g. by complying with standards, implementing specific procedures, and partaking in information sharing activities) could be awarded with significant insurance discounts.

Awarding certificates or labelling companies in a way that would be easily recognisable for clients, so that it is clear that these entities comply with standards and procedures promoting security. Gradation of labels could also be introduced. As a company may be applying safeguards at various degrees, the more advanced actions are taken, the higher level would be awarded.

Loans: this mechanism could make the companies which are either active on information sharing forums or apply appropriate security measures, eligible for attractive loan offers or financial aid to repair damages or recover losses in case an incident should occur.

The above suggestions, to a large extent, involve financial forms of incentivising private entities to engage in security-oriented activities. There are a number of other non-financial factors that can be of great importance.

Hence, the question that arises is what, besides the foregoing financial mechanisms, can persuade these entities to actively and robustly engage in security-related activities. The presented examples will refer to the participation in information sharing initiatives.

[10] It is mandatory that the standards should meet the criterion of timeliness and be flexible enough to adjust to the prevailing conditions. Rigid and outdated standards in conjunction with a minimalistic attitude towards implementing enforced solutions can bring disastrous results (e.g. a false sense of security).

[11] S. Eckert, op. cit.

[12] This element of the potential "system of incentives" requires possible effects to be further deepened through analysis. The creation of the insurance market alone can be very difficult. Hence, particularly at the outset, it is worth considering the idea of introducing a public system for supporting such initiatives, for example reinsurance.

As it was stated earlier, the belief in the value added and purposefulness of actions is the most important factor encouraging entities to enter into cooperation. Active involvement in activities of information sharing platforms should entail the prospect for obtaining data that will translate into a better and safer functioning of their companies. Therefore, information must be accurate, up-to-date, and provided on time. In addition, participation in selected mechanisms of information sharing could be rewarded with granting access to government information, particularly one that cannot be obtained elsewhere. Other potential incentives include counselling and knowledge (technical, legal, etc.) exchange between experts associated with public bodies and private entities. By analogy, the state authorities may offer assistance to the engaged entities in problematic situations. The belief held by participants that engaging in such initiatives offers them a unique opportunity to conduct a dialogue on future decisions taken by public bodies may also prove valuable. By taking part in such a discussion, private entities would have the opportunity to lobby for desired changes and point out possible negative effects of potential decisions. Ultimately, the entities partaking in information sharing forums and other initiatives (e.g. exercises), can be given an opportunity to participate in coaching and training sessions held or funded by the state. They can constitute a very attractive incentive as they strengthen competences and expertise as well as increase the level of knowledge.

To summarise the information on effective, mutually beneficial collaborative engagement of public and private entities, it is worth invoking a Dutch model initiative known as the ICT Response Board.[13] Consisting of the representatives of the private and public sectors, this body convenes ad hoc in crisis situations involving cyberattacks.[14] The IRB aims to provide support to appropriate entities, be they elements of the crisis management system, or private entities. Activities undertaken by the IRB involve flagging up potential threats, identifying and interpreting threats, coordinating activities when a crisis situation occurs, counselling entities stricken or threatened by security incidents, collecting information and distributing it among stakeholders. In addition, the entities engaged in the initiative hold joint scenario-based exercises during which they are testing procedures, specific solutions and activities.

The Future of the public-private cooperation in Poland

Prepared by the GCS, the NCIPP opts for a non-sanction-based approach to the protection of the key components of the state's infrastructure.[15] The suggestions presented above are not only likely to contribute to enhancing the effectiveness of voluntary forms of cooperation, but also increase the chances for a robust execution of numerous initiatives.

At the same time, it is worth noting that in the coming months international solutions that Poland most likely will have to implement will require certain areas of cooperation to be regulated. This statement refers to a directive concerning network and information security[16]; at the time when this chapter was written, the directive was passed by the European Parliament. As

[13] ICT Response Board, https://www.ncsc.nl/english/services/crisis-management-reinforcement/ict-response-board.html, [accessed: 13/04/2013].

[14] Alternatively, in the situation of a looming crisis.

[15] GCS, *National Critical Infrastructure Protection Programme*, pp. 6–7.

[16] *Directive of The European Parliament and of The Council concerning measures to ensure a high common level of network and information security across the Union*, COM (2013) 48 final.

the next step, the final text will be negotiated with the EU Council. If the directive is adopted in its current form, it will impose mandatory elements of cooperation on public and private entities. First and foremost, the directive will force CI owners[17] to implement appropriate measures aimed at increasing security and to report on incidents that jeopardise network and information security.[18] Clearly, we need to be aware that the directive concerns only a limited segment of tasks related to CI security – ICT security to be precise. Nevertheless, it interferes in the manner in which public and private cooperation is established, which can affect other areas in the future.

If the directive comes into force, Poland will be required to apply elements of the sanction-based approach. This gives rise to a concern that private entities will realise predetermined tasks only to avoid punishment and with minimal engagement. In order to help alleviate all possible negative effects of the sanction-based cooperation (imposed by the directive and any other prospective collaboration), it is advisable to consider combining these regulatory efforts with actions supporting the private sector and presented in the list above. The implementation of the directive to national legal orders can be done in a flexible manner; therefore, there is merit in safeguarding the effectiveness of its implementation by stimulating efficient public-private cooperation.

Summary

The understanding of differences in the way the two parties define security objectives and priorities should underpin effective public-private cooperation. Another prerequisite is to guarantee that both sectors will benefit from all joint initiatives. This stipulation is particularly relevant in the context of voluntary initiatives. The decision to adopt a mandatory approach should be well-pondered and based upon case-by-case analysis with particular attention paid to high-risk sectors. Lastly, private entities should be encouraged to engage in collaboration by means of incentives, both financial and non-financial, which will increase the likelihood of effective involvement.

[17] See COM (2013) 48 final, Annex II.

[18] COM (2013) 48 final, Article 14(1); Article 14(2).

4. The methodology of governing collaboration forums for critical infrastructure protection

Dominika Dziwisz – the Kosciuszko Institute

The majority of existing forms of cooperation between public and private partners are driven by the facilitation of information sharing on risks, weaknesses, threats, and vulnerabilities as well as best practices and recommendations for securing critical infrastructure (CI). In order for them to be effective, they must be organised across three levels: national, systemic, and regional.[1] Information sharing at each of these levels must be conducted on an ongoing basis, ideally with the parties staying in direct contact, so that robust and sustainable relationships between the partners could be maintained.

The rudimentary form of information exchange leading to an increase in CI security is joint meetings of participants who are engaged in public-private cooperation[2] within CI protection forums. Therefore, in 2013, the Government Centre for Security (GCS) recommended establishing a network of forums aimed at identifying key problems that affect CI protection and developing suggestions for solutions.[3]

As ENISA identified in the report examining the efficiency of forum activity, one of the biggest barriers and challenges, apart from the low quality of information and inappropriately tailored incentives for cooperation[4], isthe poor management of forums.[5]

The article supplements recommendations issued by the GCS, offering concrete solutions for governing CI forums as well as highlighting major problems involved. The analysis was based on the examples of effective solutions applied in the United States of America, but

[1] GCS, *National Critical Infrastructure Protection Programme*, http://rcb.gov.pl/?page_id=261 [accessed: 10/04/2014].

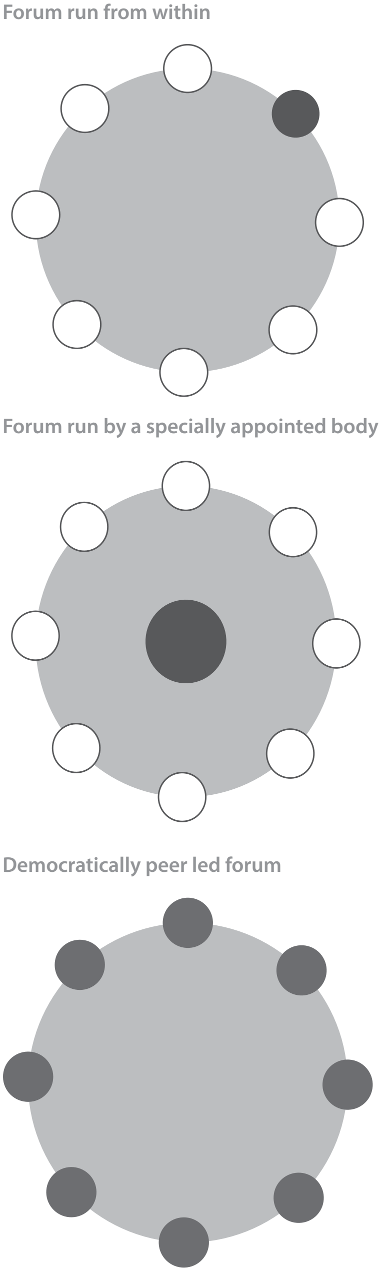
[2] There are numerous mechanisms designed to manage the protection of CI. They range from methods where the government determines the rules to be observed, in other words, it plays the role of the only authority that can set out security standards and execute compliance, to approaches where the government allows the security of CI to be regulated by market-based mechanisms. In between these polarised solutions, there are a number of other, intermediate forms of cooperation. They vary according to the extent with which the state interferes with the work of CIs owned by private entities. For this reason, the author resigned from using the phrase "public-private partnership", which represents only one form of collaboration, in favour of a broader concept of "public-private cooperation." In this context, public-private cooperation for CI security should be understood as initiatives aimed at collecting, processing and sharing information relevant for CI security between governmental and private sectors and between private entities themselves.

[3] *The National Critical Infrastructure…*, op. cit.

[4] Incommensurate with the risk taken.

[5] ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, 2010.

Figure 3, 4, 5. Forum governance types. Source: Own compilation based on ENISA, *Desktop Research on Public Private Partnerships*, 2011.



Forum run from within

Forum run by a specially appointed body

Democratically peer led forum

predominantly on the observations and suggestions offered by ENISA (European Network and Information Security Agency). ENISA is a centre for sharing cybersecurity experiences and information between Member States and the EU Institutions. In reports from 2010 and 2011[6], ENISA compared different governance models of public-private cooperation, specifically in the area of CIIP (Critical Information Infrastructure Protection). However, ENISA's observations and recommendations are also used to establish general rules and the framework of cooperation for other information sharing initiatives.

Lastly, the author would like to emphasise that the observations and recommendations refer predominantly to managing sector-specific forums.

Forum organisational structure

In principle, in order to prevent discrimination against any one of the parties, the principle of equality of all public and private partners should underlie public-private cooperation. In view of this fact, when setting up an information sharing forum, all entities involved should be given similar rights, possibilities for action and responsibilities for the security of the "client" (public and private). At the same time, even if we assume that all cooperating parties are on an equal footing, as in any other organisation, it is mandatory to choose an entity responsible for governance and coordination.

The first and most commonly practised form of governance is assigning the leadership role to one of the partners from either the public or private sector, i.e. running by one from within. This works best for forums where the information is shared among partners representing the same CI sector since they are fully familiar with the specific nature of their activity as well as possible problems that may occur.

Another, less popular form, involves assigning the leadership to a specially appointed body. This solution is most effective when managing the collaboration of individual sector-specific forums. It can prevent a situation where participants, having detailed knowledge about their own

[6] ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security, 2010, ENISA, Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*, ENISA, 2011.

sector, are unable to counteract potential threats due to a lack of a broader picture. Thus, the coordinating body, being aware of the complexity of the problem, is able to direct the activity of all participants in the most optimal way.

In the case of American Information Sharing and Analysis Centers (ISACs), this function has been assigned to the National Council of ISACs that was appointed in 2003. Consisting of ISACs sector-specific representatives, the Council convenes once a month with the aim to foster cooperation between them and build mutual trust as well as tackle current problems and develop strategies for responding to existing threats. In addition, the Councilconducts training and acts as an intermediary between the private sector and the National Infrastructure Coordinating Center (NICC), which is part of the U.S. Department of Homeland Security, in crisis situations at the national level. The Council also sponsors an annual Critical Infrastructure Protection (CIP) Congress.

Democratic peer leadership is a third form of forum governance. In practical terms, this form is not only least effective, but it is also most the conflict-prone, therefore hardly used. However, attempts are being taken to "democratise" this form of governance by appointing a rotational chair in order to prevent one participant from gaining a dominant position and actually leading the network.

Levels of forum organisational structure

As it was mentioned in the introduction, for CI security information sharing to be effective, it needs to be organisedacross several levels: national, systemic, and regional. Again, American ISACs are an example of good organisation and governance of the public and private partner network. The Centres collect information, security data and share them with institutions co-creating a given centre. As initially planned, there was supposed to be a single ISAC established for all economic sectors. In practice, the solution turned out to be ineffective. Therefore, a separate centre was established for each sector mentioned in Presidential Decision Directive No. 63 (PDD 63).[7]

The decision to set up a separate ISAC for every CI sector was key to the effectiveness of the ISACs networks. In view of the specific nature of CI sectors, establishing a single "collective" ISAC for all sectors had minimal chances for success. Also, creating general standards for cooperation would be highly inefficient because each sector functioned in its own specific way. Therefore, a better solution was to set up separate ISACs with responsibility for the security of their respective sector. American ISACs were amongst the first forums designed for sector-specific information exchange. Today, similar solutions have been adopted by countries which, on numerous occasions, followed the example of ISACs.[8] In Poland, the Government Centre for Security (GCS) has issued a recommendation for establishing separate, systemic forums

[7] *Presidential Decision Directive 63*, 22.05.1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, [accessed: 10/12/2013].

[8] Sector-specific information sharing forums operate, inter alia, in Australia. Australian Trusted Information Sharing Network (TISN) is a forum for sharing information between owners and operators of critical infrastructures. TISN consists of seven Sector Groups: two Expert Advisory Groups as well as the Communities of Interest (CoL) and Critical Infrastructure Advisory Council (CIAC). Sector Groups serve as intermediaries between the governmental and private sectors. After: ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, 2011, p. 49.

for every CI sector that will convene at least biannually or more often, depending on the circumstances. When designing forums for information sharing, the GCS employed international sector-based standards. This solution, for reasons mentioned above, has every chance of success and can bring the same positive effects as the American solutions.

Hierarchical vs. network governance

The problem of building effective forms of cooperation is invariably linked to the clash of two governance cultures. Engaging multi-stakeholders, the private sector is open, predisposed to change and governed horizontally. By contrast, the public sector is often a more rigid, hierarchically governed structure[9] that displays less reactivity in the face of change. It has, however, the capability to resolve complex problems over long periods of time. Currently, with the private sector having a relative potency of action, setting ground rules for cooperation with the government can cause numerous conflicts.[10] The situation is further complicated by the fact that each of the interested groups wants to be in charge.[11]

Some experts argue that a solution could be to resign from "traditional" forms of cooperation and governance and replace it with network governance. According to this concept, the hierarchical organisation of roles where some entities monitor other participants forced to cooperate under the threat of criminal sanctions are abandoned in favour of more complicated network systems. What is characteristic of them are numerous centres for decision-making, equal status of participants and sharing responsibility for initiatives undertaken as well as voluntary involvement in developing solutions for a mutual benefit. In the case of information sharing forums, it would entail departing from thinking of the government as the monopolist of their governance, namely issuing instructions and monitoring the fulfilment of tasks by a single entity and, as a consequence, applying a model of more dispersed decision-making. Appropriate conditions should be created in which "public administration thus becomes a team sport where persuasion, negotiations, and mutual trust are more important than control and regulation.[12] Mutual understanding and complementary cooperation on an equal footing will allow the private and public sectors to achieve their goals, which, as a rule, is impeded or made impossible if control and regulation is in the hands of a single entity only. In practice, "in order to facilitate such new forms of cooperation, small and relatively homogenous networks are required that involve all actors who will and can contribute to the fulfilment of a public service in their own interest. Such actors, most of whom come from both the public and the private sectors,then organize themselves quasi autonomously. They fix rules for common action and determine the responsibilities and commitments of the individual partners."[13]These various networks self-monitor their activities, which mean that a number of independent, self-regulating networks are involved in performing public tasks. While both the public and private

[9] J. Healey, *Preparing for Cyber* 9/12, http://www.isn.ethz.ch/DigitalLibrary/Publications/Detail/?ots591=966c9813-6e74-4e0b-b884-8ed9f3f0978c&lng=en&id=143486, [accessed: 01/04/2014}.

[10] Ibidem.

[11] Ibidem.

[12] M. D. Cavelty, M. Suter, *Public-Private Partnerships are no silver bullet: An expanded governance for Critical Infrastructure Protection*, "International Journal of Critical Infrastructure Protection" 2009, doi:10.1016/j.ijcip.2009.08.006, p. 5.

[13] R.A.W. Rhodes, *The new governance: Governing without government*, Political Studies 44 (1996), p. 658f, After: Ibidem, p. 5.

sectors have their own “representatives”, agencies representing the public sector resign from their special, privileged status. The network will only function if decisions are taken through negotiations and all parties are on an equal footing.

Forum funding

A crucial aspect of the organisation of the information sharing forum is funding its activity. The forum can be funded either from the government budget or by participants themselves who undertake to pay a membership subscription. In the first scenario, the private sector is highly incentivised to engage in participation when the government covers administrative costs. The example of ISACs in the U.S. which are subsidised or in some cases fully funded from the federal budget proves that the absence of fees for participants from the private sector is a successful motivator for action. It is not by all means a common practice. The report by ENISA shows that 24 percent of organisations studied require their members to pay subscription to cover administrative expenses.[14]

Forums and other forms of information sharing can also be funded using alternative methods. For instance, the participants can pay for real value services, such as access to expert studies, or use a mixed method where the members cover the costs of their time and expenses whereas the government pays for coordination costs, venue, etc.

Forms of communication

Another aspect of forum governance is the choice of a communication channel between partners. Information sharing can occur traditionally, i.e. during regular or occasional “face-to-face” meetings. As practice shows, this method is the most productive and effective. It is also possible to take advantage of modern technologies, above all the Internet, which facilitates the cooperation through video conferences or transferring information via private distribution lists. The participants can also use specifically dedicated Internet platforms to publish information that is crucial for the security of CI. This platform can consist of specific systemic and expert groups (rooms).[15] Coordination and administrative management of the forum can be done virtually; however, decisions that are fundamental to cooperation should be taken during direct physical meetings. According to the report by ENISA, direct contact maintained by forum participants allows for information sharing to be more effective.

Trust among forum participants

The lack of trust among the forum participants, particularly among the representatives of the private and public sectors may fundamentally impede the functioning of the forum. Private enterprises are mostly concerned about insufficient confidentiality and security of information shared, which can adversely affect their reputation and competitiveness. The same concerns are harboured by the government. “The culture of secrecy” and a deeply entrenched fear to share information with non-governmental entities pose a risk of the information sharing initiatives ending in stalemate.

[14] ENISA, *Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*, 2011.

[15] *The National Critical Infrastructure…*, op. cit.

In view of this, the building of mutual trust and ensuring the highest possible security of transferred data is both a priority and a challenge for effective collaboration. Trust building should be understood as a gradual and long-lasting "process" during which the forum participants constantly work on strengthening their contacts. There are a number of ways to increase the level of trust.

First, it is mandatory for the forum members to determine the type of information shared – they must be up to date, factual and useful from the point of view of the entire group. A situation where the forum participants themselves formulate rules for information sharing minimises a risk of uncertainty as to the possibility for disclosing any information on the forum other than that which was specifically defined. At the same time, it is necessary to establish procedures for removing any sensitive personal and contact details from databases.

Second, the size of the forum may be an obstacle to building relationships and trust among forum participants. The larger the group, the more difficult it becomes to build trust among the participants. Increasing the number of participants often goes hand in hand with a greater variety and dissimilarity of goals and priorities that make it hard to reach a consensus. At the same time, it is difficult to find common benefits of cooperation that are equally important for all participants. However, it is difficult to determine how many participants should comprise a model forum. It is dependent upon the specific nature of a given CI sector, but most of all, upon a unanimous decision of partners.

Third, it is impossible to avoid a risk that some of the information shared may be used for commercial purposes. Therefore, it is worth considering whether sales and marketing professionals should participate in sector-specific forums right next to security specialists and technical experts. As ENISA demonstrated in its report, the risk of commercial exploitation of confidential information is a barrier to building mutual trust. Hence, it is essential to specify the exact preferences regarding target forum participants as well as to obtain their consent to establish collaboration in the proposed composition.

Fourth, sustainability and continuity of the forum are the cornerstone of trust. Therefore, it is essential to implement the principles that guarantee the continuity of membership, such as detailed rules for the participation in the forum supplemented with concrete incentives for cooperation, rules for conscientious performance of duties, declaration of rights and responsibilities as well as rules that regulate the process of excluding an entity from membership. A situation where some members take advantage of the efforts of others while offering a negligible contribution of their own cannot take place. At the same time, it is necessary to prevent unhealthy competition. Each of the forum members should be aware of the importance of their actions and strive for optimisation of their own efforts, thus creating a value added for the entire group.

Fifth, the choice of the method of communication between forum participants has a direct influence on trust within the group. Using Internet-enabled tools to share information, e.g. Internet platforms, virtual conferences or electronic mail effectively help build the sense of stability and assurance that cooperating entities can respond quickly if needed. It does not change the fact that the undeniable advantage of in-person meetings of forum participants is their ability to overcome the barriers of uncertainty and distrust that stem from not knowing the other members. In-person meetings help build knowledge about common objectives and strategies for action on the basis of which the members can predict further prospective actions. Therefore, as it was earlier emphasised, "face-to-face" communication should underlie all forms of contacts between the forum participants.

Forms of cooperation and flexibility of choice

Finally, it is worth noting that due to the specific nature and differences between CI sectors, no forms of collaboration should be predetermined. Again, based on the example of the American project of collaboration, we can notice that ISACs have evolved varied structures due to their independence of federal agencies. Every sector has its specific problems; therefore, the flexibility in the way the partnership is organised allows for designing solutions that most adequately reflect the specific character and requirements of each sector. It is precisely the needs of a given sector and clearly formulated objectives of the partnership and not conventional solutions adopted within the framework of public-private cooperation that should affect the structure and rules governing the forum and its members.

Summary

When setting up the collaboration forum for CI security, it should be assumed from the outset that the collaborating parties should be on an equal footing and at the same time choose the best possible form of governance and coordination depending on whether information sharing will take place between the participants of the same or different CI sectors. Due to its own specific problems, it is important that every CI sector has its separate systemic forum. As practice shows, establishing a single forum for all CI sectors proves ineffective. However, in order to gain a bigger picture of the situation and understand the complexity of different problems, there is a need for one entity that should manage the cooperation between individual sector-specific forums. In Poland, this function could be appointed to the GCS.

When organising and administering the forum, it is also necessary to abandon the historically-entrenched attitudes claiming that some solutions can be worked out only at a governmental level. In other words, thinking of forums in terms of hierarchical subordination should be abandoned in favour of flexibility and network governance which, in practice, turns out to be far more effective. Other important factors that determine the effectiveness of the forum for opinion sharing include tailored mechanisms for funding its activity, appropriate types of collaboration channels as well as the flexibility in terms of the choice of the form of collaboration for every sector. However, the all-important condition determining the effectiveness of the forum is a trusting relationship between its members as well as a willingness to share information rooted in the belief in the significance, effectiveness, success and security of the partnership. Even if we assume that the membership is mandatory, in the absence of willingness and trust, any initiatives are bound to fall through.

part II

5. The role of ICT components in the functioning of critical infrastructure

Mirosław Ryba – EY

Today, the fact of the ICT (digitization) development is no longer surprising to anyone. It is more about the spectacular pace of this development that draws the admiration and sometimes disbelief. In the past, technological change took years whereas today modifications in ICT systems happen in the space of months. Solutions, which 10 years ago could be described as "science-fiction" concepts, are currently being implemented for not only military, but also commercial use. An example today includes extensively tested autonomous cars[1], which – according to manufacturers' forecasts – should be commercially available soon, not to mention mobile devices that are launched on the market every few weeks and whose computing power is greater than that one NASA had when landing the first man on the Moon (e.g. AGC computer, designed specifically for this purpose at MIT, was equipped with a 64-KB memory and clocked by 43 KHz signal).

So widespread in everyday life, ICT solutions have naturally become applicable to critical infrastructure systems (CI) and today no one dares to question the fact that the efficient functioning of CI is impossible without the proper support of ICT systems.

ICT systems used in CI

ICT systems for CI can be divided into two groups of solutions: Information Technology (IT) and Operational Technology (OT). The application of these solutions is closely dependent upon the industry, or to be precise, the functioning area of CI in which they are utilised. CI systems offering citizen-oriented services (finances, communication, emergency services, etc.), i.e. resources where Information and Communication Technologies support business processes or are employed to gather and process data, widely use IT solutions. Conversely, in all CI facilities associated with technological processes (extraction, manufacturing, processing, etc.), OT solutions such as devices and applications for managing production facilities and a technological process, play a key role.

Capacity and availability of these solutions are key differentiating features between IT and OT. Although in the case of IT solutions an interruption of operational continuity of the system is

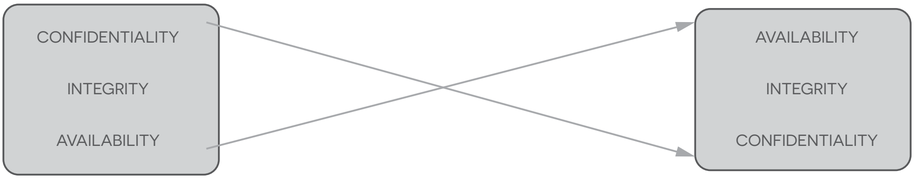
[1] Autonomous or driverless cars – robotic, self-driving cars that are capable of navigating and sensing changes in the surrounding (other vehicles, obstacles, traffic lights, etc.) without the need for human interference.

acceptable (despite often being costly business-wise), in OT we deal with real-time solutions where the response to changes in the manufacturing environment must be instantaneous and any delays are unacceptable.[2] This is mostly dictated by economic factors (unscheduled interruption to the operational continuity of certain manufacturing installations results in multi-million financial losses), but above all the factors related to the safety of people. Providing control over the manufacturing environment has a direct influence on people's safety (their health and sometimes their lives) and the safety of the natural environment.

Another key difference between IT and OT solutions is the period of time for which these solutions are designed. For IT solutions, the average service life of systems/components is 3 to 5 years whereas OT solutions are planned to last for at least a decade, with an average of about 15 years. Hence, with such a long operating period, it needs to be considered that OT solutions will undergo fewer upgrades compared to IT solutions, and that obsolete technologies that are no longer developed will be encountered in the OT environment. This also results in limited resources (understood as the capacity of processors, memories, disks, etc.) when it comes to the availability of equipment components, which very often makes it impossible for the OT system to be expanded (or additional safety enhancing components to be installed) and in the case of pending upgrade or expansion, it requires the entire environment to be replaced.

The application of IT and OT in different domains leads to differences between IT and OT in the perception of safety aspects. From the point of view of the safety of IT solutions, the key problem is to ensure (business) data confidentiality whereas for OT, the all-important aspect is to ensure the availability of the manufacturing process. The following picture visualises this relationship.

Figure 6. Priorities for IT and OT security attributes. Source: own compilation.



It needs to be noted that inasmuch as IT solutions entered the realm of CI (e.g. telecommunications) following the technological revolution that took place at the turn of the 20th century, the realm of OT solutions remained hermetic for long years. It was not until the beginning of the 21st century that dramatic changes in OT started taking place involving the transfer of IT solutions to OT, OT standardisation, abandoning closed protocols, the introduction of virtual and mobile solutions to OT, and the implementation of ICT safety tools. It should be remembered, however, that the decision to implement any solutions, including ICT, to critical infrastructure must result from a conscious and careful consideration of both advantages that the technology brings and threats it can pose to the existing environment.

[2] From the perspective of IT, even such a banal action as rebooting system is very often utterly unacceptable in the case of OT solutions.

Following the division of CI presented in the "National Critical Infrastructure Protection Programme"[3] it needs to be emphasised that the role, nature, and type of ICT solutions utilised in individual CI systems are diametrically different. Below is a general overview and working principles of ICT solutions used in distinct CI systems.

IT and OT solutions utilised in individual CI systems

The area that most heavily relies on OT solutions is the system of energy, energy resource and fuel supply within which we can distinguish manufacturing, transmission and distribution of electric power, thermal energy and natural gas, transmission and processing of crude oil, and coal mining. OT systems that are key to entities belonging to these sectors and responsible for monitoring and technological process control include SCADA (Supervisory Control and Data Acquisition), DMS (Distribution Management System) or in the case of energy industry – EMS (Energy Management System). Production facilities (e.g. power blocks in power stations or refinery installations) are controlled by means of DCS (Distributed Control System) solutions, i.e. comprehensive and integrated systems that are responsible for the control and visualisation of the industrial process.

Occasionally, in order to increase the capacity of the production process, APC-class solutions (Advanced Process Control) are applied, particularly those helping minimise downtime, optimise installation maintenance and better adjust volumes and manufacturing methods to fluctuating macroeconomic needs.

Very similar solutions are utilised in the system of production, storage, and use of chemical and radioactive substances as well as the system of water supply where SCADA systems have an oversight over the entire technological process.

In processing plants, being part of the food supply chain, individual industrial machines are controlled by means of dedicated PLC (Programmable Logic Controller) controllers that carry out programmed instructions for specific production tasks. In more advanced facilities, it is MES (Manufacturing Execution System) solutions that oversee the entire manufacturing process by collecting real-time data sent by PLC controllers and facilitating immediate decision making which allows for the production process to be effectively controlled and optimised as well as any potential irregularities occurring during production to be detected and responded to.

ICT solutions utilised within the financial system face completely different challenges. Here, securing the confidentiality of financial data and providing control mechanisms warranting the integrity of the stored and processed data is of utmost importance. As practice and recent IT system breakdowns in the biggest banks in Poland demonstrate, temporary unavailability of financial services – be it a lack of access to cash on account or inability to make credit card transactions – becomes such a common phenomenon that a great majority of users find it hardly concerning or astonishing.

[3] GCS, *National Critical Infrastructure Protection Programme*, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf, [accessed: 06/06/2014].

Furthermore, IT solutions used in the banking system are intended to process large volumes of transactional data and need to possess outstanding analytical capabilities so that financial institutions can take informed decisions about the appropriate categorisation and stratification of their clients based on the user data collected. A similar challenge faces telecommunications entities which decide on their approach to various groups of clients based on data about user activity in the telecommunications network, but above all they determine the development of telecommunications infrastructure, which is crucial from the perspective of CI.

Another area where ICT technologies currently play an essential part are systems ensuring the continuity of public administration activities. However, the multitude of IT solutions used by separate administrative units and at the same the absence of a proper, comprehensive approach to the security of the entire administration (e.g. based on the internationally recognised methodology of SABSA – Sherwood Applied Business Security Architecture) results in disjointed – and therefore highly ineffective and costly – security solutions. Clearly, it needs to be remembered that not all ICT systems used in public administration are equally important; nevertheless, some of them such as ZUS (the Polish Social Insurance Institution) systems which store information about pension savings of millions of Poles requires advanced control mechanisms to be used and supported with response mechanisms to potentially adverse events. Nevertheless, a lack of a comprehensive view on the aspects of safeguarding ICT systems supporting the functioning of the state will lead in the long term to imminent and successful attacks on this infrastructure and weakening its function.

Advances in technology not only impel the necessity to continuously update ICT-based solutions used in CI, but also generate the need to constantly adapt legislation to the changing environment by the government and regulators. The autonomous cars mentioned in the introduction will become unserviceable if relevant legislative changes that put them into service are not implemented. Such a change, however, should not be made on the spur of the moment; its implementation must be preceded with a number of studies and decisions determining the target model. For instance, it will be necessary to answer the question about civil liability (what will happen if an autonomous car is the party at fault for the traffic collision). When autonomous cars become popular, thus increasing the risk of taking over the control of the vehicle, will integrated communication systems, built upon autonomous cars, be classified as CI elements? Therefore, when discussing CI protection, the following questions need to be taken into account: what components currently comprise CI? How organisational, process, or technical solutions (including ICT) support CI and how to define control mechanisms to ensure the security of CI and, indirectly, all citizens?

Summary

This chapter has presented two groups of ICT solutions – IT and OT – applicable to CI whose undisrupted functioning is key from the point of view of CI security. It has described fundamental difference between IT and OT (i.e. systems for industrial control processes) that are particularly important from the point of view of CI protection. The article has demonstrated how individual IT and OT solutions are applied to particular CI systems.

6. Threats posed to the security of critical infrastructure in the context of the advanced application of ICT solutions – challenges for the state

Aleksander Poniewierski – EY

Before setting out to analyse the threats facing critical infrastructure (CI), or to be precise its ICT component, it is necessary to set the subject of analysis against the background of technological changes that occurred over the last three decades. These changes are fundamental to the understanding of the essence and gravity of threats in today's technological world, both in the context of information technology (IT) that helps automate information and decision-making processes and Operational Technology (OT) that serves to monitor and control industrial automation. These changes need to be considered from three main angles:

- economic change
- technological change
- organisational change

Clearly, there is a wide range of other factors that pose a threat to CI's ICT systems, but the aforementioned have a fundamental and pivotal influence on today's level of risk. It needs to be emphasised here that this phenomenon is not solely limited to our country, but has a global character and involves most installations, enterprises, and countries all over the world.

Economic change

The development of technology after World War II, especially during the 1970s and 1980s of the previous millennium, was combined with the gradual departure from major outlays being dedicated to research and development conducted in the USA, Western Europe, Japan, and the countries of the Eastern Block. Such turn of events resulted in the "patenting" of complete technological solutions while maintaining a fixed cost of their purchase. This complicated description of the automated world during the Cold War era could be simplified by comparing it to a situation in which a country or a concern spends a fortune to discover or enhance a given technology. As a result of long-term studies, a complete (the word has a crucial meaning) and self-sufficient technological solution would emerge. Being installed in a given enterprise, the solution would contain producer-specific industrial automation solutions as well as the means to control, model, and monitor it. It was quite often that IT and OT solutions developed during the research and development process were specific to a given technology and its specific version. Therefore, when we discuss the cost of a new installation, for instance a new switchboard, a new power block, or a new hydrocracking system, we speak in fact about a manufacturer-specific "turnkey" technology. Moreover, this technology was being sold and delivered throughout the entire depreciation and operation period, which excluded the scenario of setting up the installation in order for it to be subsequently serviced and maintained internally by the company's IT and OT services. It could be argued that any such interference involving these services would result in a loss of warranty or refusal to repair the damage. Hence, until the second half of the 1980s, the economics of applying IT and OT solutions referred to technology as a whole and not to its single IT components and industrial automation.

In addition, in the 1990s and at the beginning of the 21st century, a strong pressure to cut costs emerged while technology-related patents started to expire. For this economic reason (pricing pressure – cost pressure), a need arose to seek savings in technological solutions. What happened next was a great wave of standardisation of IT and OT solutions. Instead of dedicated operating systems and programming languages, classic and widely available corporate systems were introduced; instead of dedicated communications solutions and galvanically isolated transmission networks, corporate and public networks were used. This change fundamentally reduced the costs of the solution, both its purchase and maintenance. In addition, there was a strong tendency to look for cheap production facilities across Eastern markets, initially in Thailand, Malaysia, and finally – China. It did not only bring down the price even further due to the lower cost of manufacturing, but more importantly, it gave birth to cheap substitutes being manufactured by Chinese or Korean concerns. Thus, it could be concluded that the economic change (pricing pressure) changed altogether the technological market and was key to shaping the IT and OT technologies applied in CI systems.

Technological change

We have analysed above the impact of the economic change resulting in IT and OT technological modifications in critical infrastructures. This section will discuss the technological change related to the facets of scale and computing speed. This issue is often overlooked in studies devoted to the safety of IT and OT solutions. Since these changes have a considerable impact on security, these problems should be examined more closely. The above-mentioned, rapid technological change that took place during the Cold War, was a peculiar type of arms race. Acting as a barrier to technological exchanges between West and East, the CoCom (Coordinating Committee for Multilateral Export Controls) was supposed to restrict access to technologies, particularly in the IT and OT sectors which today are the foundation of CIs worldwide. Individual installations (production facilities) created IT and OT technological solutions that were specific to a given plant or refinery. Throughout years of service, they generated requirements for specific technological changes (improvement suggestions) adopted by technology producers and transferred to other installations. Alas, technological advancement and the need for a rapid expansion of installations (following the freeing of Eastern market and the transfer of production to Asian countries in particular) made it necessary to delocalise teams providing maintenance management solutions, mainly for IT and OT systems. Remote supervision of installations was being introduced and most importantly, producer's wide-ranging Configuration Databases were established, containing information about all elements of the installation. It also became necessary to provide fully mobile installers equipped with laptops and mobile devices as well as to share the ICT systems described above. For this reason (i.e. the scale and mobility as well as diversity of service and maintenance teams), the standardisation of protocols (their publication) and openness of signal-coded command-and-control servers (SCADA) were pursued. If we add to this an economically enforced replacement of technology-specific operating systems and databases for generally available market-based solutions, we get a picture of a technological environment transformed uncontrollably into an architecturally incoherent conglomerate of connections that is highly susceptible to disruption and interference. Despite this,, a popular belief prevails about the high reliability and immunity of this environment. It is one of the most misleading pictures of the IT and OT technological environment which underlies the security of the countries' CIs.

Organisational change

The above sections have alluded to the organisational layer on numerous occasions. In the context of CI security, the change in this area appears particularly important. Again, if we go back fifty years, the group who maintained technological solutions was a line of their users whom the manufacturer of the technology in question reduced to teams performing orders according to a list available in the facility and provided by the supplier. On the other side, there was a dedicated, highly qualified group of engineers that continuously and rotationally monitored the installation in different environments.

In such an organisation, the self-controlling organism equipped with checkpoints and maintenance windows could operate continuously. The organisation was concerned with only one element, namely to preserve the culture of the "mentor and apprentice." Such structuring of the educational process was necessary and sufficient to ensure the continuity of installation activity. What it meant in practical terms was that on the one hand vocational (job training) schools attached to plants were established in which the facility's workers-mentors trained young employees from the new generation (operators); on the other hand, engineering schools were founded (mainly associated with technology producers and therefore set up in Western Europe), educating staff who were familiar with a given technology and had potential for its development. Unfortunately, the balance between these two elements, educational and organisational, have been disturbed these days, which has a knock-on effect on security.

Contemporary threats associated with CI's Information and Communication Technologies systems

Contemporary threats are to a large extent associated with the changes described above. Being aware of the source of threats is a prerequisite for knowing how to develop security mechanisms. Without this knowledge and awareness, any activities undertaken to enhance security will be futile. The diagram presented below outlines the classification of threats reflecting the selection of particularly important groups of threats which can be further broken down into groups specific to CI solutions and areas. This article is not aimed at providing a systematic and complete description of all groups of threats. Instead, it focuses on those constituting core elements that need to be acted upon.

Poor awareness and a lack of education pose by far the highest threat to the security of CI's IT and OT systems and should be mentioned first. The owners of CI installations–facilities have poor awareness about the ICT-related IT and OT risks and threats. Being unaware of the influence of the economic, technological, and organisational changes on security and, as a consequence, the lack of knowledge about the effects they produce for the functioning of CI, constitute fundamental risk factors. These problems are well worth highlighting as the lack of awareness leads to insufficient interest in the subject, no funds being raised for safeguarding CIs and the overall lack of understanding of the scale of interconnections between CI facilities. This, in consequence, leads to a situation where even a single unsecured link weakens the entire chain. Unfortunately, the above-mentioned lack of awareness is also attributable to the ruling authorities (a large part of business people owning enterprises that comprise CI) as well as the managerial and executive staff. This leads to the conclusion that insufficient awareness in all levels lulls everyone into a false sense of security – the worst case scenario for those involved in risk management. The absence of systemic education provided at the levels stated above is very strongly connected to this threat. This applies to systemic education (schools and universities) which educate managerial staff, but also personnel that would be capable of preventing security incidents affecting CIs, e.g. sabotage or hacking activity. It needs to be remembered, however, that it takes about 7 years for an educational cycle to complete, so these are long-term actions, impossible to accomplish over a short period of time.

Another threat group is related to change management. This concept should be understood as a chain of actions involving the change of technology, organisation, or ownership of IT and OT systems, but also a spectrum of factors linked to the cultural change within the organization. The latter is a consequence of mergers and acquisitions between companies or a result of legislative and regulatory changes. Project changes that introduce complete and new technological solutions to the chain of CIs, such as IT and OT, open solutions or smartgrids, are particularly significant for the security of CI. The scope of indirect IT and OT network modifications is so large that it is impossible for it to be thoroughly examined and managed accordingly without holistic architectural planning. The last category within the group of change-related threats involve performance testing. At present, the issue of CI's IT and OT system testing is a highly complex and critical problem. The absence of an appropriate methodology for testing solutions and the behaviour of organisations in the event of an unexpected error is a serious global problem.

The third group of threats is related to the change in the IT and OT economic and material security paradigm. Generally speaking, the threat involves a radical lowering of possible and economically justifiable financial means dedicated to safeguarding IT and OT. The change (reduction) of outlays for IT and OT infrastructures entails the change in the economically justifiable spending on safeguards.[1] Under the scenario of economic and technological changes described above, possible expenditure on safeguards is reduced, which at the same time results in a rapid, if not radical, increase in needs arising from a heterogeneous architecture. As a consequence, we are facing a problem that will increasingly re-emerge over time while conventionally appraised and mandatory safeguards to minimize the risk will consume tens of millions Polish zloty. At the same time, the (material) value of the infrastructure itself will increasingly diminish. We will face a dilemma on whether we should safeguard or perhaps replace altogether particular sections of infrastructure. We will also face (or in fact already are facing) a dilemma on whether we should apply cheap solutions for mainstream applications (technology) such as cloud computing, use unified solutions, or perhaps view them through the prism of potential risks. In order to understand the extent of the threat, it is necessary to picture how much cloud computing is changing the need for safeguards.

[1] The economic paradigm of security assumes that the costs of safeguards can, at most, equalise the loss, but in general they should be lower.

A fourth group of threats that are fundamental to IT and OT are technology dissemination and its general availability. In recent years, when CI installations applied specialised and unique solutions, their security could only be threatened by accidental errors in production, misuse of ICT systems or deliberate sabotage by individuals having authorised access. Today, it is possible (without running into much trouble) to take over the control of individual elements of CI without the need to be physically present near the installation. There is a chance that even untrained individuals who are hundreds or thousands miles away can take over the control of the production system or its individual components. Furthermore, such activities are run by organisations either established at the state level or supported by the state (officially, unofficially), but also by non-governmental organisations and entities, which constitutes a real threat to the security of countries. It is precisely this group of threats (involving the dissemination of technology) which the decision makers nowadays find most "spectacular" and persuasive. The issues described above hold the key to understanding its essence. This group of threats has another, more complicated and unknown dimension, namely, sourcing. Enigmatically sounding yet widely prevalent in the realms of IT and OT, the word comes down to only one thing – those who create the technology and control its development have the knowledge about potential problems associated with it and can take advantage of the existing security loopholes. In the coming years, this issue (transparency of technology) will give rise to widespread controversies and concerns. This proves a key challenge.

The last group of threats for CI's Information and Communication Technologies systems are ICT solutions themselves. Although OT and IT systems are critical to the functioning of CI, they are poorly looked after (due to the lack of education on the one hand, and on the other hand the safeguarding and monitoring solutions currently applied), thus constituting the weakest link of the countries' CIs. This makes them particularly vulnerable to attacks instigated by terrorists, hostile governments, and criminal organisations whose actions may be targeted at the incapacitation of CI, its destabilisation, and in the worst case scenario, its destruction.

This may seem like a bold conclusion but – figuratively speaking – why should we ever assume that the electronics applied in the latest versions of a luxury BMW or Ferrari will be their weakest link? According to the principles of security, overcomplexity and a lack of transparency pose the greatest risk. We are afraid of what we do not understand and cannot fully use without the necessary knowledge. Then, the very object of use becomes a threat in itself. This last, slightly provocative group of threats is often touched upon at international conferences or expert forums where questions are being raised about the scale of applying ICT solutions in CI. These questions are about the future of such solutions and how to effectively safeguard and monitor them. These queries are in fact questions about security.

Summary

In this chapter the author has analysed three types of changes that took place in the realm of ICT solutions being applied to CI today. Based on these changes, four main groups of threats have been distinguished that should be counteracted. They refer to low general awareness about the threats and risks posed by the ICT aspects of IT and OT; they are associated with the problem of change, dissemination of technology and its general availability as well as economic calculations which lead to cutting down the expenditure on security; finally, they are about challenges being introduced by ICT solutions themselves.

7. ICT components of critical infrastructure protection

Włodzimierz Kotłowski – MATIC

The effective protection of critical infrastructure (CI) primarily involves the preservation of integrity and continuity of processes a given infrastructure directly supplies or indirectly supports in the chain of activities undertaken in conjunction with external structures. State-of-the-art ICT (Information and Communication Technology) solutions are applied to provide optimal protection of CI. Today, the level of protection is contingent upon the speed with which an adverse event is detected as well as the swiftness and completeness of the response to the occurring event in order to maintain the continuity of critical processes. With the incorporation of ICT into CI protection, the process of identifying resources that are critical to a given infrastructure also needs to take into account the ICT resources used for its protection, in line with inherent threats and detected vulnerabilities that compromise them, as well as the consequences for business in case negative scenarios should occur.

CI protection supported by ICT solutions

Amongst the issues of the ICT-supported protection of CI, we can distinguish the following elements:

- inventory and management of CI resources
- monitoring and management of physical access (perimeter protection of CI, internal protection, access management by authorised persons)
- monitoring and management of logical access to ICT resources
- collecting data from monitored processes/facilities, including selected industrial automation data
- collecting business environment data
- automatic analysis of data collected in real time
- data storage and archiving (including computer forensics)
- managing adverse events and crisis situations
- risk assessment and risk management
- recovery planning (scenario-based events and respective procedures)
- testing recovery plans
- information protection (confidentiality, integrity, accessibility)
- CI maintenance (service, repairs, controls)
- communication (coordination of actions, inclusion of external institutions)
- security and business continuity planning training

It is difficult to imagine these days how to carry out protective actions without implementing ICT solutions in parallel to the existing industrial ICS systems (Industrial Control System – software being part of OT systems, such as SCADA). The question whether the exchange of data between ICT and ICS is necessary should also be considered. If such a need arises, it is requisite to appropriately secure such interconnected communication channels.

The Annex attached to this report contains a table presenting a framework approach to CI protection in accordance with the methodology for enhancing ICS system security ("Framework for Improving Critical Infrastructure Cybersecurity"), issued by a U.S. agency NIST (National Institute of Standard and Technology) in February 2014. The column "Document references" quotes ICT and ICS security standards corresponding to a given issue.

All CI security management functions and processes listed in the table can be fully run by dedicated software with a central management function and the allocation and control of tasks assigned to selected individuals in line with predefined roles in the security system.

Mobile workstations and mobile devices in the protection of critical infrastructure

Immediate response of services (internal and external if applicable) intervening when adverse events occur that compromise the security of CI would be severely impeded or even made impossible (mainly due to the requirement to respond within prescribed time limits) if the entire documentation, including recovery plans, was only available as hard copies or on a digital carrier in an isolated, closed network.

Services responsible for the protection of CI should be equipped with stationary equipment (supervision, monitoring) and mobile devices that enable voice calls and the exchange of specific data (maps, plans, procedures, etc.) provided for handling negative event scenarios that are often dynamically changeable in time and require the services to be on the move.

Apart from ensuring safe connections (also encrypted if the need for it arises from the risk analysis), efficient and safe mobile communication requires that it has the software to manage all mobile devices (MDM –Mobile Device Management) that operate in the CI owner's network.

MDM software should meet the requirements of the developed and implemented mobile device security policy (tablets, smartphones, laptops) which guarantees:

- centralised control over all in-network mobile terminals
- mobile resource management – recognition, storage and reporting on mobile device data (also management of devices with multiple operating systems)
- configuration management – remote configuration of network connections
- application management – central application repository, remote distribution and installation of applications, software patches and upgrades for defined users
- protection of data transferred via a mobile network (preserving the attributes of confidentiality, integrity, and availability) together with an automatic authentication of an authorised

user (applying risk-based multi-level authentication); mechanisms to prevent sensitive data leakage (DLP – Data Leak Prevention)
- automatic data backup – creating backups for critical mobile device contents
- security management – defining, updating, and remotely transmitting security policies to mobile devices (including remotely locking devices, deleting data, changing configuration and permissions, etc. provided for in the policy)

Monitoring threats and vulnerabilities as an essential step towards better security

Implemented ICT and ICS solutions are exposed to threats which, due to their causes, can be divided into natural, accidental, and deliberate. Natural hazards, such as fire, flooding, etc., do not evoke concern as they are as old as our civilisation and we have learned how to prevent them. What makes us feel uneasy are unknown, accidental and deliberately induced hazards stemming from the currently existing vulnerabilities of resources, or vulnerabilities that are about to emerge together with new threats. The statement itself stirs up some concern – vulnerabilities that depend on dynamically changing external and internal environments can also become a source of danger (e.g. a rebellious employee). Furthermore, there are particular types of vulnerabilities associated with the use of operating systems, software, and databases. Individuals carrying out attacks on ICT or ICS resources take advantage of the knowledge they have about the latter vulnerabilities. Very often such breaches of security go undetected.

The main task lying before individuals who are responsible for the security of critical resources is to gain knowledge about the existing and associated vulnerabilities of ICT and ICS resources. If CI security is directly contingent upon the security of ICT and ICS resources, it is required then to continuously monitor the vulnerability of these resources. Recommended frequency for conducting vulnerability tests should result from the risk analysis.

The recommended features of ICT resource vulnerability testing tools are the following:

- testing tools should be safe for our systems (they should not introduce changes and damage resources)
- tests should be conducted using tools produced by only well-known and worldwide vendors (suppliers)
- vendors offering testing tools should have at their disposal an adequately large vulnerability database along with a database containing existing vulnerability-specific threats as well as additional guidelines that help the administrator to eliminate the effects of the vulnerability in case software patches should be unavailable at the time
- testing tools should detect zero-day vulnerabilities (immediately following its first occurrence in the world when no software patch has been released yet)
- testing tools should provide test results that are easy to understand for a person that is not trained and skilled in IT
- testing tools should be constantly updated in response to dynamically changing knowledge about threats and vulnerabilities considering a wide array of software used (maintaining constant communication between the tools and the knowledge base or competence centre is required; updating the base once a week may be insufficient).

The selection of methods for testing ICS resource vulnerability should be performed carefully and adequately to the requirements of the specific CI environment, its technological solutions, control system architecture, operating systems used, software and data transmission techniques. Tests cannot cause the ICS system to go unstable but secure the continuity of CI processes.

With such formulated requirements regarding the accumulation of knowledge about threats and vulnerabilities springing from operating systems and software currently in use, the idea of establishing a national competence centre in this field, i.e. a Polish company that would have knowledge and world-class testing tools, should be considered. The only question that remains is whether we can afford it and how quickly it could be set up. Other options to consider include an alliance with a worldwide vendor in this field or a joint protection of critical ICT resources within the framework of existing collective defence arrangements (the EU or NATO).

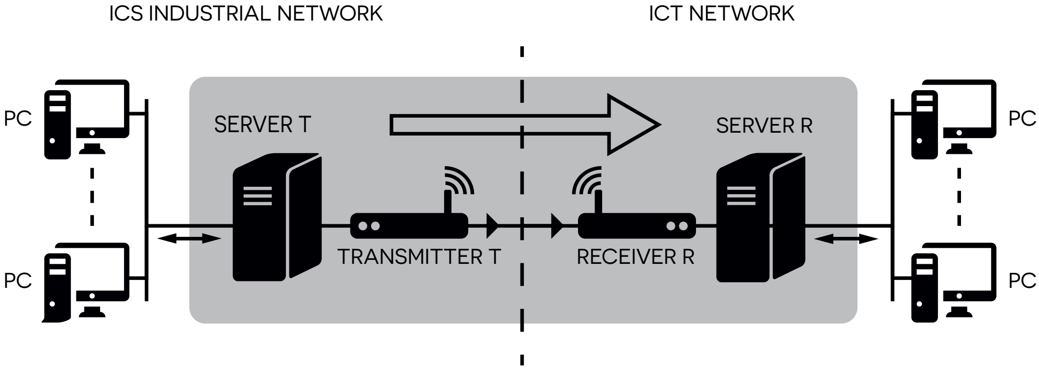
Safe integration of the enterprise's ICT solutions and IC's ICS systems

Is it absolutely necessary to isolate ICT solutions from industrial control systems (ICS)? If ICT solutions are to protect CI in real time and at the same time eliminate or considerably minimise the involvement of the attending personnel, then creating completely separate ICT and ICS systems cannot be substantiated. Necessary connections and resulting communication channels and methods should be subject to a detailed risk analysis. Conclusions drawn should determine the selection of solution architecture and the methods of two-way communication. The section below presents possible options for building interconnections between ICT and ICS.

Option 1

Applying one-way data flow (data diode) that protects against Internet attacks from external networks.

Figure 7. One-way data flow (data diode). Legend: Transmitter T – laser emitting light into the optical fibre; data can be transmitted outside but they cannot return to the protected industrial network; Receiver R – receiving photodiode. Source: own compilation. Icons come from www.nounproject.com.



Option 2

- Applying SCADA firewalls (they physically secure a specific type of communication through their electronic and optoelectronic construction)
- Applying distributed firewalls that operate inside the entire automation network in such a way that an attack on a single point of entry does not give access to the entire automation network (a good analogy for a distributed firewall architecture are bulkheads in a submarine)
- Encryption by means of equipment solutions (cipher machines and decryption devices)
- Applying multilateral authentication methods
- Automatic warning and simultaneous tracking of Quality-of-Service (QoS) parameters in an internal network

The solution presented in Option 1 (used for years in military technology) and involving switching over connection directionality can also be used in numerous processes associated with the maintenance of the ICT and ICS critical infrastructures (software updates, patch management, vulnerability tests, etc.). The switch-over could be scheduled in selected time intervals and accompanied with additional monitoring and protective safeguards.

When establishing safe communication channels between ICT and ICS, it is mandatory to conduct a risk analysis and subsequently select a solution that most adequately corresponds to the value of protected resources and processes.

Summary

This chapter has demonstrated that along with the incorporation of ICT elements into CI protection, the process of identifying critical resources for a given infrastructure should also consider the ICT resources in question. It is therefore essential to adapt undertaken actions to the inherent threats and detected vulnerabilities that compromise them as well as to couple them with consequences for business in case negative scenarios should occur. The author has also touched upon the problem of mobile workstations and mobile devices in CI protection.

8. The security of industrial control systems

Piotr Ciepiela – EY

In recent years, critical infrastructure (CI) protection has become one of the burning issues pertaining to a broadly understood concept of worldwide security. CI was more often understood to only comprise installations, facilities, and physical infrastructure in general, largely ignoring the element of industrial automation which in fact controls and manages them and nowadays constitute an integral part of the industrial environment. This area, however, is increasingly considered and readily included in CI. Such an approach has also been recently adopted in Poland.

OT (Operational Technology) security involves equipment, software (ICS systems such as SCADA/DCS), staff and any activities that are aimed at detecting and introducing changes to technological processes by means of controlling physical devices, such as pumps, valves, etc. OT security has recently become a high priority given the comprehensive view on CI protection which up to this point often came down to mere physical protection. It is due to the fact that control systems have been noted as an absolutely critical and yet at the same time the most sensitive and attackable element of CI. In addition, the attack can be carried out anonymously, remotely, and practically with no risk of suffering the consequences by the attacker who might as well be in a far corner of the world. As a result, CI cybersecurity has made it to the list of priority actions instigated by many countries all over the world, which is proven by legislative initiatives in the United States, the European Union and its individual Member States.

There are several reasons for OT system cybersecurity issues to become so prominent. First and foremost, OT systems used to operate in isolated environments which protected them against attacks or computer virus infections stemming from Internet activity because they simply worked offline. Practically tailored-made to match the needs of a given entrepreneur, OT systems constituted closed and producer-specific structures that used dedicated communication protocols (other than those in traditional IT). The security of those systems was determined by the level of their accessibility. Dictated predominantly by economic reasons, the industrial automation environment experienced a technological change which led to a greater openness of systems and a closer integration of industrial automation and IT worlds through the convergence of infrastructure (e.g. servers and control stations), communication (industrial protocols being replaced with

TCP/IP standards), and operating systems. Continual systems development and the new situation somehow urged the need to introduce new security standards already well-established in the IT domain.

OT and ICS standards in CI

Industrial systems have operated in the world for over 40 years. However, it was not until recently that protection standards and sets of guidelines started to be developed following the above-mentioned changes within the OT environment. In a very short period of time, these transformations resulted in a dramatic increase in the number of threats endangering OT systems which were totally unprepared for such a turn of events.

It was the United States who was the precursor of protective activities, remaining the biggest producer of OT standards ever since. It is worth noting that the very concept of critical infrastructure also originated in this country ("Marshall Report" 1995). CI protection in the United States is so advanced that in the key sectors, i.e. energy and petrochemical industries, regulations were introduced that impose the implementation of specific security solutions on infrastructure operators.

Another source of regulation is international organisations affiliating, inter alia, OT system users (e.g. petrochemical and energy companies).

Finally, the third source are OT solution vendors who recognised that a high-level safety for their systems can give them a competitive advantage, but most importantly, that it is a strategic area from the perspective of PR management. Subsequent media reports on attacks targeting CIs by exploiting of system vulnerabilities, which press releases increasingly mention by name, can very badly damage the image of suppliers.

Starting with governmental standards, one of the first publications that substantially and seriously approached the issue of supervisory control system security, is a publication numbered 800-82 "Guide to Industrial Control Systems (ICS) Security" issued by a U.S. agency NIST (the National Institute of Standards and Technology) in 2011. This comprehensive document for years set the standard for approaching security in this area. While failing to address technical guidance, it put a greater emphasis on network security, environmental management, awareness-raising, and employee training. However, a major flaw of all these types of "guidelines" is their model character. Typical industrial automation environments are complicated (different classes of systems supplied by different vendors and coming from different "technological eras") and at the same time practically inseparable and hard to modify due to the requirement of continuous availability. Hence, adapting to presented models has always been far more challenging than building the model itself. The supplement dedicated to industrial systems (Appendix I – "ICS Security Controls, Enhancements, And Supplemental Guidance") the NIST attached to its flagship 800-53 publication "Recommended Security Controls for Federal Information Systems and Organizations" also merits a mention. The publication is a collection of security controls applicable to the ICS environment.

Issued in February 2014, the methodology for enhancing the security of OT/ICS systems ("Framework for Improving Critical Infrastructure Cybersecurity") crowns the activities undertaken by NIST. Ordered directly by president Barack Obama ("Executive Order 13636"), the methodology provided a framework for an independent group of experts to create general guidelines on how CI operators can systemically approach the establishment of an internal cybersecurity programme.

The U.S. chemical sector is the first branch of industry that was provided with official guidelines regarding industrial automation security. The sector is controlled by the DHS (Department of Homeland and Security) which established CFATS ("Chemical Facilities Anti-Terrorism Standards"). CFATS was supposed to ensure that every organisation that produced, stored or transported hazardous chemical substances should have implemented both physical and ICT safeguards. Non-compliance could trigger the immediate shut-down of the enterprise concerned. Interestingly, DHS initially assumed that the standard would be fully and effectively enforced within 2 years – over 10 years later, it is still in the implementation stage. This demonstrated how demanding an area the security of control systems is and how comprehensively its implementation needs to be planned.

Another so-called regulated sector in the United States is the energy sector. With this industry in mind, the NERC agency (North American Electrical Reliability Corporation) created CIP (Critical Infrastructure Protection) – a set of rules regarding CI security including guidelines for control systems (commonly referred to as NERC-CIP). The first version of the publication consisted of several, very high-level guidelines (the currently available version is the 5th edition of the standard). Its main aim was to draw the attention of board members and management to the fact that such infrastructures and industrial systems existed and required protection. However, the main flaw of the guidelines was that they were not detailed enough and left too much room for interpretation. A noteworthy fact is that in the U.S. energy sector, the NERC-CIP is an absolute requirement. Its implementation is verified through compliance testing while revealed non-compliance can result in a penalty of up to USD 1 million per day of non-compliance.

From the point of view of the sector-specific approach, two more sets of guidelines deserve to be mentioned:

"API-1164 – Pipeline SCADA Security" and "API-1165 – Recommended Practice for Pipeline SCADA Displays", both developed by the American Petroleum Institute for the petroleum refinery sector. These documents are a collection of ICS security system rules which can be successfully applied to other sectors as well. Conversely, the American Gas Association created "AGA-12" (SCADA encryption) for the gas sector. The entire standard is exclusively devoted to encryption, which can be surprising considering the fact that the gas sector has no special additional requirements in this area. This example perfectly illustrates that while every sector made attempts to set down industrial automation security guidelines, the scope they covered was not necessarily similar. Given the time of the publication (2005), the state of systems at that time, and no formal requirement to comply with the standard, its implementation remained at a low level.

At the European Union level, the activities of ENISA (European Union Agency for Network and Information Security), the Community's agency for security should be noted. At the end of 2011 and the beginning of 2012, ENISA issued a document "Protecting Industrial Control Systems – Recommendations for Europe and Member States" which described the situation of industrial system security at that time as well as seven steps to improve security in this environment. The publication drew attention to the need for creating national and pan-European strategies for OT/ICS system security as well as the necessity to improve education and raise awareness of the society in this respect.

Other Members States are also developing their own internal standards. For instance, Germany and Great Britain have their own mature regulations whereas Estonian CI operators take advantage of the government-sponsored industrial automation security controls.

Currently, the biggest ever worldwide undertaking that brings together independent industrial automation and cybersecurity experts as well as the representatives of ICS-class solution producers is ISA (Instruments, Systems and Automation Society). ISA99 in particular is a body established to lay down a set of security standards for industrial automation. These norms are therefore created by individuals who both work with ICS systems and perfectly understand the specific nature of this environment. The guidelines developed so far are so popular and effective that they will become an official series of IEC standards (International Electrotechnical Commission) with a reference number IEC 62443. So far, ISA has issued the following publications pertaining to OT security:

- "ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models"
- "ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems"
- "ANSI/ISA–99.02.01–2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program."

The most anticipated standard ISA 99.03.03 ("Security for Industrial Automation and Control Systems – System Security") that specifically addresses the security of industrial systems is still under development.

Solutions that safeguard and enhance security

In a sense, the standards described above are supposed to provide a structured approach to specific industrial system security-related areas. However, most of them are not universally applicable to all solutions and sectors. The aim to ensure utmost security in technologically varied, highly complicated and widely accessible environments is not easy to accomplish, let alone possible. One of the methods to increase security is to apply an approach known in the computing world as "defence in depth". Clearly, transferring IT solutions without adequate changes to the OT realm is far more dangerous than maintaining the status quo. Sometimes, it is possible, however, to employ a well-known solution at least at a conceptual level. Regardless of the type of environment, the "defence in depth" approach attempts to provide multiple layers of protection. However, it is always best to consider such protection in three fundamental dimensions: technological, organisational, and process-related. Each of these dimensions should be appropriately secured; otherwise the technological process can be easily disturbed.

The technological dimension of security involves safeguarding equipment starting from the lowest level, namely installation devices, to controllers (PLC/RTU) directly connected to installations, to industrial systems. Securing the exchange of data between individual elements of the environment, thus the appropriate safeguarding of the network layer (both industrial protocols and network devices), cannot be overlooked. The area that is closest technologically to IT encompasses the safeguarding of servers and workstations along with the operating system used. The final vital issue concerns the physical security of the installation – the most widespread method of infrastructure protection practised so far. Irrespective of a significant rise in cyber threats, it is still indispensable to protect the infrastructure against ordinary acts of vandalism committed with a traditional "hammer."

The organisational dimension entails creating an appropriate organisational structure of individuals responsible for security in the company and the following tasks: allocation of roles, knowledge management and competence building, provision of knowledge at an appropriate level, and awareness-raising. It also includes personnel management, e.g. verification that a given employee did not imperil industrial systems in a previous workplace (employee references).

Finally, the process-related dimension involves identifying and defining technological and managerial processes followed by the development and effective implementation of a set of internal policies, procedures, and technical standards that lay down the principles of operation in the industrial automation environment. The procedures that need to be taken into account include adequate change management in the aforementioned environment, user and incident management, supply management, and securing the continuity of the process.

This is what a general approach to increasing security looks like. Notwithstanding the adopted model, it is worth drawing attention to the three most fundamental problems.

1. The first is identification and possible elimination of SPOFs (Single Points of Failure). The adequate redundancy rate of key infrastructure elements must be able to preclude the situation in which a failure of a small switch can result in installation downtime. As it turns out, hardly any enterprise has actually performed such an analysis, thus being perpetually dependent on potentially insignificant elements of infrastructure.

2. Isolation from the outside world understood as external networks such as the Internet and office network is another area. It does not denote, however, a galvanic isolation, i.e. a philosophy that accompanied the industrial automation environment in the 1980s and 1990s when these systems were genuinely and completely separated. However, due to technological evolution, network integration, or simply routine business requirements to immediately receive managerial information from production, these networks are largely, or will be in the near future, connected to the corporate

network. This trend cannot be reversed. It requires a difficult architectural task to be performed, namely to appropriately organise and secure communication channels with the office environment as well as to control any attempts to access ICS systems remotely.

3. The last point in our discussion refers to an issue that is partially organisational and partially related to the awareness among ICS system users. Historically, the supply of the entire system designed to perform a specific function was very often the responsibility of the system-supplying vendor. It would not seem odd and concerning – after all, the supplier supervised the system and its accessibility – if, as a consequence, it did not lead to a situation when the enterprise could end up having poor knowledge about the system architecture, possibilities for its configuration, development, etc. This could result in the permanent inability to either develop the system or to introduce even the simplest configuration changes in case the supplier should go bankrupt, not to mention a complete paralysis in the event of a failure. Another example of an extreme scenario is a so-called "vendor lock-in" where the supplier of the key system makes the customer pay exorbitant prices for every modification or configuration change. Due to no access to the source code and knowledge of the system logic, no other vendor can perform these tasks.

Therefore, it is mandatory to be familiar with one's own systems and exercise some form of control over suppliers, e.g. through source code escrow arrangements. In short, the latter is a method to secure the interests of the company that involves entrusting the source codes of the IT solution to a third party. In case the vendor should go out of business, the third party passes on the source code to the company. These types of safeguards deserve to be considered as they apply to systems comprising CI and therefore have a major impact on a considerable part of the citizens.

Techniques and methodologies for creating an integrated CI security management model for OT and IT

Attempts to implement security solutions without the management layer are bound to be unsuccessful in the long term. Security is a process that has to be constantly checked upon to ensure it is properly defined and managed. Therefore, the creation of an integrated model for security management is still a very relevant and up-to-date topic. To draw an analogy with IT again, there is a well-known guidance document, namely the norm ISO27001, which sets down guidelines on how to establish an information security management system. Alas, the norm has been developed exclusively with the IT sector in mind (emphasising information processing), so it cannot be fully used in the context of industrial automation. While in the realm of IT security is tantamount to confidentiality of information, OT is predominantly concerned with securing an industrial process – its continuity and integrity. Therefore, the first difference may be the issue of protection against malicious software. Inasmuch as IT should apply such solutions everywhere and as much as possible automate the process of updating and eliminating threats, for OT deletion or even simply the putting of files in quarantine may bring the entire industrial installation to a standstill. Another example is a seemingly straightforward thing such as a password change. Although the justification for the idea is indisputable, it nevertheless gives rise to certain problems. A simple change of password in the SCADA system may turn out to be quite problematic as the account with a standard password can be used for instance once every six months and fail in the most critical moment. The complexity of passwords should also be thoroughly contemplated as the speed with which a password is entered will decide on human lives being jeopardised by the failure of the installation. In a potentially life-threatening situation, humans tend to make more mistakes; therefore, mistyping the password three times in a row and locking the account may do more harm than good. The same holds true about the automatic shut-down of sessions at operating stations.

ISO27001 does not provide recommendations on how to set up the network architecture – practically one of the most crucial aspects of OT security. It does not mention server or workstation level devices either. Although similarities between OT and IT are numerous, if we move on to compare controllers and information exchange protocols, the differences in their approach to security will prove significant.

In principle, the ISO27001 norm should be considered a supplementary document. However, the implementation of its principles to the OT realm should be preceded with a critical analysis of its appropriateness.

Considering the available literature, the guidelines on how to set up a security system or a programme has been described in the aforementioned NIST 800-82. However, the actual explanation of how to establish a security management system for industrial automation can be found in the "ISA-99.02.02 Security for industrial automation and control systems – Operating and IACS Security Program." Interestingly, at a conceptual level, it is recommended – similarly to ISO27001 – that a Deming Cycle-based system is introduced (Plan/Do/Check/Act). The cycle and guidelines themselves were, however, developed with industrial automation systems and technological process security in mind; hence different sections of the document describe how to perform organisational set-up, how to segment the network, how to approach system updates, etc. Following the widely accepted rule, the cycle should involve:

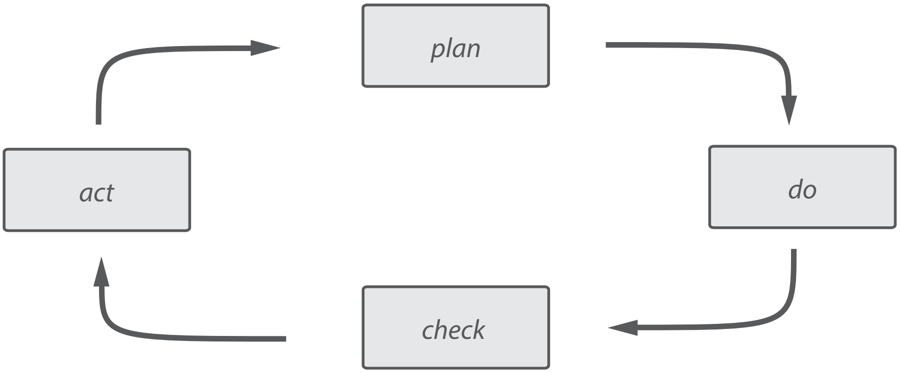
Plan: establishing the security management system policy (SMS) for ICS systems together with adequate objectives, processes, and procedures enabling the risk to be managed and the level of security to be increased

Do: implementing and utilising SMS for ICS systems in the sense of applying processes, policies and procedures

Check: assessing and measuring the effectiveness of the process as well as reporting on results

Act: introducing corrective actions based on the results of security controls and audits of SMS for ICS systems in order to continuously improve SMS.

Figure 8. The Deming Cycle. Source: own compilation



However, the fundamental step is to appropriately identify the ICS system security requirements and lay down a set of procedures and guidelines. Moreover, the implementation of controls is needed in order to enable the industrial automation risks to be managed as an integral part of the enterprise's business risks. Finally, it is necessary to monitor the effectiveness of the security management system to constantly improve it based on the degree of objective accomplishment.

Organisational structure and awareness-raising measures

Efforts to considerably raise the awareness about the security of industrial automation systems must be realised both at the state (protection of its own CI) and company levels (protection of its own resources).

The role of the state is to prompt educational efforts involving the introduction and update of appropriate IT education programmes at schools and universities.

Moreover, the state as a CI security stakeholder should motivate CI owners and operators to implement safeguards which overall are in the interest of general public. Following the example of the highest developed countries security-wise, the incentives (e.g. tax reliefs, lower insurance premiums, or state-sponsored training and expert support for business resembling the solution adopted in Estonia) should both encourage entrepreneurs to invest in security and legitimise certain rudimentary standards that will subsequently and gradually be developed to adapt them to the growing scale of threats. While awareness-raising is indispensable, it is also necessary to consider the introduction of mandatory security requirements similar to NERC-CIP. Described in fairly simple terms, they draw attention to the problem of management board security and at the same time penalise for non-compliance. As life shows, the mere awareness of existing threats hardly translates into practical applications to the extent we would wish for. With no Highway Code and penalties for not observing it in place, the situation on the roads would be far worse than it is today. Therefore, we should follow in the footsteps of the highest developed countries.

While enterprises should be high on a training list, each company should in fact consider training its priority as preventive actions and personnel's awareness considerably minimise financial losses. At the enterprise level, technological and organisational safeguards should be considered to either eliminate or minimise the set of required actions to those that are absolutely indispensable. It is also necessary to appropriately monitor the environment in order to have an intimate knowledge of one's own infrastructure as well as to be able to identify and adequately respond to any occurring changes. Representing distinct types of enterprises, ICS solution suppliers should be subject to strict regulatory requirements that force them to comply with security standards. As numerous examples demonstrate, their peculiar light-hearted and, in a sense, incomprehensible trust in their own solutions have led to the occurrence of ill-famed incidents and the creation of cyber weapons targeting industrial installations. In the past few years, producers could persuade their customers that their solutions were safe by trusting that their highly unique and low-profile solutions will not rivet the interest of cyber criminals. This era is now long gone.

Summary

This chapter systematises information pertaining to standards increasing OT security in CI. In addition, it has discussed solutions which ensure and increase security in three dimensions: technological, organisational, and process-related. The author has also commented on issues such as the elimination of single points of failure that are key to the functioning of CI, separation from the external environment, and awareness-raising activities.

9. Critical infrastructure and incident response

Mirosław Maj – Safe Cyberspace Foundation[*]

The domain of ICT-based critical infrastructure (ICT-CI) requires a well-organised incident response process. Practice has demonstrated that the supervision and control of devices responsible for overseeing this infrastructure is directly exposed to virtually all Internet-originating threats. The series of serious security breaches affecting SCADA systems world-wide has proven that the problem is real and the attempts to sweep it under the carpet can be particularly dangerous. The Stuxnet incident provides the most spectacular evidence in this respect. Along with advances in ICT security technology and processes, the experts recognise that incident response is becoming increasingly important over time and should not be neglected as a preventive action.

The observation of trends in incident response (IR) for ICT-CI demonstrates the existence of two implementation paths, followed by a third one that is currently emerging.

First of all, the IR function is a task often attributed to either government or army CERTs. This happens predominantly in Europe: in Spain, Lithuania, Luxembourg, Finland, Denmark, Slovenia, and Georgia. A similar situation exists in Poland where government CERT.GOV.PL communicates that "CERT.GOV.PL engages with and considers its prime 'constituency' all users of ICT systems within the public administration (in Polish: domena*.gov.pl) as well as entities that comprise the ICT critical infrastructure of the state."

This trend is closely linked to a historically important role of European CERTs whose active and effective actions led to a situation where critical IT security issues are tackled by these types of organisations. When the concept of CERTs was also adopted by public administrations of the majority of European countries, government CERT departments have started to be entrusted with the most important tasks.

Another method of tackling the issue of incident response in the area of ICS-CI is a U.S. style, task-based approach, typical to Northern Americans. It led to establishing a new entity – the Industrial Control Systems-CERT (ICS-CERT) – whose actions focus on specifically defined tasks. In contrast to government CERTs, ICS-CERT engages in issues pertaining exclusively to ICT-CI

[*] The article was partially published in *CIIP focus,* a bulletin issued by the Government Centre for Security.

protection. The United States, which is the cradle of the CERT philosophy, also has a federal CERT – US-CERT as well as the CERT Coordination Center, the first centre of its kind established in the world in 1988 which plays a leading role in activities that improve national ICT security.

It is worth noting another trend where the role of IR in ICT-CI is being assumed by newly established organisations concentrating all functions associated with cyberspace security in a given country. This happened for instance in the Netherlands where the local government CERT (GOVCERT.NL) evolved into the National Cyber Security Centrum.

By avoiding the assessment of individual models, which would only be possible if detailed studies investigating the effectiveness of individual solutions were performed, let us move on and take a look at the U.S. solution. As it was mentioned, the selection singles out this model for purely practical reasons: due to narrowed down and precisely defined expectations, ICS-CERT does only what a CERT responsible for IR in ICT-CI should do. As a result, the observation of activities of such a CERT gives an opportunity to identify the most critical tasks.

Incident response tasks following the example of ICS-CERT

Set up as a division of the Department of Homeland Security, ICS-CERT operates as part of the "Protected Critical Infrastructure Information Program" (PCII Program) and "Control System Security Program" (CSSP). The latter programme brings together other ICS-CI initiatives, including incident response. US-CERT, a federal government CERT, also participates in the programme. The main aims of the programme include:

- analysis and safeguarding CIs and protected systems
- identification of systemic vulnerabilities and risk assessment
- supporting business continuity procedures and recovering resources and services under attack

The programme is supposed to ensure that the representatives of the private sector, who, as we know, own a decisive majority of CIs, have access to confidential information about ICT-CI security and can share it safely and without the risk of disclosing it to an unauthorised audience, which according to the authors of the programme could additionally heighten the risk. Apart from information exchange itself, the programme intends to encourage the exchange of experiences and collaboration to improve security and the coordination of efforts to repel threats. It appears that ICS-CERTs are best positioned to take on these tasks.

In order to achieve the above-mentioned objectives, two working groups were created:

- Industrial Control Systems Joint Working Group (ICSJWG)[1] – for collaboration with the private sector
- Control Systems Security Working Group (CSSWG) – for representatives of federal institutions

ICS-CERT is active in two major areas of CERTs activity: responding to security-breach incidents and conducting continuous warning, awareness-raising, and analytical activity. Some of these services are provided via other entities. First and foremost, incidents related to

[1] ICS-CERT, https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG, [accessed: 25/05/2014].

system weaknesses or malicious software are reported to the CERT Coordination Center which specialises in these two fields. Conversely, phishing incidents are "forwarded" to the US-CERT. The ICS-CERT itself focuses its efforts on incidents directly related to ICT-CI. Incidentally, this example is a perfect illustration that a task-based approach and setting up new structures is possible due to a very precise allocation of responsibilities.

As far as warning, analytical, and awareness-raising actions are concerned, it is recommended that the IR team publishes information such as

- advisories including the latest news about vulnerabilities and exploits that target them
- special alerts that are issued in situations requiring particular attention and response
- newsletters that combine in one place all information gathered on specifically selected topics. They are specifically designed for staff engaged in ICT-CI protection
- awareness-raising reports, namely materials and information (e.g. about various planned initiatives and conferences) that are valuable tools helping raise the awareness about the necessity to ensure ICT-CI protection
- technical reports from risk analyses
- periodic reports (including annual reports)

The CERT team should supplement these proactive efforts by providing either online or onsite training.

Types of ICS-CI-related incidents

In order to present types of incidents that most commonly affect ICT-CIs, we drew upon data from two major areas: Member States of the European Union and the United States. In the former case, data came from the European Network and Information Security Agency (ENISA). They cover incidents reported to ENISA in 2012[2] under the so-called Article 13a[3]. To begin with, it should be emphasised that this is a second report that has been published since the obligation to report such cases was introduced to the Framework Directive. This obligation applies to telecommunications operators who are required to report incidents to national authorities regulating the telecommunications market.

In 2012, 51 incidents were reported to the Agency (they occurred in 2011) whereas in 2013 it was 79 cases. However, the increment is not as dynamic as the numbers would suggest as it is strongly determined by the number of reporting countries. In 2013, it was 20 whereas last year it was 28. Not all reporting countries recorded significant incidents. There were only 18 in total that did. However, no information is provided that would specify which countries reported exactly or how many and what kind of incidents occurred in the countries concerned – all details are shrouded in secrecy.

As it was mentioned at the beginning, incidents are reported to National Regulatory Authorities.[4] According to the adopted workflow, National Regulatory Authorities should share

[2] The report is the latest publication issued by ENISA (April 2014).

[3] The full report is available on the ENISA website: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 [accessed: 25/05/2014].

[4] In Poland, it is the Office of Electronic Communications.

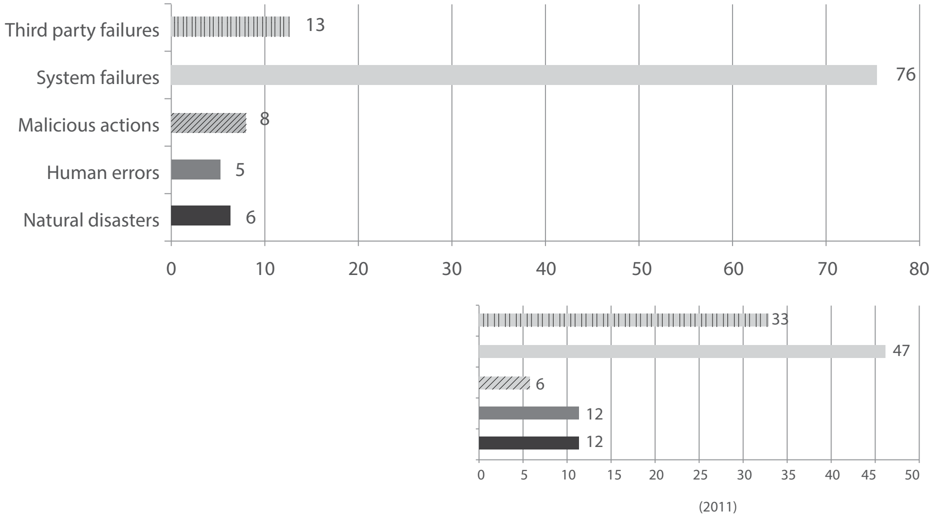
incident data with ENISA and their counterparts in other countries in case the breach of security should have cross-border ramifications as well as submit an aggregated report to ENISA on an annual basis. Events that should be reported are described as "security incidents, which had a significant impact on the continuity of supply of electronic communications networks or services."

The examples of reported incidents are the following:

- a switch from temporary network services to a target network solution caused the VoIP services to be unavailable to 400,000 users
- a faulty update of one of the core routers stopped IP-based traffic, causing a number of services, including the emergency number 112, to go down. The incident resulted in a 17-hour downtime affecting 3 million users
- copper cable thieves cut optic fibre cable. The Incident led to a 10-hour outage of fixed telephony and fixed Internet for 70,000 and 90,000 users respectively.
- a series of DDoS (Distributed Denial of Service) attacks targeting DNS (Domain Name Service) resulted in 2.5 million of users having no access to mobile Internet for 1–2 hours
- telecommunications operator implemented a faulty system update at a Home Location Register (HLR) causing a failure that impacted mobile telephony and Internet-based services. The incident affected half of the operator's customers and lasted for 8 hours

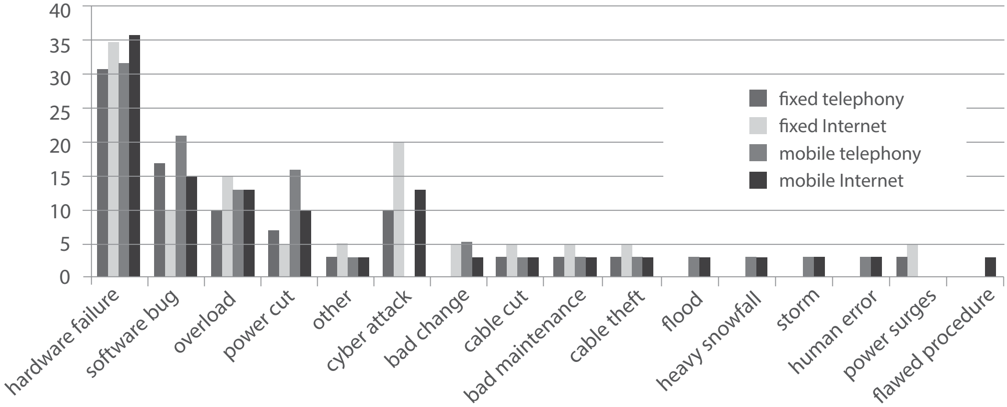
As the above quoted examples demonstrate, the cases reported are to a large extent related to incidents caused by involuntary action. Nevertheless, the DDoS attacks on DNS prove that deliberately induced incidents also occur. The report identified five chief root causes of incidents listed in the order of occurrence: system failure (76%), third party failure (13%), malicious action (8%), natural phenomena (6%) – that cause the longest-lasting incidents (36 hours on average) – and human errors (6%). Interestingly, quite a significant change occurred compared to the preceding year when third party failures accounted for 33% (one in every three cases).

Figure 9. Security-breach incidents by root cause category. Source: ENISA Annual Incidents Report 2012.



Although the number of computer-related incidents is quite low, they nevertheless merit a brief analysis. Naturally, they are classified under the malicious action category which, as we remember, comprises 8% of cases. If we take a look at the statistics presenting the detailed root causes of incidents, we will discover that "cyber-attacks" induced six incidents, which makes them the sixth most common root case. It is noteworthy, however, that if we confine our considerations to attacks on the Internet network exclusively, it will transpire that cyber-attacks are the second most common cause of incidents. In all categories, hardware failure prevails as a dominant root cause of incidents.

Figure 10. Detailed root causes of incidents by service. Source: 14 ENISA Annual Incidents Report 2012.

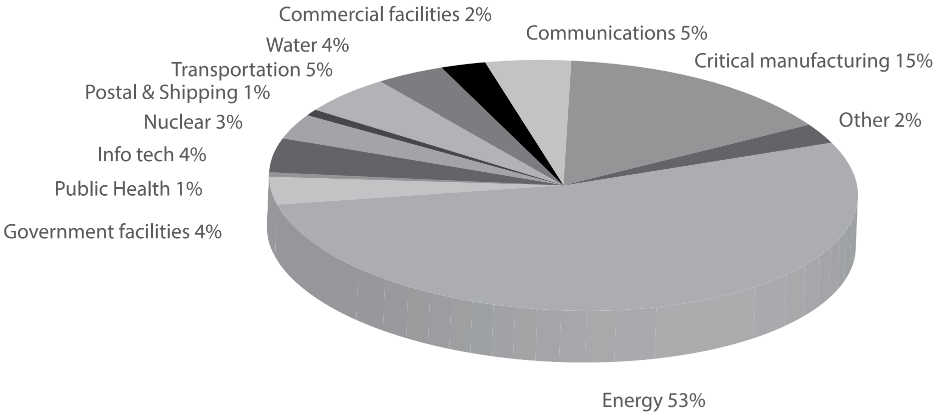


In the report, ENISA also provided criteria that should be taken into account when reporting incidents. These principles serve as guidelines for telecommunications operators and national telecommunications market regulators on how they should investigate their cases. According to the guidelines, every incident where the service outage is longer than 8 hours (even if it affects only 1% of users) or applies to more than 15% of service users (even if it lasts only 1 hour) should be reported. These are the threshold criteria for the two characteristics (duration and the number of users affected). A table showing the complete breakdown of thresholds can be found in the report.

As regards incidents reported to the U.S. ICS-CERT, in 2012 the team recorded 198 incidents while in the first half of the first year 2013 (October 2012 – May 2013) as many as 200 incidents were reported. More than half of them (53%) was associated with the energy sector with the most common types of attacks involving SQL Injection, spear-phishing (phishing targeting specific individuals) and "watering hole"[5], an attack strategy aimed at those who seem "immune" to spear-phishing. In the case of the U.S. organisation, we have access to very detailed information about the nature of the attack.

[5] See RSA, *Lions at the Watering Hole – The "VOHO"* Affair, https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/.

Figure 11. Breakdown of incidents reported to ICS-CERT in the first half of 2013. Breakdown by individual sector. Source: ICS-CERT Monitor, April-June 2013



Summary

This chapter has discussed tasks that face the entities responsible for responding to incidents occurring in CI's ICT systems. For this reason, it referred to the example of the U.S. The author has also examined types of incidents recorded in the ICT-CI environment by referring to data gathered by ENISA. They demonstrate that the problems to a large extent resulted from involuntary action. Based on the U.S. data, the CI sectors with the highest number of incidents have been identified. The analysis showed that the highest number of incidents reported occurred in the energy-related sector.

10. The concept of capacity development in the critical infrastructure cybersecurity of the state

Ryszard Antkiewicz, Michał Dyk, Rafał Kasprzyk, Andrzej Najgebauer, Dariusz Pierzchała, Zbigniew Tarapata – Modelling, Simulation and Computer-Assisted Decisions in Conflict and Crisis Situations Research Group, Institute of Computer and Information Systems, Faculty of Cybernetics, Military University of Technology[*], Mirosław Maj – Safe Cyberspace Foundation

The chapter presents the concept of an IT toolkit that improves the effectiveness of detecting, countering and neutralising the effects of cyber threats. Drawing upon sensor and vulnerability scanner collected data, the toolkit should enable the effective identification and classification of cyber-induced threats and vulnerability analysis in order to facilitate the effective use of mechanisms that counter and neutralise danger. The proposal to build an original taxonomy as well as formal models and patterns of cyber threats is the backbone of the presented idea. It will also underlie the development of the methods of identification and classification, detection and analysis of ICT system vulnerabilities, optimisation of both sensor networks and mechanisms for countering and neutralising the effects of cyber threats. The presented concept dovetails into the domain of the defence and security of the state, particularly the acquisition of new defence capabilities such as the state's cyber defence. Hence, its wide use can exceed a purely military realm and, for instance, encompass crisis management at various levels of central and local administrations.

Cyberspace

The beginning of the 21st century was dominated by the globalisation of processes and the rapid development of the Internet and other telecommunications networks. What is becoming conspicuous is an ever increasing dependence of the public administration, private institutions and society as a whole on the proper functioning of communication networks and IT systems. Also the Internet itself is increasingly perceived as a highly vulnerable infrastructure,

[*] The head of the unit is Professor Andrzej Najgebauer, PhD, DSc, Military University of Technology, Warsaw.

upon which the security of the state is heavily reliant. To carry out a successful attack on this critical infrastructure (CI) does not require mobilisation of the troops. Equipped with standard computer technologies and relevant knowledge, an individual is capable of carrying out an attack that could have catastrophic consequences for the modern political and economic system. Therefore, it is extremely important to have the capacity to detect, counter, and neutralise the effects of these types of threats in good time.

The notion of cyberspace was first used in 1982 in a short story "Burning Chrome" by William Ford Gibson and subsequently in his novel "Neuromancer" where it was used to describe "mass consensual hallucination" generated by computer networks. Gibson understood cyberspace as space filled with data and/or information which could be physically penetrated by characters. Nowadays, cyberspace is defined primarily as virtual space in which open communication takes place via computer networks or other digital media (e.g. mobile telephony). This definition was coined by Pierre Levy in his paper "Deuxième Déluge" (The Second Flood). It is difficult, however, to speak about a universally acceptable definition of cyberspace. Nevertheless, certain common characteristics are being flagged: fluid, pliant, and intangible in nature; inability to explicitly delimit it; decentralisation; the absence of a control and supervisory centre; widespread availability; digital information processing and highly accurate computation in real time; numerical, hypertext, interactive and, finally, virtual character.

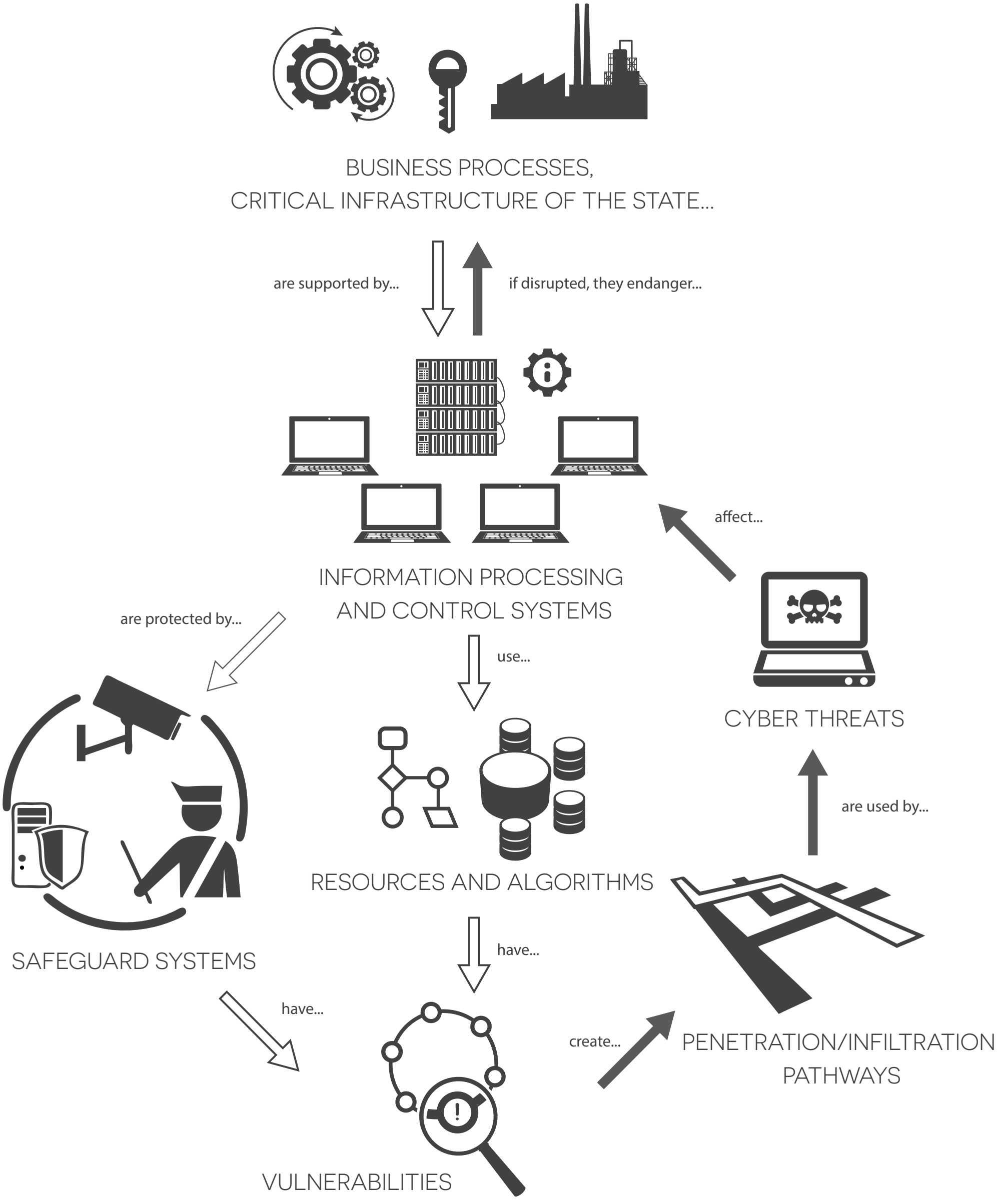
The key factor that will determine the success of the presented idea involves the definition of fundamental concepts related to cyberspace and phenomena that occur within it as well as the ability to establish dependencies between these components. The concept will put a particular emphasis on the building of the taxonomy and cyber threat mathematical models. The idea behind the approach has been outlined in Figure 12.

A rapid advancement of the Internet has caused cyberspace to grow in popularity (this is also why both notions are often used interchangeably). In this context, cyberspace can be understood as space where information that is "generated" by collaborative ICT systems is produced, collected, processed and shared. It is also perceived as a new type of social space where people can "meet." Given the features listed above, cyberspace is also increasingly seen as a domain that is extremely vulnerable to attacks. What is particularly emphasised is the fact that since the Internet cannot be treated as a legal entity and is neither a subject of law, no physical or legal person exists that can be made liable for what is happening in the network as a whole. Neither state (cyberwar) nor non-state entities (cyber criminals, cyber terrorists) can be ruled out as potential cyber aggressors, which constitutes a major challenge for the majority of contemporary countries.

It should be added that the definition of cyberspace that is currently in force in Poland can be found in the Act of 30 August 2011 o*n the amendment of the Act on martial law and the competences of the Chief of the Polish Armed Forces and regulations governing his subordination to the constitutional bodies of the Republic of Poland and other acts* (Journal of Laws of 2011 No. 222, item 1323).[1]

[1] Cyberspace is understood as the domain for information processing and exchange, created by ICT systems and determined in Article 3, point 3 of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Journal of Laws No. 64, item 565, with further amendments) along with connections between them and relations with the users.

Figure 12. Diagram of relationships between elementary cyberspace concepts. Source: own compilation. Icons come from www.nounproject.com.



The concept of implementing an IT toolkit that improves the effectiveness of detecting, countering and neutralising the effects of cyber threats

The capacity to ensure the cybersecurity of the state's CIs includes trained personnel, procedures, organisation, tools and doctrine. The presented concept solely involves the development of tools and procedures. A separate issue that requires supplementation is the development of a doctrine for their use, a suitable organisation at a state and individual institution levels as well as training and maintaining preparedness of suitable personnel.

The proposed IT toolkit is essentially based on applying cyberspace threat driven mathematical models and vulnerabilities of protected systems as well as mathematical methods that allow for the identification and assessment of threats, the evaluation of the degree of vulnerability and the optimisation of structures, parameters and operating methods of the cybersecurity assurance system. The utilisation of the aforementioned models and methods in the area of cyberspace security is by no means a completely new approach. However, what makes the proposed concept stand out from the others is its comprehensiveness and the fact that it incorporates issues which so far have been poorly explored, namely the optimisation of sensor networks and mechanisms to counter cyberattacks or the enhancement of mechanisms to counteract the effects caused by the occurrence of cyberattacks.

It will be possible to develop such an IT toolkit through the realisation of the following partial tasks:

Task 1: Developing a taxonomy and formal cyber threat model assumptions

As part of the task, a review of existing taxonomies will be performed in order to assess their relevance for constructing IT tools to improve the efficiency with which cyber threats are detected, countered and neutralised. As a result of the review, one of the analysed taxonomies will be recommended for either adaptation or suggestion for creating an original catalogue of cyber threats that will form the foundation for the execution of subsequent tasks. The analysis should include, inter alia, such classifications as eCSIRT (The European CSIRT Network), CVE (Common Vulnerabilities and Exposures), Common Language for Incident Response, and CAPEC (Common Attack Pattern Enumeration and Classification). In the process of analysis and evaluation of standards that could be used for threat modelling, the following standards should also be taken into consideration: OVAL (Open Vulnerability and Assessment Language), XCCDF (Extensible Configuration Checklist Description Format), OCIL (Open Checklist Interactive Language), IODEF (Incident Object Description Exchange Format), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration).

The presented concept assumes that a part of the task will involve describing patterns and procedures for the execution of selected types of attacks (most critical from the point of view of the security of the state, including those targeting CI) from the developed catalogue of cyber threats.

Task 2: Developing formal models and patterns for selected cyber threats

The execution of this task will involve the development of mathematical models for cyber threats (significant from the point of view of state security) selected from the catalogue of cyber threats (outcome of task 1) on the basis of which cyber threat identification and classification methods will be performed (outcome of task 4). The building of the mathematical model requires TTP (Tactics, Techniques and Procedures) used in cyberspace to carry out attacks, particularly those identified and described in task 1 to be diagnosed as well as ICT system vulnerabilities to be recognised.

Performing a detailed analysis of methods of attacks requires access to historical data on attacks that were detected in the past and the engagement of ICT security experts. It will allow essential parameters of mathematical models underlying the identification and classification of cyber threats to be established. The next step will involve the development of patterns (parametrised models) for selected types of cyber threats. It is also assumed that the mathematical models and patterns produced should be used to depict and identify new cyber threats. This will allow for new and previously unencountered threats, constituting peculiar anomalies (deviation from "normal or typical" situational patterns) to be taken into consideration.

Task 3: Developing methods for analysing the vulnerability of IT systems to cyberattacks

Defining a formal model to describe vulnerabilities for selected working conditions in which ICT systems operate must precede the actual development of methods for analysing the vulnerabilities of ICT systems. Such a model will enable vulnerability patterns (signatures) to be constructed. This, in turn, will provide the basis for developing effective methods of vulnerability detection which will simultaneously generate fewer false-positive reports. The methods for identifying vulnerabilities will take into account the ICT system work environment (the type of ICT environment and the type of cyber threats in particular). Apart from standardised LAN network environments, it is necessary to consider teletransmission and IT systems found in networks serving CIs, including industrial control systems such as SCADA (Supervisory Control and Data Acquisition).

The methods of vulnerability analysis will allow for the consequences of successful exploitation of specific vulnerabilities to be assessed by considering the type of a threat and the specific nature of the environment in which the vulnerability may occur.

As part of task execution, currently used vulnerability rating standards that are likely to influence the formal model and the vulnerability analysis method should be examined, including CVSS (Common Vulnerability Scoring System) and CCSS (Common Configuration Scoring System).

Task 4: Developing the method for identification and classification of cyber threats

The task should start with reviewing the existing methods and tools for cyber threat identification and classification. The presented concept in particular envisages the use of methods drawing upon the time series analysis, stochastic networks, including Bayesian networks and hidden Markov model, Petri nets, attack graph models, models for social networks (botnet modelling) and game models. An important differentiator of the presented approach is its natural assumption that cyber threats can be complex. This means that two (or more) different attacks can be carried out against a predetermined system at the same time. One of the attacks can be designed to absorb the attention of the system protection team so that the other "proper" attack can be carried out successfully. The catalogue of cyber threats (outcome of task 1) as well as formal models and patterns of selected (important for the security of the state) types of cyber threats (outcome of task 2) will have a significant influence of the final shape of the methods used for the identification and classification of cyber threats.

The algorithms developed to identify and classify cyber threats will determine the work being done as part of tasks associated with the sensor operating principles (task 5), management (task 6) and the optimisation of a sensor network (task 8).

Task 5: Developing sensor operating principles

As part of this task, a review of hardware devices and technologies used to exercise the function of a network sensor should be performed. Under consideration is the use of passive probes, typical for HIDS (Host Intrusion Detection System) and NIDS (Network Intrusion Detection System) based systems, as well as methods for collecting representative samples of suspicious network traffic, e.g. by using "honey pot" type techniques. While the sensors should collect data significant for the method of identification and classification of cyber threats, the method itself should effectively operate by linking to data which the sensors are capable of providing; hence, the coordination of tasks 4 and 5 is so extremely important.

Under consideration are two basic functions of the sensors, i.e. related to network traffic analysis and tracing. The former should allow for examining the contents of transferred packets, detecting traffic/communication with specific addresses in the network (particularly with the so-called "darknet", an area within the Internet that should not occur in the network traffic) and finally signalling a change in traffic characteristics.

The other function should enable non-standard or forbidden system calls to be detected, which would suggest that the control over the process has been taken over and its appropriate performance modified.

A successful completion of the task will lead to recommendations being submitted as to the potential and appropriate locations where ICT network monitoring sensors can be deployed.

Task 6: Developing a management method for a sensor network

The operating principles for sensors developed in task 5 will become the basis for developing a method for managing a sensor network. Organising single elements into a network requires mechanisms to be developed that should include the methods of communication between sensors, management of their resources and means to acquire data from the network as a whole. The key to communication between sensors is to develop routing algorithms and effective data acquisition methods (observations) so that "querying" single sensors can be avoided. It is assumed that a certain hierarchical structure will be introduced to the network with distinguished nodes constituting data hubs which gather and share data made available by "subordinate" sensors.

An essential determinant of the network management approach will be methods for identification and classification of cyber threats (outcome of task 4). The proper functioning of the sensor network should then allow input data indispensable for identification and classification of cyber threats to be obtained and collected. In turn, the very method of their identification and classification, assuming that data from sensor network are available, will in effect come down to the amalgamation of collected data and, in consequence, the use of deduction algorithms to determine the occurrence of danger and algorithms for the classification of identified cyber threats.

The work being done on this task and tasks 7 and 8 require close coordination as sensor network optimisation algorithms (outcome of task 8) will have a direct impact on its management methods (algorithms).

Task 7: Developing a mathematical model for a sensor network

The mathematical model for the sensor network can be defined by using network/graph theory language. Graph could be used to model the network structure whereas quantitative graph models could be used for quantitative description (weighted graphs, formal networks). In such a case, the sensors (represented by graph nodes) and communication channels between then (represented by graph edges/arcs) will comprise the structure components.

Parameters describing the work of sensors and communication channels will be given by functions described on the respective nodes and edges/arcs of the graph (formal network). The aforementioned parameters will result from the technical implementation of the sensor network described under tasks 5 and 6. Also, an essential element of the model will be a mathematical description of the sensor working environment, namely the existing network infrastructure and sensor distribution (sensor network) in this environment.

This model will underlie the development of sensor network optimisation algorithms (task 8), thus ultimately affecting the management method for sensor network (task 6).

Task 8: Developing algorithms for sensor network optimisation

It is assumed that the algorithms developed will involve the optimisation of the sensor network whose primary role will be to collect data for the purposes of early identification and classification of potential cyber threats (task 4). The optimisation should encompass both the stage of network structure planning (including the distribution of nodes) as well as parameters and quantitative characteristics describing its operation. It should also use a sensor graph-network mathematical model developed in task 7, queueing theory, and computer simulation that enables numerous practical problems to be resolved, particularly when their complexity makes it impossible to arrive at a solution by applying analytical (classical) methods.

The algorithms developed should allow for sensor network optimisation by taking into account the criteria such as reliability (ability to operate despite failure), resistance to damage or the disruption of sensors and communication channels, the cost of construction, and the effectiveness of incident data collection (symptoms of cyber threats). It is therefore mandatory to formulate and resolve a multi-criteria task involving the optimisation of the sensor network structure. Improving parameters and the characteristics of optimised-structure network should primarily concern data transmission speed (routing aspects), which also requires the multi-criteria task of network optimisation parameters to be formulated and resolved.

Task 9: Developing mechanisms for preventing the possibility of carrying out a cyberattack

After a cyber threat has been detected, it is imperative to undertake actions aimed at countering or interrupting the execution of a cyberattack by applying the methods for identification and classification of cyber threats (outcome of task 4).

Threat counteraction is commonly understood as a set of activities associated with providing a response to situations where the risk of carrying out a cyberattack has been identified but the attack itself has not yet occurred. Apart from mechanisms designed to counteract threats, the task will also aim at developing mechanisms to interrupt attacks targeting protected facilities. In the case of both the counteraction and interruption of a cyberattack, the capacity for a vigorous response of a party under attack needs to be assumed. The examples of such mechanisms include for instance the disruption of TCP connections, generating packet filtering rules in near real time, or interrupting selected system processes.

It is also necessary to draw particular attention to the fact how important it is to develop not only technical, but also organisational procedures for response. Counteracting the possibility of carrying out a cyberattack will only be effective if precise and practically feasible (observing legal regulations) principles of cooperation are defined between various stakeholders, e.g. telecommunications operators, content and hosting providers, data centres and emergency response teams. It is indispensable for the effective use of the "notice and take-down" method (notification of security breach incident followed by the elimination of a threat should the notice be valid).

Task 10: Optimisation of mechanisms for preventing the possibility of carrying out a cyberattack

The task involving the optimisation of (technical and organisational) mechanisms for preventing the occurrence of the selected types of cyber threats draws upon the outcomes of task 9. Its assessment should take into account various types of criteria (effectiveness, cost of implementation, cost of usage, time required to use the mechanism, etc.). The understanding of the effectiveness criterion should be twofold. On the one hand, it is essential to evaluate the efficacy of threat prevention. However, the introduction of various mechanisms of defence (e.g. network filters – firewall) causes delays in the execution of principal tasks by the systems under protection. Therefore, it is essential to assess the influence of these mechanisms on the efficiency (delays, throughput) with which the system performs its fundamental functions. These criteria should be used to optimise the mechanisms owned to prevent the occurrence of selected types of cyber threats. Therefore, the aim of the optimisation should be such a selection of mechanisms and their configuration that will be optimal from the perspective of chosen criteria and fixed assets (usually limited) as well as specific working conditions of the system. It is therefore mandatory to formulate and resolve a multi-criteria task involving the optimisation of mechanisms countering the possibility of carrying out selected types of cyberattacks.

Task 11: Developing mechanisms for neutralising the effects of cyberattacks

The task involving the development of mechanisms neutralising the effects of the occurrence of selected type of cyberattacks is analogous to task 9. The cardinal difference between these tasks lies both in the fact that most activities neutralising the effects of the attack are undertaken in the domain of a victim constituency, as well as the necessity to consider the fact that we are facing a situation where the cyberattack has proved successful. The examples of technical mechanisms used to neutralise attacks include generating a list of cryptographic hashes for binary and configuration files, comparing the lists between predefined points in time, generating the list of modified files that should be restored from the backup, etc.

At the same time, it needs to be noted that the effects of cyberattack can vary dramatically depending on the type of response that follows its occurrence. Although the initial phases of a successfully carried out attack usually set the groundwork for the proper phase of system exploration, they do not yet cause real losses. Only the absence of an adequate response to these attacks, which is inseparably connected with the ability to detect them, may turn out to be critically dangerous for the functioning of the entity under attack and require the mechanisms for neutralising the effects of cyber threats to be applied.

As part of this task, both technical and organisational procedures for neutralising the effects of cyber threats should be developed, which are particularly important for large entities, including the operators of the state-level CIs.

Task 12: The optimisation of mechanisms neutralising the effects of cyberattacks

The task involving the optimisation of mechanisms to neutralise the effects of selected types of cyber threats draws upon the outcomes of task 11. Having a set of possible mechanisms to use for neutralising cyber threats at our disposal requires it they need to be assessed by taking into account various types of criteria (effectiveness, cost of implementation, cost of usage, time required to use the mechanism, etc.). These criteria should be used to optimise the mechanisms owned to neutralise the effects of the selected types of cyber threats. In other words, the aim of the optimisation should be such a selection of mechanisms and their configuration that will be optimal from the perspective of chosen criteria and fixed assets (usually limited) as well as specific working conditions of the system. It is therefore mandatory to formulate and resolve a multi-criteria task involving the optimisation of mechanisms neutralising the effects of selected types of cyberattacks.

Summary

The chapter has presented the concept of an IT toolkit designed to improve the effectiveness of detecting, countering and neutralising the effects of cyber threats. This type of solution should be used to support competent state services and CERT-type organisations. Using the toolkit should contribute to achieving the synergy effect due to supporting coordination activities of competent services and the automation of the information flow.

The appropriate distribution of sensors (detectors, filtering elements) is paramount to early detection of a threat, which allows for the effective identification of threat symptoms and, in consequence, the counteraction of hazards and the neutralisation of their effects. For this reason, in case the concept described in this chapter should be implemented, it would require a detailed analysis of determinants and legal restrictions affecting the distribution of sensors to be conducted. One of the multiple benefits of a well-suited distribution of sensors is the ability to identify computers using anonymising Proxy or TOR network.

11. The analysis of academic study programmes related to the security of critical infrastructure's ICT systems

Krzysztof Rzecki – Cracow University of Technology

The aim of this chapter is to analyse the tertiary computer science study programmes with a focus on ICT network protection as part of the CI system. Defined in the Act of 26 April 2007 on Crisis Management (Journal of Laws No. 89, item 590 with further amendments, hereinafter referred to as "the Act"), ICT networks are one of eleven systems that comprise CI. Each system described in the Act consists of mutually bound functional objects (including constructions), facilities, installations and (key) services they provide. Being also part of other CI systems, ICT networks not only support, but often determine their proper functioning.

A field of study and technology, Information and Communication Technology (ICT) combines the achievements of computer science and telecommunications in the area related to a broadly understood electronic transmission through various media and transmission control between network devices.

Since ICT system protection involves information protection (processing systems) and the protection of production systems, both these components merit equal attention. Despite the ICT network system and communications system being closely linked to one another, the latter will not be subject to analysis due to its detachment from the topics included in the computer science study programme. Whether a given element belongs to a system or not will be determined by its application. Hence, in special cases, a given element can be a part of more than one system.

The classification of individual parts of a given infrastructure as an object, facility, installation, or a service should be precisely defined; however, the multi-functional nature and interconnections between these components can make the classification difficult. In the case of ICT networks, the objects may include such things as buildings together with furnishings (physical safeguards, fire prevention devices, emergency power supplies, etc.) that comprise server rooms, ICT nodes, computation centres, etc. The set of equipment not only includes hardware and software which implements the functionalities of the ICT network, but also devices that protect these networks within the scope discussed. Installations can comprise sets of ICT devices bundled with software that enable access to specific functionalities and allow predefined processes to be carried out as ICT services involve data transmission, storage, processing, etc.

The legal basis

The Act of 27 July 2005 Law on Higher Education[1] is a primary, entry level document that specifies the principles of the functioning of higher education institutions. The Act defines the National Qualifications Framework for Higher Education as "a description, expressed through relevant learning outcomes, of all qualifications awarded within the Polish higher education system." In turn, learning outcomes denote "a body of knowledge, skills and social competencies acquired as a result of a process of learning." Based on the assessment of learning outcomes achieved, a competent institution awards a document (diploma, certificate, or another document) which attests the qualifications. Qualifications refer to a particular degree profile, namely "either a practical profile comprising educational components which serve to equip students with practical skills or a general academic profile comprising components which serve to expand students' range of theoretical skills."

The National Qualifications Framework for Higher Education is published by regulation of the Minister of Science and Higher Education. The currently binding regulation of 2 November 2011 contains Appendix 5 which describes the learning outcomes of technological sciences, including computer science. The description of these outcomes applies in general terms to all technological sciences; additionally, in accordance with the provisions of the Act, every institution of higher education is entitled to "design curricula and programmes of studies giving due regard to the intended learning outcomes for the areas of study, in compliance with the National Qualifications Framework for Higher Education [...]." Thus, the senate of each institution of higher education can autonomously determine by resolution the learning outcomes for the fields of study they offer.

Until recently, the Ministry of Science and Higher Education would publish the education standards it set. They would serve as a basis for determining the scope of knowledge to be gained in the particular fields of studies offered by a given institution of higher education. Even though the role of education standards are currently taken over by learning outcomes, the latter, in numerous cases, result from a smooth transition from these very standards, which became the source of information for the analysis.

Education standards

Although Information and Communication Technology is missing from the list of study programmes for which the Ministry of Science and Higher Education prepared education standards, the list nevertheless mentions two fields related to Information Technology:

- computer science
- computer science and econometrics

The above standards fail to provide information on CI education, particularly regarding ICT networks.

Amongst the study courses similar in subject-matter to CI protection we can find:

[1] Act of 27 July 2005 *Law on Higher Education* (Journal of Laws of 21 April 2011 No. 84, item 455).

- In the programme for first-cycle computer science studies, the contents of the major curriculum related to network technologies include "Safety in computer networks and cryptography"
- In the programme for first-cycle computer science and econometrics studies, the contents of the core curriculum related to business informatics include "Information and information system security"
- In the programme for first-cycle computer science and econometrics studies, the contents of the major curriculum related to databases include "Data security"

The fields of study for which the Ministry of Science and Higher Education has developed education standards incorporating issues related to CI protection include:

- national security
- internal security
- security engineering

In the description of education standards for national security studies, the contents of the core curriculum for the second-cycle studies contain modules from the area of defence law for the Republic of Poland including "Defence law for security and public order, civil protection, border protection, constitutional order, and the protection of the economy and critical infrastructure." In the description of education standards for internal security studies, the contents of the major curriculum for the second-cycle studies contains modules in civil protection and civil defence including "Critical infrastructure protection" as well as "Duties resulting from allied obligations, ratified agreements and international conventions on crisis management, emergency services, civil protection, civil planning and critical infrastructure protection." In the description of education standards for security engineering studies, the contents of the major curriculum for the first-cycle studies contains modules in threat modelling including "Projection of threats to critical infrastructure, water intake pollution." In the same standards, there are contents of the major curriculum for first-cycle studies which entirely refer to CI system protection and involve technical security systems.

On the basis of the analysis of education standards, it can be concluded that although the Ministry of Science and Higher Education does not directly provide for education in CI protection in computer science-related courses, yet the contents of curricula to some degree include issues associated with information security. However, the curriculum content included in education standards for security engineering studies devote an entire chapter to discussing the problem of CI system protection.

The outline of the scope of knowledge in education on ICT network system protection

In order to establish the appropriate scope of knowledge that should constitute the didactic material on ICT networks included in degree-level computer science, it is necessary to perceive the system from the perspective of elements that comprise it. It could be noticed then that the foundation of object protection are the aspects least related to computer science. A similar scenario will apply to devices for which protection is an offshoot of object protection. The only elements most strongly linked to computer science are installations and services; hence graduates in this field who are well informed about them will be best qualified to protect the ICT network system.

In previous chapters of this report, different aspects and fundamental differences between two fields of study – Information Technology (IT) and Operational Technology (OT) were presented. This section will identify the most fundamental issues related to them that underlie protocols, processes, technologies, etc. for the protection of the ICT network system. These foundations characterise the scope of knowledge that should be passed on to computer science students.

The requisite skills and knowledge in education on information protection (IT systems)

Information-related operations include both simple activities such as information change, and more complex ones such as obtaining, analysing, cleansing, obfuscation, transformation, processing, storage, backup, archiving, and transmission, etc. of data. If information is significant for the security of the contents it carries, each of the operations listed above may take into account some security aspects.

ICT network protection within the meaning of information protection should be understood from the point of view of an entity (person, institution, computer program, etc.) aiming to get access to a particular resource (information, computer programme, etc.). This type of protection is based on several interconnected processes (in short):

- identification, namely the entity's declaration of identity
- authentication, namely the confirmation of identity declared
- authorisation, namely whether and to what extent the entity can access resources
- integrity, namely asserting whether information is authentic
- confidentiality, namely assuring that unauthorised person cannot have access to information
- non-repudiation, namely the lack of possibility to deny the authorship of information

To execute all the above processes, techniques related to cryptography, protocols and cryptographic algorithms, etc. are applied. They can be implemented both as hardware or software solutions. Based on the aforementioned processes, solutions with a higher level of abstraction can be designed and constructed.

The requisite skills and knowledge in education on production system protection (OT systems)

The rudimentary knowledge about production system protection starts with placing them among other systems comprising a typical corporate IT infrastructure. This arrangement is supposed to draw attention to dependencies with the remaining systems which affect (not necessarily directly) manufacturing processes. Starting from the highest level of corporate management we have:

- EIS – Executive Information System

- SCM – Supply Chain Management
- ERP – Enterprise Resource Planning
- MRP – Manufacturing Resource Planning
- MES – Manufacturing Execution System
- LIMS – Laboratory Information System
- PCS – Process Control System
- SCADA – Supervisory Control & Data Acquisition
- DCS – Distributed Control System
- PLC – Programmable Logic Controller

The list is by no means exhaustive of existing systems, yet it presents what appears to be the most general and comprehensive set. Taking into account the fact that the systems are largely tied to manufacturing processes, systems such as Human Resource Management (HRM) or Customer Relationship Management (CRM) have been disregarded.

From the perspective of CI, the systems of the highest importance are SCADA and other directly linked systems such as DCS and PLC. This results from the dynamic nature of these systems and therefore the level of their susceptibility and vulnerability to external factors.

Operations performed by a computer-aided system involve a diverse array of actions, strongly dependent on the purpose of the system. In the area of security, they will primarily cover the following aspects:

- accountability – involves incident logging in order to determine the originator of activity
- monitoring – non-invasive observation through incident logging analysis
- anonymity – property of the system inverse to accountability
- availability – giving access to an entity in a given time and place
- failure – the state when the system is disabled, which makes it impossible to use it in a normal way
- reliability – the property that gauges the likelihood that a failure will not occur
- threat – the state of lowered security
- risk – the likelihood of a threat transforming into a failure
- vulnerability – high risk of a threat changing into a failure
- safeguard – lowering the risk that a threat (failure) may materialise
- redundancy – maintaining an up-to-date copy of a given system
- copy/archive – maintaining a disabled system back-up
- recovery – reverting the system to the state of that prior to failure.

The above presented issues point to the areas of knowledge regarding the protection of production computer-aided systems. They become the basis for defining security needs and capabilities to satisfy them and at a higher level of abstraction they involve:

- identification, authorisation and authentication systems
- monitoring, login, and response systems
- anti-virus, anti-malware, and anti-spam systems
- network protection systems and firewalls
- intrusion and penetration attack detection systems
- back-up, archiving, and safety copy maintaining procedures

- procedures for system restore and data recovery
- systems and procedures for managing configuration, change, and incident or configuration, change, or incident management procedures and systems
- etc.

Summary

The analysis of tertiary study programmes presented in this article was conducted on the basis of recently published education standards which have been gradually supplanted by learning outcomes. The analysis has touched upon aspects of education on critical infrastructure ICT network system protection.

Drawing exclusively upon the standards laid down by the Ministry of Science and Higher Education, the study programmes related to computer science disciplines fail to include issues closely linked to CI protection; it is fair to observe, however, that they cover most of the topics associated with the protection of information and production systems. Amongst the available study programmes there are at least three courses related to CI protection, but none of them provides specialist knowledge and training in ICT network system protection with regard to elements such as installations or services.

In order for computer science studies to adequately prepare for ICT network system protection, they should be founded on the body of knowledge concerning the protection of information and production systems mentioned in the earlier section of this chapter. What should definitely be considered, however, is the introduction of lectures that present key features describing the field of CI protection in order to transfer knowledge and practise skills that will help answer the following questions:

- What information should be protected and why?
- What should be monitored and why?
- What should be fail proved and why?
- What should be archived and why?
- etc.

Therefore, the element that should be introduced to complete the overall picture is the ability to find answers to questions of “what” and “why” since the answers to “how to do things” is largely known and implemented.

Another analysis of study programmes, performed no sooner than 12 months after the last evaluation, should no longer draw upon education standards, but descriptions of learning outcomes developed by individual institutions of higher education.

Factors affecting security and recommendations

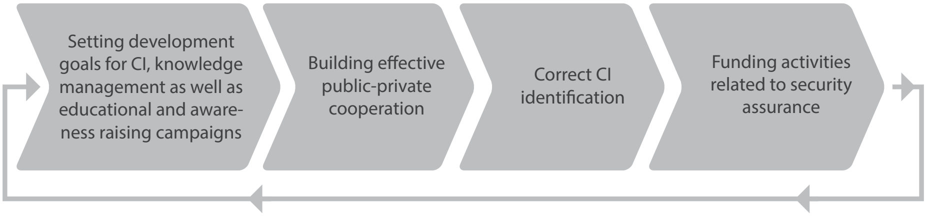
the Kosciuszko Institute Team

Below are the most important factors influencing general CI security (based on key conclusions following the first part of the report) and ICT security of CI (conclusions from Part Two). Factors with an impact on CI security are presented as elements in a general process leading towards achieving the goal of ensuring the security of CI as a whole. Factors affecting the ICT security of CI are presented by means of the Ishikawa Diagram, which makes it possible not only to categorise them, but also to discover hitherto unknown relations between different causes and so present a map of the topic discussed.

The identified and presented factors related both to CI security and the ICT security of CI should be interpreted as opportunities and weaknesses impacting the above-mentioned security objectives.

Recommendations have been divided in a similar way. The first group covers general, systemic issues – the other deals with more specific problems related to ICT aspects. Regardless of the break-down, both categories should be treated as complementary.

Factors determining effective CI security assurance


Setting development goals for CI, knowledge management as well as educational and awareness raising campaigns
Building effective public-private cooperation
Correct CI identification
Funding activities related to security assurance

1. Setting development goals for CI, knowledge management as well as educational and awareness raising campaigns:
   1.1. educational campaign on threats and the need to take security measures

* Preliminary proposal is presented in the text.

** See Chapter Four

   1.2. specialist academic education
   1.3. promoting knowledge of legal mechanisms, e.g. public procurement

2. Building effective public-private cooperation:
   2.1. building a system promoting effective cooperation and improving security
   2.2. creating sectoral fora for information exchange with Government Centre for Security acting as a "liaison" institution
   2.3. organising forum activity

3. Correct CI identification
   3.1. reliable information as a pre-condition for correct identification
   3.2. potential involvement of local actors in CI identification

4. Funding activities related to security assurance:
   4.1. financial support for CI owners and operators covering the costs of building, maintaining and protecting CI (e.g. from a special-purpose fund)
   4.2. promoting EU funding options

Recommendations and suggestions

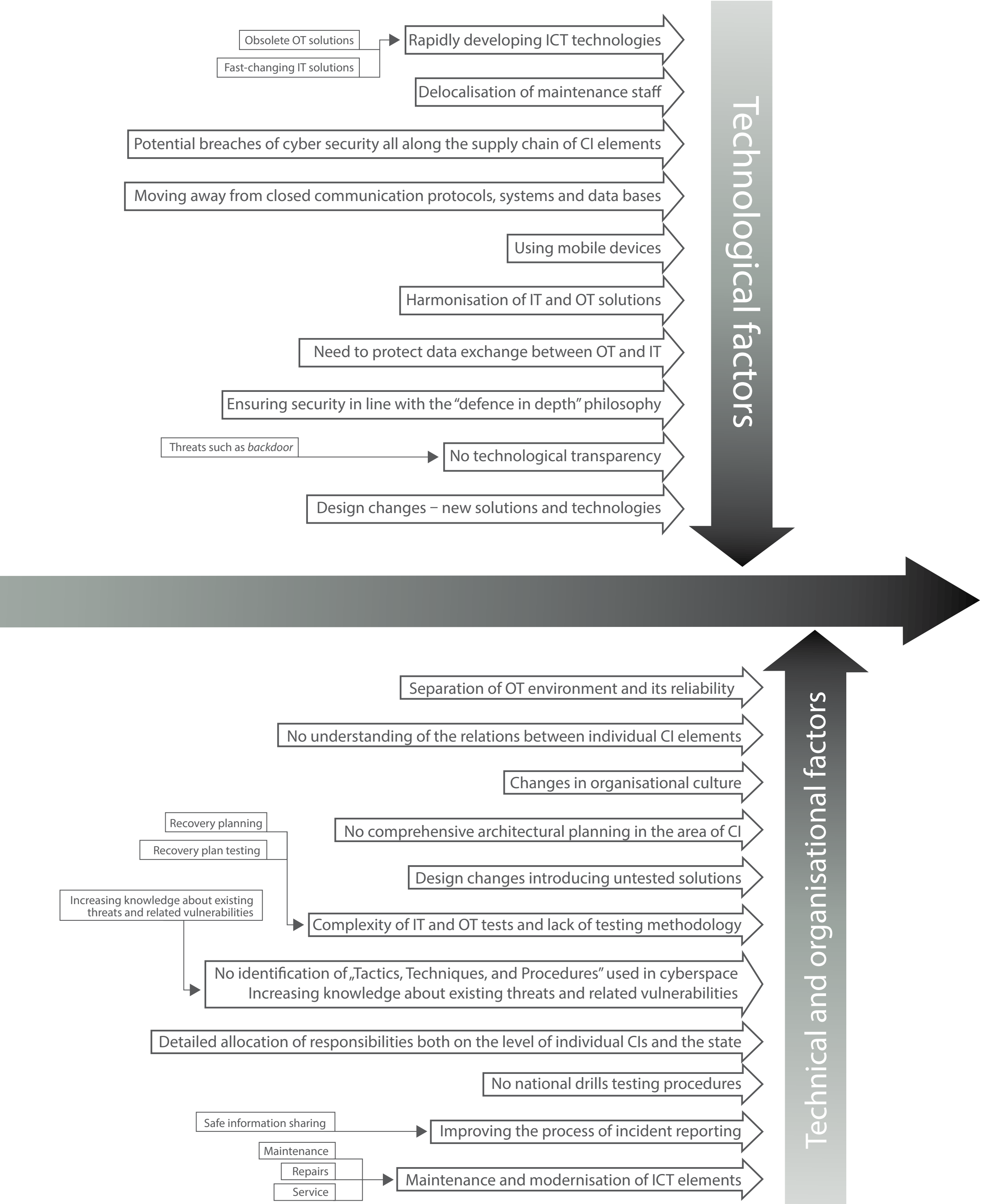
1. It is recommended that the possibility to update the definition of CI is considered so that it leaves no doubt that it covers virtual infrastructure (information) such as information stored in databases.

2. The Government Centre for Security should aim to abandon sectoral criteria as suggested in the National Critical Infrastructure Protection Programme and so get closer to the "bottom up" approach to CI identification.

3. The state should create a system of incentives (financial and non-financial)* encouraging to establish public-private cooperation, provide solid security and take self-regulating measures.

4. Sectoral cooperation forums should be based on the best practices of work organisation**. The bottom line should be to move away from the "classic", hierarchical governance towards flexible, "network" solutions.

5. The state should support CI owners financially to cover the costs of building, maintaining and protecting CI (e.g. from a special-purpose fund).


Technological factors
Obsolete OT solutions
Fast-changing IT solutions
Rapidly developing ICT technologies
Delocalisation of maintenance staff
Potential breaches of cyber security all along the supply chain of CI elements
Moving away from closed communication protocols, systems and data bases
Using mobile devices
Harmonisation of IT and OT solutions
Need to protect data exchange between OT and IT
Ensuring security in line with the "defence in depth" philosophy
Threats such as *backdoor*
No technological transparency
Design changes – new solutions and technologies
Technical and organisational factors
Separation of OT environment and its reliability
No understanding of the relations between individual CI elements
Changes in organisational culture
Recovery planning
Recovery plan testing
No comprehensive architectural planning in the area of CI
Design changes introducing untested solutions
Increasing knowledge about existing threats and related vulnerabilities
Complexity of IT and OT tests and lack of testing methodology
No identification of „Tactics, Techniques, and Procedures" used in cyberspace Increasing knowledge about existing threats and related vulnerabilities
Detailed allocation of responsibilities both on the level of individual CIs and the state
No national drills testing procedures
Safe information sharing
Improving the process of incident reporting
Maintenance
Repairs
Service
Maintenance and modernisation of ICT elements

Recommendations and suggestions

1. The state should consider imposing regulatory and control measures on operators supplying IT and OT solutions for CI regarding compliance with necessary security requirements (such as access to codes through *escrow*).

2. Global security standards for industrial systems should be adapted to Polish reality. This could be done by, for example, the Polish Committee for Standardisation or organisations representing the industry.

3. Discussion should be launched on regulations requiring CI owners and operators to comply with specific IT standards in OT (introducing measures to verify compliance and penalties in case of non-compliance). Potential regulations should be accompanied by a system of incentives (see Recommendation 3 in Part One).

4. The state should consider relieving CI owners and operators by sponsoring security controls of selected elements in IT and OT systems as well as trainings on CI risk management, protection and continuity planning.

5. The state, the industry and the stakeholders themselves should support and implement new measures related to raising awareness of IT and OT security as well as improving educational practices in this area.

6. The government (via appropriate entities) should be engaged in on-going monitoring of future trends and anticipate changes in a dynamic environment (*Foresight*).

7. There should be support for measures helping owners and operators of CI understand the relations between individual CI elements. This should in particular involve adopting a holistic perspective of protecting ICT systems.

8. It is recommended that a catalogue of cyber threats is drawn up. In this context, it would be advisable to create a national centre of competence in the area of threats and vulnerabilities, which would be a Polish body equipped with expertise and world-class testing tools.

9. The Government Centre for Security should keep strengthening and building effective mechanisms of sharing confidential information on CI security between CI operators in a way that ensures safe information transfer.

10. Teaching curricula in IT studies include topics covering the protection of information and production systems but do not relate directly to the problems of critical infrastructure. Education should involve modules teaching characteristic aspects of CI protection in order for the students to acquire knowledge and practise skills. Actions to this end should be taken both by higher education institutions as well as CI owners and operators.

11. The state should support financially any activities (for instance carried out by the National Centre for Research and Development) related to research and development in such areas as, for example, creating national IT tools increasing the effectiveness of detecting, countering and neutralising the effects of cyber threats. A National Research and Development Plan for cyber security should be drawn up in consultation with private operators with, for example, main objectives, priorities and a "road map".

Annex

Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1
	· **COBIT 5** BAI09.01, BAI09.02
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISA 62443-3-3:2013** SR 7.8
	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	· **NIST SP 800-53 Rev. 4** CM-8
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2
	· **COBIT 5** BAI09.01, BAI09.02, BAI09.05
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISA 62443-3-3:2013** SR 7.8
	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	· **NIST SP 800-53 Rev. 4** CM-8
ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1
	· **COBIT 5** DSS05.02
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISO/IEC 27001:2013** A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02
	· **ISO/IEC 27001:2013** A.11.2.6
	· **NIST SP 800-53 Rev. 4** AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02
	· **ISA 62443-2-1:2009** 4.2.3.6
	· **ISO/IEC 27001:2013** A.8.2.1
	· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.2.3.3
	· **ISO/IEC 27001:2013** A.6.1.1
	· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
ID.BE-1: The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
	· **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2
	· **NIST SP 800-53 Rev. 4** CP-2, SA-12

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01
	· **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01
	· **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6
	· **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3
	· **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	· **COBIT 5** DSS04.02
	· **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	· **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
ID.GV-1: Organizational information security policy is established	· **COBIT 5** APO01.03, EDM01.01, EDM01.02
	· **ISA 62443-2-1:2009** 4.3.2.6
	· **ISO/IEC 27001:2013** A.5.1.1
	· **NIST SP 800-53 Rev. 4** -1 controls from all families
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· **COBIT 5** APO13.12
	· **ISA 62443-2-1:2009** 4.3.2.3.3
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1
	· **NIST SP 800-53 Rev. 4** PM-1, PS-7
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **COBIT 5** MEA03.01, MEA03.04
	· **ISA 62443-2-1:2009** 4.4.3.7
	· **ISO/IEC 27001:2013** A.18.1
	· **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** DSS04.02
	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3
	· **NIST SP 800-53 Rev. 4** PM-9, PM-11
ID.RA-1: Asset vulnerabilities are identified and documented	· **CCS CSC** 4
	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **ISO/IEC 27001:2013** A.6.1.4
	· **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	· **COBIT 5** DSS04.02
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **COBIT 5** APO12.02
	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

ID.RA-6: Risk responses are identified and prioritized	· **COBIT 5** APO12.05, APO13.02
	· **NIST SP 800-53 Rev. 4** PM-4, PM-9
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
	· **ISA 62443-2-1:2009** 4.3.4.2
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.3.2.6.5
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PR.AC-1: Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16
	· **COBIT 5** DSS05.04, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.3.5.1
	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
	· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
	· **NIST SP 800-53 Rev. 4** AC-2, IA Family
PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05
	· **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8
	· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
	· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Remote access is managed	· **COBIT 5** APO13.01, DSS01.04, DSS05.03
	· **ISA 62443-2-1:2009** 4.3.3.6.6
	· **ISA 62443-3-3:2013** SR 1.13, SR 2.6
	· **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15
	· **ISA 62443-2-1:2009** 4.3.3.7.3
	· **ISA 62443-3-3:2013** SR 2.1
	· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
	· **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **ISA 62443-2-1:2009** 4.3.3.4
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8
	· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, SC-7
PR.AT-1: All users are informed and trained	· **CCS CSC** 9
	· **COBIT 5** APO07.03, BAI05.07
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-2, PM-13
PR.AT-2: Privileged users understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.02, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03, APO10.04, APO10.05
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** PS-7, SA-9
PR.AT-4: Senior executives understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.AT-5: Physical and information security personnel understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.DS-1: Data-at-rest is protected	· **CCS CSC** 17
	· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.4, SR 4.1
	· **ISO/IEC 27001:2013** A.8.2.3
	· **NIST SP 800-53 Rev. 4** SC-28
PR.DS-2: Data-in-transit is protected	· **CCS CSC** 17
	· **COBIT 5** APO01.06, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SC-8
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1
	· **ISA 62443-3-3:2013** SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
	· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	· **COBIT 5** APO13.01
	· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
	· **ISO/IEC 27001:2013** A.12.3.1
	· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	· **CCS CSC** 17
	· **COBIT 5** APO01.06
	· **ISA 62443-3-3:2013** SR 5.2
	· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
	· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SI-7

PR.DS-7: The development and testing environment(s) are separate from the production environment	· **COBIT 5** BAI07.04
	· **ISO/IEC 27001:2013** A.12.1.4
	· **NIST SP 800-53 Rev. 4** CM-2
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	· **CCS CSC** 3, 10
	· **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05
	· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
	· **ISA 62443-3-3:2013** SR 7.6
	· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	· **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **COBIT 5** AP013.01
	· **ISA 62443-2-1:2009** 4.3.4.3.3
	· **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
	· **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PR.IP-3: Configuration change control processes are in place	· **COBIT 5** BAI06.01, BAI01.06
	· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
	· **ISA 62443-3-3:2013** SR 7.6
	· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	· **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· **COBIT 5** AP013.01
	· **ISA 62443-2-1:2009** 4.3.4.3.9
	· **ISA 62443-3-3:2013** SR 7.3, SR 7.4
	· **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
	· **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **COBIT 5** DSS01.04, DSS05.05
	· **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
	· **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
	· **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4.3.4.4.4
	· **ISA 62443-3-3:2013** SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
	· **NIST SP 800-53 Rev. 4** MP-6
PR.IP-7: Protection processes are continuously improved	· **COBIT 5** AP011.06, DSS04.05
	· **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **COBIT 5** DSS04.03
	· **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1
	· **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2
	· **NIST SP 800-53 Rev. 4** CP-2, IR-8

PR.IP-10: Response and recovery plans are tested	· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11
	· **ISA 62443-3-3:2013** SR 3.3
	· **ISO/IEC 27001:2013** A.17.1.3
	· **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
	· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
	· **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4
	· **NIST SP 800-53 Rev. 4** PS Family
PR.IP-12: A vulnerability management plan is developed and implemented	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2
	· **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4.3.3.3.7
	· **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5
	· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **COBIT 5** DSS05.04
	· **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
	· **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1
	· **NIST SP 800-53 Rev. 4** MA-4
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CCS CSC** 14
	· **COBIT 5** APO11.04
	· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
	· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
	· **NIST SP 800-53 Rev. 4** AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	· **COBIT 5** DSS05.02, APO13.01
	· **ISA 62443-3-3:2013** SR 2.3
	· **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
	· **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· **COBIT 5** DSS05.02
	· **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
	· **ISO/IEC 27001:2013** A.9.1.2
	· **NIST SP 800-53 Rev. 4** AC-3, CM-7
PR.PT-4: Communications and control networks are protected	· **CCS CSC** 7
	· **COBIT 5** DSS05.02, APO13.01
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
	· **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· **COBIT 5** DSS03.01
	· **ISA 62443-2-1:2009** 4.4.3.3
	· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4

DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
	· **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· **ISA 62443-3-3:2013** SR 6.1
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	· **COBIT 5** APO12.06
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
DE.AE-5: Incident alert thresholds are established	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.2.3.10
	· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
DE.CM-1: The network is monitored to detect potential cybersecurity events	· **CCS CSC** 14, 16
	· **COBIT 5** DSS05.07
	· **ISA 62443-3-3:2013** SR 6.2
	· **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **ISA 62443-2-1:2009** 4.3.3.3.8
	· **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **ISA 62443-3-3:2013** SR 6.2
	· **ISO/IEC 27001:2013** A.12.4.1
	· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	· **CCS CSC** 5
	· **COBIT 5** DSS05.01
	· **ISA 62443-2-1:2009** 4.3.4.3.8
	· **ISA 62443-3-3:2013** SR 3.2
	· **ISO/IEC 27001:2013** A.12.2.1
	· **NIST SP 800-53 Rev. 4** SI-3
DE.CM-5: Unauthorized mobile code is detected	· **ISA 62443-3-3:2013** SR 2.4
	· **ISO/IEC 27001:2013** A.12.5.1
	· **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06
	· **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1
	· **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	· **COBIT 5** BAI03.10
	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7
	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** RA-5
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· **CCS CSC** 5
	· **COBIT 5** DSS05.01
	· **ISA 62443-2-1:2009** 4.4.3.1
	· **ISO/IEC 27001:2013** A.6.1.1
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14

DE.DP-2: Detection activities comply with all applicable requirements	· **ISA 62443-2-1:2009** 4.4.3.2
	· **ISO/IEC 27001:2013** A.18.1.4
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02
	· **ISA 62443-2-1:2009** 4.4.3.2
	· **ISA 62443-3-3:2013** SR 3.3
	· **ISO/IEC 27001:2013** A.14.2.8
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
DE.DP-4: Event detection information is communicated to appropriate parties	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.3.4.5.9
	· **ISA 62443-3-3:2013** SR 6.1
	· **ISO/IEC 27001:2013** A.16.1.2
	· **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, DSS04.05
	· **ISA 62443-2-1:2009** 4.4.3.4
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RS.RP-1: Response plan is executed during or after an event	· **COBIT 5** BAI01.10
	· **CCS CSC** 18
	· **ISA 62443-2-1:2009** 4.3.4.5.1
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
RS.CO-1: Personnel know their roles and order of operations when a response is needed	· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
	· **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1
	· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
RS.CO-2: Events are reported consistent with established criteria	· **ISA 62443-2-1:2009** 4.3.4.5.5
	· **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2
	· **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.2
	· **ISO/IEC 27001:2013** A.16.1.2
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.5
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **NIST SP 800-53 Rev. 4** PM-15, SI-5
RS.AN-1: Notifications from detection systems are investigated	· **COBIT 5** DSS02.07
	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISA 62443-3-3:2013** SR 6.1
	· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4

RS.AN-3: Forensics are performed	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
	· **ISO/IEC 27001:2013** A.16.1.7
	· **NIST SP 800-53 Rev. 4** AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.6
	· **ISO/IEC 27001:2013** A.16.1.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
RS.MI-1: Incidents are contained	· **ISA 62443-2-1:2009** 4.3.4.5.6
	· **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** IR-4
RS.MI-2: Incidents are mitigated	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10
	· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5
	· **NIST SP 800-53 Rev. 4** IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
RS.IM-1: Response plans incorporate lessons learned	· **COBIT 5** BAI01.13
	· **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.RP-1: Recovery plan is executed during or after an event	· **CCS CSC** 8
	· **COBIT 5** DSS02.05, DSS03.04
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
RC.IM-1: Recovery plans incorporate lessons learned	· **COBIT 5** BAI05.07
	· **ISA 62443-2-1** 4.4.3.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	· **COBIT 5** BAI07.08
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.CO-1: Public relations are managed	· **COBIT 5** EDM03.02
RC.CO-2: Reputation after an event is repaired	· **COBIT 5** MEA03.02
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· **NIST SP 800-53 Rev. 4** CP-2, IR-4

Abbreviations

APC	–	Advanced Process Control
CAPEC	–	Common Attack Pattern Enumeration and Classification
CDB	–	Configuration Data Base
CI	–	Critial Infrastructure
CII	–	Critical Information Infrastructure
CIP	–	Critical Infrastructure Protection
COCOM	–	Coordinating Committee for Multilateral Export Controls composed of 17 countries (the USA, Japan, Australia and Western European countries)
CRM	–	Customer Relationship Management
CSSWG	–	Control Systems Security Working Group (ICS-CERT's working group for cooperation with representatives of federal institutions)
CVE	–	Common Vulnerabilities and Exposures
DCS	–	Distributed Control System
DDoS	–	Distributed Denial of Service (an attack on a computer system or a network service that compromises their operation)
DHS	–	Department of Homeland Security
DLP	–	Data Leak Prevention
DMS	–	Distribution Management System
DNS	–	Domain Name Service (a system of servers, a communication protocol, and a service supporting a distributed network address database)
ECI	–	European Critical Infrastructures
eCSIRT.net	–	The European Computer Security Incident Response Team Network
EIS	–	Executive Information System
EMS	–	Energy Management System

ENISA	–	European Union Agency for Network and Information Security
EPCIP	–	European Programme for Critical Infrastructure Protection
ERP	–	Enterprise Resource Planning
HIDS	–	Host Intrusion Detection System
HLR	–	Home Location Register
HRM	–	Human Resource Management
ICS	–	Industrial Control Systems
ICS-CERT	–	Industrial Control Systems-CERT
ICSJWG	–	Industrial Control Systems Joint Working Group
ICT	–	Information and Communications Technology
IEC	–	International Electrotechnical Commission
IR	–	Incident Response
ISA	–	Instruments, Systems and Automation Society
IT	–	Information Technology
LIMS	–	Laboratory Information System
MDM	–	Mobile Device Management
MES	–	Manufacturing Execution System
MRP	–	Manufacturing Resource Planning
NCIPP	–	National Critical Infrastructure Protection Plan
NERC	–	North American Electrical Reliability Corporation
NIDS	–	Network Intrusion Detection System
NIST	–	National Institute of Standard and Technology
OT	–	Operational Technology
PCIPP	–	Provincial Critical Infrastructure Protection Plan
PCS	–	Process Control System
PLC	–	Programmable Logic Controller
PPC	–	public-private cooperation
PPL	–	Public Procurement Law
PPP	–	public-private partnership
QoS	–	Quality-of-Service (overall characteristics of the telecommunications service providing the basis for fulfilling the user’s needs)
SABSA	–	Sherwood Applied Business Security Architecture (a methodology used to develop a security architecture, in particular for the public administration)

SCADA – Supervisory Control and Data Acquisition (a system for supervising a technological or production process)

SCM – Supply Chain Management

SMS – security management system

SPOF – Single Point of Failure

SQL – Structured Query Language (a structured query language used to create and modify databases as well as to place and retrieve data from databases)

TCP – Transmission Control Protocol (connection-oriented, reliable, stream communication protocol used to transfer data between processes running on different machines)

TCP/IP – Transmision Control Protocol/Internet Protocol

TOR – the Onion Router (a virtual computer network that provides users with almost anonymous access to Internet resources.)

VoIP – Voice over IP (a technology allows for speech sounds to be transmitted via Internet connections or dedicated networks using IP protocol, commonly known as “Internet telephony”

Authors

Grzegorz Abgarowicz

Ph.D. in social sciences, specifically security sciences; employee at the Government Centre for Security and a lecturer at the Institute of Political Science at the University of Cardinal Stefan Wyszyński in Warsaw. Professionally, Mr Abgarowicz is involved in social planning and risk management. Mr Abgarowicz is an author of publications concerning common security, population protection and crisis management.

Ryszard Antkiewicz

Professor, Ph.D., Eng. at the Military University of Technology and an employee at the Institute of IT Systems at the Faculty of Cybernetics at the Military University of Technology in Warsaw and also a member of the Modelling, Simulation and Computer-Assisted Decisions in Conflict and Crisis Situations Research Group. His scholarly interests include modelling and effectiveness assessment as well as IT systems security, combat modelling, and support in combat and crisis management decision-making.

Piotr Ciepiela

Manager in Technology Advisory Services, EY. He is a co-author and leader of consulting services in the field of critical infrastructure security and industrial automation systems for Central Europe (23 countries). Mr Ciepiela managed numerous projects in the United States, Europe, and the Middle East. He participates in the creation of international standards for Cybersecurity and Industrial System Security (ISA and NIST). He is one of the first to have received the Global Industrial Cyber Security Professional certificate awarded by GIAC and the first one in Poland to have received the Certified SCADA Security Architect certificate awarded by IACRB. He took part in the prestigious Control Systems Cyber Security Advanced Training approved by the U.S. Department of Homeland Security. He is an author of articles about industrial systems published, among other places, in the Harvard Business Review. He has certificates in security management (CISM, CISA, CISSP, ISO27001), corporate architecture, security architecture (TOGAF, SABSA CF), project management (PRINCE2 Practitioner) and IT management (ITIL Service Manager). He also has access to information tagged with "NATO SECRET" and "SECRET UE" clauses.

Michał Dyk

MSc Eng., he graduated from the Faculty of Cybernetics at the Military University of Technology. Since 2013 Mr Dyk is a member of the Modelling, Simulation and Computer-Assisted Decisions in

Conflict and Crisis Situations Research Group. His scholarly interests include mainly network sensors, the Internet of Things, and computer simulation. Currently, he is studying for a Ph.D.

Dominika Dziwisz

Ph.D., graduated from International Relation as well as Management and Marketing at the Jagiellonian University. Her research spectrum includes forms of modern terrorism, including those related to modern technologies, cybersecurity and the security policy of the U.S.

Zbigniew Fałek

Graduated from the Faculty of Management and the Faculty of Mathematics at the University of Łódź. He has also graduated from The Strategic Leadership Academy (Executive Development Program Management II) run by HBSP&CIMI.

Mr Fałek has been involved in the energy industry since 1994. In 2006–2009 he was a chairman of the ZEŁ-T S.A. Board (now PGE Distribution S.A.). Subsequently, he became an investment director in RE-Invest Sp. z o.o. Since 2009 he has been running a consulting business. Mr Fałek is an author of numerous publications on business management.

Piotr Gajek

Lawyer at the WKB barrister's office and a member of a dispute resolution team. Mr Gajek co-operates with state aid and competition law teams. He graduated from the Department of Law, Administration and Economy at University of Wrocław as well as the Department of Law at the European School of Law and Administration in Warsaw. Mr Gajek was a scholarship holder of the Leonardo da Vinci programme. During his studies, he took part in a several-month internship at the European Law and Competition department in Brussels.

As part of the internship in the Department of State Aid in the Directorate General for Competition (DG COMP) in the European Commission, he was involved in preparing projects concerning the evaluation of complaints against alleged unlawful state aids. He has several years of experience in the field of European Funds. He took part in the preparation of legal opinions for business people and public entities, evaluating the risk of either receiving or granting state aid as a result of concluding transactions.

Rafał Kasprzyk

Major, Ph.D., Eng., academic employee at the Faculty of Cybernetics at the Military University of Technology in Warsaw and a member of the Modelling, Simulation and Computer-Assisted Decisions in Conflict and Crisis Situations Research Group. His main areas of interest include modelling, simulation and network system analysis using models and operational research methods such as graph and network theories as well as selected elements of artificial intelligence. Together with undergraduate and Ph.D. students, Mr Kasprzyk manages projects numerously distinguished at international innovation fairs.

Włodzimierz Kotłowski

Expert in ICT security. He has been involved in this topic for 15 years. He took part in numerous ICT projects both in Poland and in the EU countries as a person responsible for Information and Communications Technology security. Mr Kotłowski graduated from the Military University of Technology in Warsaw where he studied technical physics. For many years he was an academic employee at the Institute of Technical Physics at the Military University of Technology in Warsaw. Mr Kotłowski is currently a member of the board in Matic Sp. z o.o.

Mirosław Maj

Since 2010 a founder and chairman of Cybersecurity Foundation and vice-chairman of the ComCERT S.A. company. Prior to that, he managed a team at CERT Poland. Nowadays, he cooperates with the Government Centre for Security in the area of critical infrastructure protection. He also runs lectures about ICT security at the Jagiellonian University, Polish Japanese Institute of Information Technology and Warsaw School of Economics.

In 2012 and 2013 he coordinated Cyber-EXE Poland, the first training on cybersecurity in Poland. Mr Maj participated in the creation of new CERTs both in Poland and abroad. Thanks to the NATO project "CLOSER", which he coordinated, new CERTs in Georgia, Moldova, Armenia and Azerbaijan were founded. He co-organises the cooperation between the European CERTs as part of the initiative of Trusted Introducer and TERENA TF-CSIRT. Mr Maj work closely with the ENISA agency, being a member of thematic task groups and a co-author of numerous studies published by the Agency.

Andrzej Najgebauer

Professor, Ph.D. Eng. at the Military University of Technology; Mr Najgebauer is the Head of the Modelling, Simulation and Computer-Assisted Decisions in Conflict and Crisis Situations Research Group at the Military University of Technology in Warsaw. He is also an expert in computer simulations of conflict and crisis situations and in the area of modelling and planning computer-assisted decisions as well as modelling and planning security systems. He has been managing multiple national and international projects in the area of IT security systems. As part of a state defence review, he participated in the creation of national security expert evaluations and was a member of a scientific and industrial research group at the Military Council of the Armed Forces of the Republic of Poland. Since 2010 he has been representing Poland in the NATO Science and Technology Organization panel – NATO Modelling and Simulation Group. In 2002–2006 he was a head of a team representing 10 NATO countries in the MSG-026 project called "M&S Tool for Early Warning Identification of Terrorist Activities."

Dariusz Pierzchała

Ph.D., Eng., Mr Pierzchała graduated from the Faculty of Cybernetics at the Military University of Technology in Warsaw and a participant of the NATO, NAF (AT2-AT4), PRINCE2, Rationale RUP, SAS Master Class and ESRI ArcGIS courses. Currently, he is assistant professor at the Faculty of Cybernetics, a Polish representative at the NATO Modelling and Simulation Group and a secretary of the Polish Society for Computer Simulation. Mr Pierzchała is involved in teaching methodology and research on heterogeneous dissipated computer simulation (system integration, aspects of discrete-event control systems). His scholarly interests also include assisting in decision-making in conflict and crisis situations by using prognostic and simulation methods as well as operational research.

Aleksander Poniewierski

Ph.D., partner in Technology Advisory Services in EY and a Leader of the IT Advisory Group in Central and South-East Europe. A post-graduate of the University of Silesia in Katowice, Mr Poniewierski completed his Ph.D. in Economic Studies at the Poznań University of Economics. He participated in numerous prestigious programmes organised by the Harvard Business School and Carnegie Mellon University. Mr Poniewierski specialises in the implementation of IT management systems, the efficiency improvement of IT systems used in business as well as risks that come along with their use. He is also interested in cybersecurity and critical infrastructure. He advised top-tier companies on IT security and management as well as IT strategies and transformation. The ISACA association has rewarded him the following CISM certificates: CISA Certified Project Manager APM, CFE, PRINCE2 Practitioner, ITIL Foundation (IT Infrastructure Library), ISSP (International Systems Security Professional), CERT Certified Computer Security Incident Handler, SABSA Chartered Foundation (SCF) Certificate.

Maciej Pyznar

Leading expert in the Department of Critical Infrastructure Protection at the Government Centre for Security. Mr Pyznar graduated from the Faculty of Naval Navigation and Armament at the Naval Academy in Gdańsk and from the National Security College at the University of Warsaw.

In GCS where he has worked since its inception, he has been involved in planning and programme activities in critical infrastructure protection.

Mirosław Ryba

Ph.D., Director in Technology Advisory Services in EY. Mr Ryba manages the EY Global OT Advisory Services Centre. During 15 years of his professional career, he has gained a vast experience in IT and OT by managing numerous projects for both government institutions and large companies in Europe, Africa, the Middle East and North America. As a specialist in architecture management and ICS security, in 2011 he gained accreditation from the U.S. Department of Homeland Security to participate in the Control Systems Cyber Security Advanced Training run by Idaho National Laboratory in Idaho Falls, USA. Mr Ryba is an active member of ISA (International Society of Automation) and was engaged in the development of ISA-62443-3-3 standard for industrial automation and control system security. He has numerous certificates, such as CSSA, SABSA, CISA, CISM and CISSP.

Krzysztof Rzecki

Ph.D., Eng., assistant professor at the Institute of Information and Communication Technology at the Tadeusz Kościuszko University of Technology in Cracow. For several years he was a head of the software department in CCNS SA and a contractor for network protocols with Siemens AG and Nokia-Siemens-Networks. Currently, Mr Rzecki does business-commissioned studies in context-awareness (Orange/ TP SA), mobile technology and virtualisation (VSoft SA). He cooperates with CTT PK in the field of modern technology.

Joanna Świątkowska

Political scientist; she is in the process of writing her Ph.D. thesis on modern information warfare.

Ms Świątkowska is an expert in cybersecurity at the Kosciuszko Institute.

She is the author and the leader of the *Target: Cybersecurity* project which she has run since 2011.

She was the initiator, coordinator and the participant of many national and international security projects, in particular information and communication technology security.

She took part in research done by Strategic Security Forum on cybersecurity that was organised by the National Security Bureau. She was on the panel of experts set up by the Supreme Audit Office with respect to the inspection of cybersecurity protection activities run by state institutions. She is also a member of the international Sino-European Cyber Dialogue.

Zbigniew Tarapata, Reserve lieutenant-colonel

Professor, Ph.D., Eng. at the Military University of Technology. Mr Tarapata graduated from the Faculty of Cybernetics at the Military University of Technology in Warsaw in 1995. He is Associate professor at MUT and, since 2012 a Director of the Institute of IT systems in the Faculty of Cybernetics at MUT. Mr Tarapata is involved in teaching methodology as well as research on algorithm analysis (complexity, accuracy, effectiveness), models and methods of graph and network theories (extremal paths, graph and network similarities, semantic networks, complex networks, transportation problems), decision-making assistance in conflict and crisis situations by using models and operational research methods as well as elements of artificial intelligence.

Agnieszka Wiercińska-Krużewska

Co-founder and partner at the WKB barrister's office. Apart from managing a team responsible for media and intellectual property law, Ms Wiecińska-Krużewska cooperates closely with the merging and acquisition team. She graduated from the Faculty of Law and Administration of the Adam Mickiewicz University in Poznań. As a holder of the Sorosa Foundation's scholarship, she completed her postgraduate studies in international economic law at the Central European University in Budapest (LLM).

She advises her clients on issues related to copyrights, industrial ownership, consumer law, acts of unfair competition, personal data and Internet domain protection, press law, and the protection of personal and property rights. Ms Wiecińska-Krużewska runs cases related to sensitive product marketing and gambling. Besides her advisory services, she also represents her clients in court proceedings and pre-trial settlements. For several years now she has also been involved in the acquisition of companies on the private market.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.

Numerous scientists, Polish and European administration employees as well as public and socio-economic practitioners are involved in the Institutes' research. It creates expert evaluations and programme recommendations for both the European and Polish public institutions

The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

Since 2011 the Kosciuszko Institute has been realising the Target: Cybersecurity project that was launched in response to the need of undertaking activities that would increase safety in cyberspace for the state, commercial entities, and citizens.

In order to effectively ensure the security of cyberspace, it is necessary to first diagnose all potential risks that stem from transferring a large part of state and private activities to cyberspace. The next step is to engage IT and security experts as well as institutions combating cyber threats in preparing a set of recommendations for decision-makers that will lead to improving the level of cybersecurity.

Such a strong foundation is a starting point for undertaking further activities within the project, namely the identification of opportunities that cyberspace can provide and the means to utilise its full potential.

THE GOVERNMENT CENTRE FOR SECURITY

Solving all the crisis situations that we encounter nowadays requires cooperation between a number of different services and institutions of public administration whose activities are determined by different internal procedures. Therefore it is of key importance to coordinate their work, which is precisely where the Government Centre for Security (GCS) steps in.

GCS is an institution that is involved in crisis management at the governmental level. Its main aim is to make sure that the administrative institutions are prepared to deal with all kind of crisis situations and therefore are able to provide the society with effective assistance.

One of the GCS's tasks is to analyse threats based on the data received from both public Polish institutions and from international partners. Additionally, the Centre coordinates the flow of any threat-related information.

GCS cooperates with the Cabinet, the Prime Minister, the Government Crisis Management Team and the Minister of the Interior responsible for crisis situation management. It also functions as the national crisis situation management centre. Moreover, it plays the main role in the creation of the critical infrastructure (CI) security system in Poland. The director of the GCS, together with ministers and managers of particular Central Offices, prepares CI and European CI lists as well as creates a National Critical Infrastructure Security Programme.

Furthermore, GCS is involved in planning and programme activities by developing the National Crisis Management Plan, as well as organising and conducting training sessions, and cooperating with NATO and the EU.

The Government Centre for Security was founded on 2 August 2008 in compliance with the Act of 26 April 2008 on crisis management (Art. 10) and on the basis of the ordinance of the Prime Minister of 10 July 2008 on the organisation and the mode of operation of the Government Centre for Security.

GCS is a national budget entity that is subordinate to the Prime Minister.

ABOUT EY

EY is a world leader on the professional services market involving auditing services, tax consulting, business consulting and transaction consulting. Our knowledge, experience and high quality services gained us trust with the capital market and the world economy. In the EY's ranks we have talented leaders managing well-tuned professional teams, and whose goal is to deliver on EY's promises. In this way, we contribute to improving the world we live in. We do it for our clients, communities, and ourselves.

The name EY relates to member companies Ernst & Young Global Limited, whereof each of them is a separate law unit. Ernst & Young Global Limited is a company limited by guarantee that does not perform services to private clients.

More information available at: www.ey.com/pl

ABOUT THE WKB BARRISTER'S OFFICE

The WKB barrister's office has been offering comprehensive legal services in economy law since 2004. A team of more than sixty employees introduces cutting-edge and innovative legal solutions in order to keep abreast of the dynamically evolving market conditions.

WKB offers expert consulting services in energy law, public procurement law, competition law, corporate law, intellectual property law, property law, and environmental protection. Our office has extensive experience in managing privatisation projects and transactions on the merger and acquisition market. Moreover, the WKB has a team of experienced legal proceeding specialists.

Every year, WKB increases the number of team and individual recommendations in Chambers Global, Chambers Europe, Legal 500, PLC Which Lawyer? and Who's Who Legal. Our lawyers are very highly noted in business rankings published in Polish opinion-shaping newspapers such as "Rzeczpospolita."

More information available at: www.wkb.com.pl

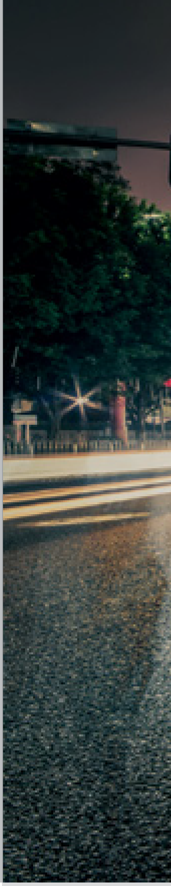
ABOUT THE MATIC COMPANY

Matic is a professional company specialising in the provision of services and solutions in the area of IT, communication, data analysis and processing, critical infrastructure protection, including cybersecurity, and defence. We offer help to entities of public administration and institutions responsible for national security. Over the last 20 years, we have successfully run numerous projects that enabled the use of the latest technology to improve security. The company has a good long-standing reputation with both private and institutional clients.

Our main goal is to offer high quality services, including comprehensive IT services and defence. The company has certified the services, maintenance, system design and production according to the ISO 9001:2001 standard. In 2013 we were also awarded ISO certification for information security management according to the 27001:2007 standard. In order to carry out defence-related projects, the company has also been granted a licence from the Minister of the Interior to produce and trade products designated for army and police.

The competences of our team focus on IT technologies, including comprehensive implementation and integration of IT systems, advanced data analysis and processing, cryptographic protection, operational management, recognition as well as tactical and operational communication.

More information available at: www.matic.com.pl



The information and communication technology systems are increasingly influencing the functionality of the most important objects, installations, devices and services being identified and designated as the components of the state's critical infrastructure (including energy and fuel supply systems, communication and ICT systems as well as financial, transport and communication systems). Given their fundamental role in ensuring the security of the entire state, it is mandatory they function impeccably. Despite the magnitude of the problem, Poland lacks a comprehensive analysis of critical infrastructure security in cyberspace. This very Report perfectly fills this gap.

The main aim of the report is to provide the institutions engaged in the protection of critical infrastructure with recommendations leading to the improvement of its security.

target: cyber security

The report has been created as part of the Kosciuszko Institute's project *Target: Cybersecurity.*

Partners

WKB WIERCIŃSKI KWIECIŃSKI BAEHR

matic IT & Defence Systems

Cooperation

FUNDACJA bezpieczna cyberprzestrzeń

PK Politechnika Krakowska im. Tadeusza Kościuszki

WAT

BBN

The representatives of the National Security Bureau have participated to the creation of the report exclusively as spectators. Any observations they made were implemented if the authors of particular sections of the report decided to do so. The report does not present an official standpoint of NSB.

ISBN: 978-83-63712-22-8

THE KOSCIUSZKO INSTITUTE