Chapter 7
Cyber Threats Impacting Critical Infrastructures

Michał Choraś, Rafał Kozik, Adam Flizikowski, Witold Hołubowicz and Rafał Renk

Abstract Nowadays it is important to note that security of critical infrastructures and enterprises consists of two factors, those are cyber security and physical security. It is important to emphasise that those factors cannot be considered separately and that the comprehensive cyber-physical approach is needed. In this paper we analyse different methods, methodologies and tools suits that allows modelling different cyber security aspects of critical infrastructures. Moreover, we provide an overview of goals an challenges, an overview of case studies (which show an increasing complexity of cyber physical systems), taxonomies of cyber threats, and the analysis of ongoing actions trying to comprehend and address cyber aspects.

1 Introduction

The CPS abbreviation stands for Cyber-Physical Systems and it refers to systems that have distributed natures, are comprised of physical elements that work in a real-time and are capable of communicating with each other by means of communication network (both wired and wireless, see Fig. 1). CPS integrate computational, communication and physical aspects in order to improve usability, efficiency, reliability, etc. However, such combinations, introduce a wide spectrum of risks related to cyber domain (e.g. privacy issues, cyber attacks).

The CPS are comprised of elements that allow for reading relevant information about controlled physical process (e.g. sensor) and elements that allows for influencing (via actuators) the behaviour of this process. The CPS are widely adapted in many critical sectors including energy, water, and transportation as well as in the area of smart houses, vehicles, etc.

M. Choraś (✉) · R. Kozik · A. Flizikowski · W. Hołubowicz · R. Renk
Institute of Telecommunications and Computer Science,
UTP University of Science and Technology, Bydgoszcz, Poland
e-mail: chorasm@utp.edu.pl

W. Hołubowicz · R. Renk
Adam Mickiewicz University, Poznań, Poland

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_7

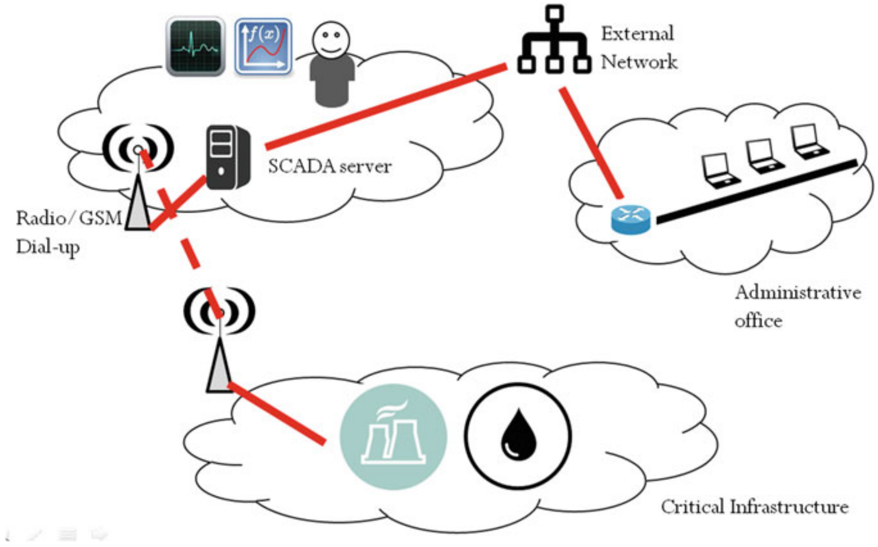


Fig. 1 Dependencies between complex systems comprising CPS

Currently, the CPS are on the direction to become an integral part of our lives, embracing in the near future such aspects as healthcare, disaster recovery, engineering, traffic control, robotic surgery, sea and space exploration, defence and military operations.

This paper is structured as follows: firstly, we analyse goals and challenges in area of cyber security of critical infrastructures, presenting case study overview and elaborating on the impact of the cyber domain on the real world. Next, we provide short overview of the taxonomies used to model and to analyse the cyber threats. Afterwards, we provide an general overview on how the cyber security life-cycle is modelled in terms of crisis management and critical infrastructures protection. Particularly, we focus on different approaches to cyber risk identification and cyber incidents handling. In the following section, we present different aspects of IT and physical networks that can be modelled with the formal tools and methodologies. The analysis of ongoing actions trying to comprehend and address the challenges of cyber aspects of critical infrastructures as well as the conclusions are given afterwards.

2 Goals and Challenges

Quantitative evaluation of cyber security is always a challenge in the area of computer science. For the CPS, the integration of ICT technologies with physical elements has introduced new threats. Currently, we may find many examples of the attackers have been able to compromise complex systems by finding vulnerable elements. In many cases those attacks have had direct impact on physical elements. Therefore, there is an ongoing effort to embrace the cyber aspects of CPS with comprehensive tools and methodologies that commonly leverage wide spectrum of technical and non-technical means. The current challenges related to CPS can fall into following groups of problems:

- Security,
- Scalability,
- Complexity,
- Subsystems interoperability.

Of course, such problems should be handled in the holistic manner, e.g. by the THOR (Technical, Human, Regulatory, Organizational) approach and aspects as proposed by recently finished European projects [1, 2].

As the cyber security of CPS systems imposes a significant challenge, in this section, we particularly focus on different aspects of the cyber domain. We start with examples of case studies that in many cases reveal the complex nature of those systems and huge amount of interconnections that span across different levels of Critical Infrastructure management.

Afterwards, we provide examples of how the European Union addresses current problems and the challenges in the H2020 work program.

2.1 Cyber World and Real Impact—Selected Case Studies

Due to the fact that the energy sector is quickly evolving and it is widely adapting different ICT technologies, we are able to identify many high profile cyber incidents. One of the most important cyber attacks in history of Critical Infrastructures happened in 2012 [3], when Iran authorities announced that computers controlling one of its nuclear processing facilities had been infected with malicious software called Stuxnet. It was the first case in which industrial equipment was a target of computer attack. Since that date, the cyber community has realised that cyber weapon can be used "… to create physical destruction […] in someone else's critical infrastructure…" [4].

Also for the water sector, we are able to find relevant cyber incidents, which show a real and high impact of the cyber world on physical infrastructures. Similarly as for Energy sector, the cyber components for both drinking water and wastewater facilities include control systems known as Supervisory Control and Data Acquisition (SCADA) systems. Cyber attacks on such utilities may cause cascading effect on a public health, economics, and nations as whole. An example presented in [5] shows how the attacker can influence water treatment plants. According to IBTimes [5], attackers infiltrated the water plant and were able to change the level chemicals that were used to treat drinking water.

Healthcare industry is also an important part of critical infrastructure. It is also targeted by cyber criminals. As examples show [6, 7], cyber-attacks targeted at this sector can slow down hospitals and expose patients to danger.

Also the financial sector is struggling with cyber attack. According to [8] the activity of cyber criminals increased by 41% in recent years. Recent example of Bangladesh bank [9] show that attackers have effective tools and skills to infiltrate bank institutions and to steal serious amounts of money.

According to the [10], also the growth of the Internet of Things and complexity of industrial control systems will lead to more vulnerabilities in hardware systems. Many companies dealing with cyber security [1] have identified serious vulnerabilities in automotive systems and home-automotive systems. This shows that not only critical infrastructures but also citizens directly are currently impacted by the attackers as the cyber domain embraces increasing number of our lives.

2.2 The Coordinated Cyber Attack—Ukrainian Case

On the 23rd December 2015, the Ukrainian power distribution operator Prykarpattya Oblenergo was suffered attack on their ICT infrastructure performed by the third party. In effect of this breach, operation of a number of power substations were interrupted and about 80 thousands of customers from Ivano-Frankivsk region were suffered an outage for next three to six hours, according to the official information published through the operator website. At the same time, the operator informed publicity about other technical failure related to the operation of the call centre infrastructure. This caused impossibility for the customers to contact operator during the blackout and deepened the crisis.

The above described circumstances indicate that the energy operator faced the well-coordinated attack, that can be decomposed into three elements: a malware attack, a denial of service attack targeted at the call centre functionalities and the opening of substation breakers to cause the outage.

Firstly, the attackers infected the main servers controlling the electricity distribution process, they infiltrated in the victim's network (possibly using a malware backdoor) and issued a command to open breakers of various substations.

The goal of the cyber criminal was to enter the power grid system by infecting the victim's machines with malware software. They used macro script in Excel files to drop the malware. The infected Excel spreadsheets have been distributed during a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine.

After the power was cut off, DoS attacks were launched to limit the target's awareness of the consequences of the attack—error messages did not reach service personnel what prevented from proper reaction on the crisis and delayed the recovering of the infrastructure operation.

The Ukrainian blackout case can be seen as the one of the first significant and publicly reported cyber attacks aimed at civil infrastructure and directly impacting civil population (e.g. in opposition to the Stuxnet, Iranian case, where industry/military premises were infected). Ukrainian case shows that motivated attackers are able to cause serious damages to the economy and public safety of countries.

In case of the Ukrainian grid, luckily at that time, the manual mechanical reaction was possible. It would rather not be possible in case of the much modern and automated energy grids in some other countries.

2.3 Hybrid Conflicts

The Ukrainian case (described in the previous subsection) gives the short glance at the possible impacts of the successful cyber attack launched at the critical infrastructure such as energy grid. Unfortunately, due to the current geo-political situation and the current market of hackers (state and non-state), there is a significant threat that a country or its critical infrastructure can be attacked by another country or hackers organization working for another hostile country. It is worth to notice, that nowadays most hackers work for organizations rather than on their own (it changed significantly since in the past there were more freelancers than hackers working for organizations). In other words, cyber attacks might be a part of so called hybrid war or hybrid conflict, where (at least at the first stages) traditional military measures (such as soldiers) are not used, but the focus is on other destabilizing aspects like cyber attacks, cyber propaganda, influencing social media and electronic media etc. If the worst scenarios become reality, the successful coordinated cyber attacks launched at critical infrastructures such as banks (no possibility to draw money from ATM), energy (no electricity), transport, media etc. could paralyze societies, countries and create chaos.

Therefore, in order to avoid situation like in the Ukraine, the effective solutions and techniques to protect cyber physical systems are needed. The created recommendations and technologies should cover the wide spectrum of aspects, such as technological, organizational, human and regulatory (similarly to the THOR approach suggested by the new cyber roadmaps by projects like CAMINO, COURAGE and CyberRoad) [2, 11].

3 Cyber Threats Taxonomies

An important part of CPS cyber threats modelling is the taxonomy of cyber threats. To combat the cyber crime effectively, it is required to identify, define and classify the problem. It is not a trivial task, and currently even the spelling of the related words is not agreed, some use cybersecurity or cyber security or cyber-security. Similarly with other words like cybercrime, cyberterrorism etc.

A taxonomy is most often defined as a classification of terms and has close a relationship with the use of ontology. The primary purpose of ontologies and taxonomies is to use them as the basis for processing, communicating and reasoning about the cyber-related aspects and threats.

Also as noted by Furnell [12], having a consistent classification of cyber crime is beneficial for bodies and organisations interested in cyber counterterrorism. One of the earliest cyber crime classifications was established by UK Audit Commission and proposed in [13]. This categorisation identifies different groups of cyber crime activities, like: Fraud (for private gain of benefits), Viruses, Theft (of data or software), Use of unlicensed software, Hacking, Sabotage, Misuse of personal data, Introducing pornographic material.

In Furnell [12] proposed classification that is based on two major types of the cyber crime, namely computer-assisted and computer-focused. The computer-assisted cybercrimes are these which use computer as supporting tool and where the target is not to be directly connected with the cyberspace (e.g. harassment). The computer-focused category of crimes includes these incidents that are almost entirely technical, associated with ICT systems and not (or weakly) connected to other sectors.

Similar dichotomized categorisation (as by Furnell) has been proposed by Gordon and Ford [14]. Authors divided cyber terrorism into two distinct classes, namely: (i) Type I Cybercrime, which is mostly technological in nature, (ii) Type II Cybercrime, which has a more pronounced human element.

Different classification is proposed in [15]. It is mainly focused on subject of criminal activity and defines following main categories, namely: against individual, against property, against organization, against society.

In opposite Walden [16] has postulated that there are five possible schemas of classification that overlap but are different in their perspective. These are: technology-based, motivation-based, outcome-based, communication-based and information-based crimes.

According to [17] motivation-based classification schema provides more holistic perspective on the topic cybercrime. The proposed motivational model is composed of five major components: people, motivation, perpetration technology, security barrier and the target. The people in the model refer either to offenders or criminals. When individuals are exposed to a certain type of the factors they may become motivated to carry out particular behaviour and commit a crime. The motivation component refers to certain factors like unemployment, low median income, poverty, or social status that push the individual to carry out a cyber crime. The perpetration technology refers to technology used as a tool to commit a crime, while security barrier indicates components (firewalls, anti-virus software, etc.) that need to be comprised in order for crime attempt to be successful. The last component of the model indicated as Target refers to the people or organization that are being targeted by a criminal.

One of the approaches intending to comprehend cyber security aspects of critical infrastructures have been attempted by the European Union-sponsored project named Vital Infrastructure Threats and Assurance (VITA) [18]. One of the outcomes of the project was a generic threat taxonomy for Critical Infrastructures (CIs). It categorises such aspects as threat cause, human intent, threat, etc. It is emphasised by authors [19] of the taxonomy that terror, sabotage or activism are not threats but motivations.

In [20] authors adapted and extended the VITA threat taxonomy for Smart Grids. While identifying threats authors have addressed both the information and infrastructure dimension. Authors particularly wanted to identify how Smart Grid hardware may influence the resilience and reliability of energy grids.

Recently, the taxonomy of the cyber crime and cyber terrorism was discussed in [1].

4 CIP Cyber-Physical Security Life-Cycle Models

A wide spectrum of services provided by intelligent critical infrastructures (e.g. Smart Grids) heavily depend on Cyber-Physical Systems (CPS) that are able to monitor, share and manage information. On the other hand, an increasing number of cyber attacks and security breaches are part of rapidly expanding cyber threat, which in many cases has form of cyber terrorism.

The cyber-physical security can be analysed from classical crisis management point of view. In fact, most of incident management processes in the cyber domain follows the ITIL model that is depicted in Fig. 2. It focuses on incidents detection, diagnosis (e.g. identification of exploits that attacker exploited), repairmen (e.g. elimination of the software vulnerability that attacker exploited), recovery and restoration (e.g. to normal business operation status).

However, this type of model may not properly show the iterative nature of continuous improvement that usually are implemented after the crisis as an element of lessons learnt. Therefore, the model of cyber security life-cycle would be that one which is intended to define how to prevent, detect, respond to and recover from cyber crisis, and finally to avoid reoccurrence. Thus, we can define Cyber Attack Timeline, illustrated in Fig. 3, which is constituted of the following three phases:

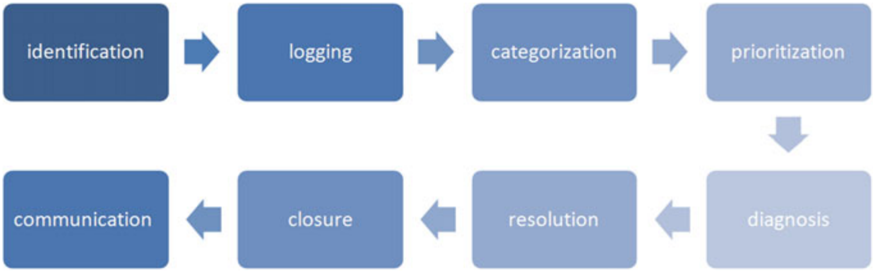


Fig. 2 Incident management according to ITIL standard [35]

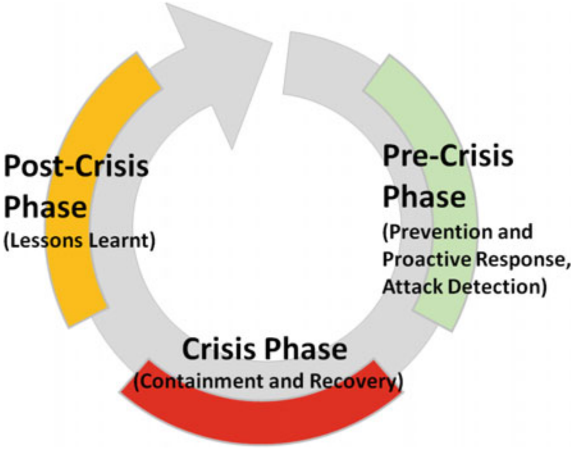


Fig. 3 Cyber crisis management cycle

- A Pre-Crisis (Steady State) phase in which organization aims at providing all services as usual while increasing the preparedness to an critical event. For this phase it is important to have risk management process that will allow the organization for risk anticipation and proactive response.
- A Crisis phase in which a threat has to be maintained and system recovered. It is an emergency case in which it is necessary to change the approach so that threats can be quickly removed and their effects mitigated.
- A Post Crisis phase during which the "lesson learned" as a result of the Crisis phase needs to feedback the whole process in order to reduce its impact in the future.

In this section, we further elaborate on different aspects related to cyber security of CPS systems that is embraced into crisis management phases namely: prevention, detection, containment, and post-incident.

4.1 Pre-crisis Phase

4.1.1 Prevention and Proactive Response

The cyber security prevention is an important aspect when it comes to cyber-physical systems and its impact on critical infrastructures. It requires some amount of the resources to be allocated, however, it is better than often costly recovery (or in worst case no recovery at all). As the value and importance of prevention is at least well acknowledged in the communities, it is still in many cases perceived as product that can be purchased and deployed in an organisation. In fact, the prevention is long-lasting and continuous process reaching far beyond technical problems embracing organisational, regulatory, and human aspects.

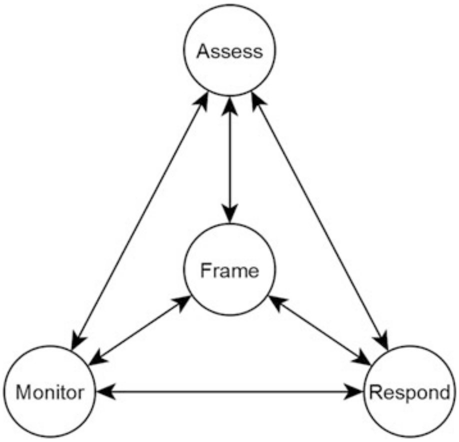


Fig. 4 Risk management—information and communication flows (NIST SP 800-39)

Particularly, the cyber attack prevention requires (within the organisation) well established roles that will be responsible for containing the cyber attack and its causes. This implies that an organisation should define detailed cyber incident response plan that will describe how an incident should be reported, investigated and responded (Fig. 4). Moreover, when the cyber incident involves personal information, it implies various data privacy and security laws that may have different shape in different countries.

As mentioned in [21], it is very important for Critical Infrastructures operators to identify the risks posed by the communication networks and existence of dependencies with third party systems. This is even more important form wider perspective, because such risk anticipation can prevent the possibility of cascading failures causing catastrophic system damages.

The risk management cycle is a comprehensive process (Fig. 2) that requires organizations to:

- frame the risk (i.e., establish the context for risk-based decisions),
- assess the risk,
- respond to the risk once determined,
- monitor the risk.

Usually this requires effective communication and an iterative feedback loop, that will facilitate continuous improvement in the risk-related activities.

As it is suggested by ENISA [22], a good practice for well-suited prevention mechanisms is to subscribe to relevant information sources that would give up-to-date overview of current cyber threats and incidents reported. ENISA also stresses the importance of information sharing.

More local (service based) approach to risk modelling has been proposed by OWASP [23]. The approach follows the idea of decomposition of complex system to smaller components (see Fig. 5 Threat Risk Modelling proposed by OWASP). It is important to stress the fact that all key players (e.g. security officers, employees)

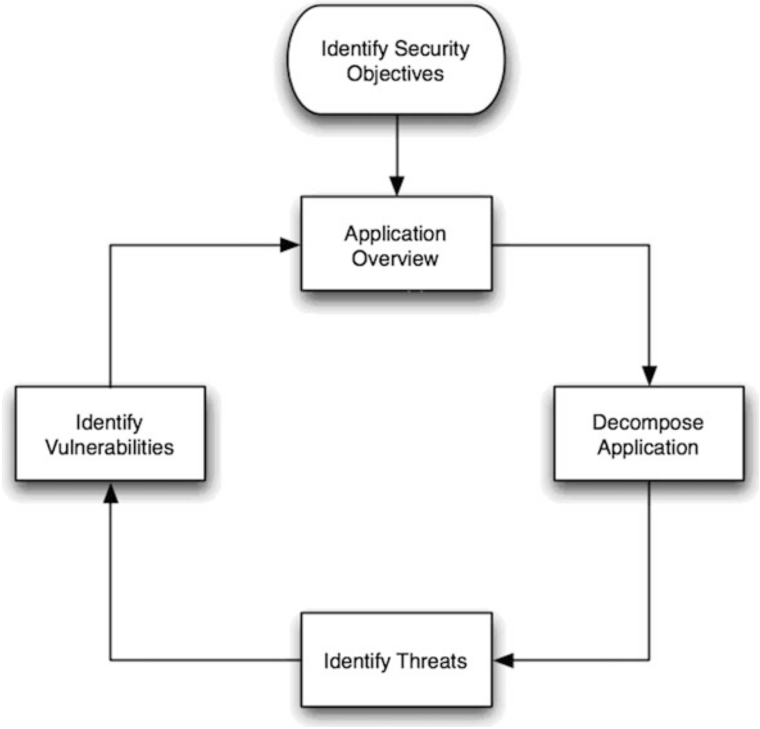


Fig. 5 Threat risk modelling proposed by OWASP [23]

need to understand the security objectives. Therefore, usually the complex system is broken down into objectives such us: reputation, availability, financial, etc. Other security objectives may be enforced by the law (financial or privacy laws), adapted standards (e.g. ISO).

The key element of this risk assessment methodology is the possible threats identification. Microsoft has suggested two different approaches to identify those threats. One is a threat graph (see Fig. 6), as shown in Fig. 2, and the other is a structured list.

4.1.2 Threat Detection

The capability of early detection of cyber threats is a very important element for good cyber crisis preparedness. Probably, one of the most classic way to categorise the cyber attack detection technique is to assign them into one of the following groups, namely: signature-based, anomaly-based or hybrid (Fig. 7).

Each of this class of algorithms has their drawbacks and advantages, and different approaches to identify attacks. Some of the methods have also different

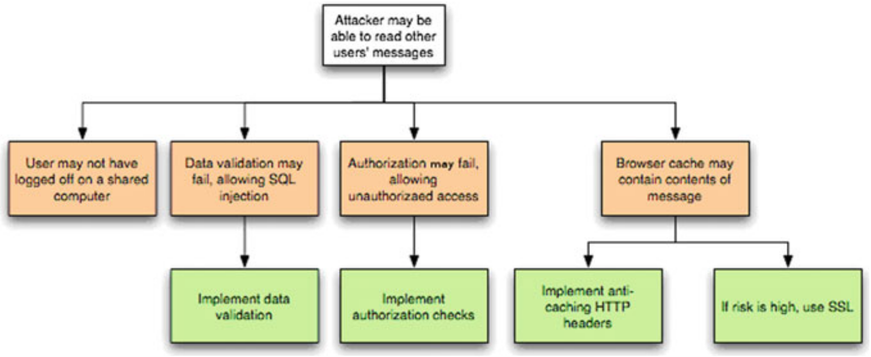
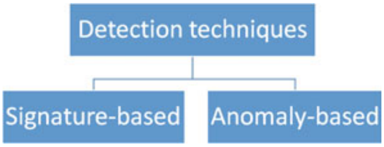

Attacker may be able to read other users' messages
User may not have logged off on a shared computer
Data validation may fail, allowing SQL injection
Authorization may fail, allowing unauthorizaed access
Browser cache may contain contents of message
Implement data validation
Implement authorization checks
Implement anti-caching HTTP headers
If risk is high, use SSL

Fig. 6 Threats identification [23]

Fig. 7 Attack detection techniques classification



methods for data aggregation (e.g. host-based or network-based) and traffic properties description (e.g. packet-based analysis or aggregated connections flows). All the above mentioned aspects are dissuaded in the consecutive subsections.

The Signature-based category of cyber attacks detection typically include Intrusion Prevention and Detection Systems (IDS and IPS) which use predefined set of patters (or rules) in order to identify an attack. The patterns (or rules) are typically matched against a content of a packet (e.g. TCP/UDP packet header or payload). Commonly IPS and IDS are designed to increase the security level of a computer network trough detection (in case of IDS) and detection and blocking (in case of IPS) of network attacks.

Commonly the patterns an attack for IPS and IDS software are provided by experts form a cyber community. Typically, for a deterministic attacks it is fairly easy to develop patterns that will clearly identify given attack. It often happens when given malicious software (e.g. worm) uses the same protocol to communicate trough network with command and control centre or other instance of such software. However, the problem of developing new signatures becomes more complicated when it comes to a polymorphic worms or viruses. Such software commonly modifies and obfuscates its code (without changing the internal algorithms) in order to be less predictive and easy to detect.

4.2 Crisis Phase

In this phase risk management is not important, because it gives priority to incident management in order to solve crisis and mitigate threats by adopting proper countermeasures. However, it is worth mentioning that the emergency and contingency procedures adopted during a Crisis Phase are developed during the Pre-Crisis phase. In other words, during the Crisis phase it is not only important to have an overall situational awareness picture, but also to have a strategy to recover form crisis in the most efficient way possible. There are different models for cyber incidents handling. For instance, ENISA defines (see Fig. 8) formal manner starting from incident reporting, going through analysis and recovery, and concluding with post-analysis followed by improvements proposal. This model of cyber crisis response is widely adapted by Emergency Response Teams (CERTs). According to definition provided by ENICS [24] CERTs are the key institutions that are obliged to receive, inform and respond to cyber security incidents. At the same time, they act as educational entities in order to raise the cyber-related awareness and provide primary security service for government and citizens. Every single country that is connected to the Internet should have capabilities to respond to cyber-related security incidents. Nevertheless, not every country has such capabilities. One of the

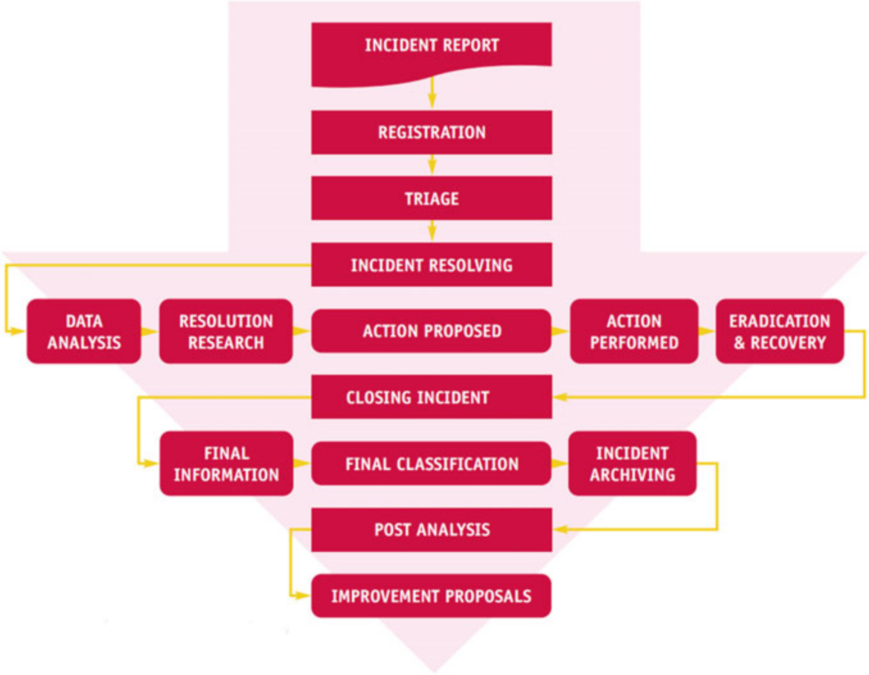


Fig. 8 ENISA incident handling model [22]

earliest CERT teams focused on critical infrastructures was the US ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) that was established in 2009 [25]. This institution aims at reducing the impact of cyber attacks. In order to achieve this goal ICS-CERT takes preventative actions such as vulnerability monitoring and reporting (each year ICS-CERT releases annual reports in order to spread the information about the security incidents).

However, before the actual incident handling will take place, usually the incident is verified and pre-classified, in order to assess its significance, severity and time constrains required to resolve it. This activity is named triage and refers to situation in which there are limited resources and the decision maker has to decide on the priorities of actions relying on the severity of the particular cases.

An important thing, which is not directly reflected by the incident handling model, is fact that CERTs also collaborate with other Computer Emergency Response Teams that are part of international or private sector institutions. This cooperation allows the CERTs to share the information about control systems-related security incidents and mitigation measures.

4.3 Post-crisis Phase

The post crisis phase is the phase in which threat has been eliminated and system has been repaired, thus allowing the restoration of provided services and return to usual business activities.

As recent cyber incidents show, it is important for the Critical Infrastructure operators to have employees that would be educated and skilled in cyber security aspects. The post-crisis phase is important for an organisation to draw some conclusion after the crisis and use this time as an opportunity to increase the number of cyber security professionals at various levels of skill and competence, as well as to upgrade the competence levels of the already hired staff.

In fact, learning from previous experiences is a continuous process for the organisation. According to the terminology adapted in [26] this problem can be decomposed into:

- acquiring experience,
- gathering and analysing experience,
- applying experience.

Obviously, in order to address all of above mentioned aspects, it is necessary to have resources allowing for relevant data gathering and analysis. In many cases, dedicated tools facilitating the end-user with such functionalities are used. Particularly, in the post-crisis phase it is necessary to collect the lessons learnt and analyse the overall crisis scenario from wider perspective in order to identify root cause of the crisis and procedural pitfalls that may have been identified.

In particular, a new risk analysis must be performed in order to evaluate if the previously defined security controls are still effective and to estimate whether risk levels have been changed.

5 Modelling Cyber Security Aspects

There are different approaches to model cyber security aspects. Depending on the goal of the modelling process one can divide these as problem of modelling the (Fig. 9):

- Network,
- Risk,
- Cyber Attack,
- System Behaviour.

5.1 Network Modelling

As for the Network modelling, one can use different network simulation tools (e.g. NS3, NS2, OPNET, NetSim) to analyse selected impacts of cyber attacks on modelled network. For instance, in [27] authors used NS2 simulator to predict the impact of malware propagation, Denial of Service and Man In The Middle attacks on SCADA systems. The authors measure the impact among others in terms of loss of control, Quality of Service (QoS), and number of dropped packets.

Different tools suits allow the user to model different aspects of telecommunication network with a varying granularity using different modelling techniques. In the NS3, the topology and the configuration of the simulation are provided either in *.py (python) or in *.cc (c/c++) files. Commonly, these files contain the following information:

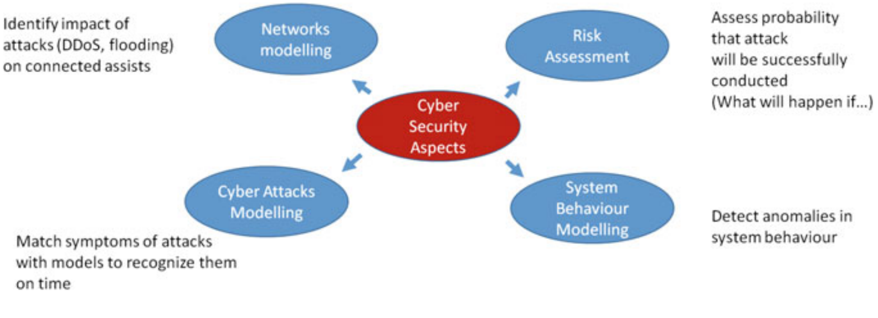

Identify impact of attacks (DDoS, flooding) on connected assists
Networks modelling
Risk Assessment
Assess probability that attack will be successfully conducted (What will happen if...)
Cyber Security Aspects
Cyber Attacks Modelling
System Behaviour Modelling
Detect anomalies in system behaviour
Match symptoms of attacks with models to recognize them on time

Fig. 9 Different approaches to model cyber aspects

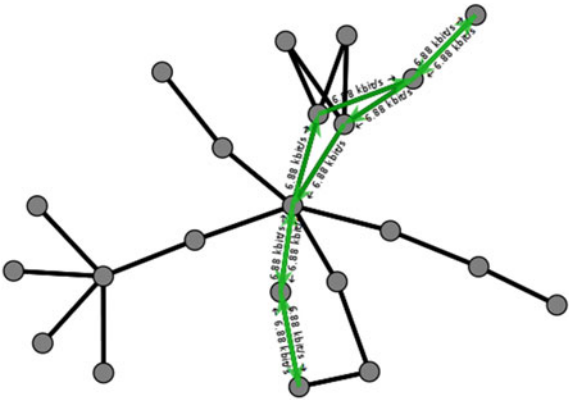


Fig. 10 Example of network topology visualized with PyViz (NS3)

- Nodes definition (names, types, positions, etc.)
- Communication links definition (data rates and delays)
- Topology definition
- IP stack installation
- IP addresses assignment
- Routing definition
- Configuration of the application layer.

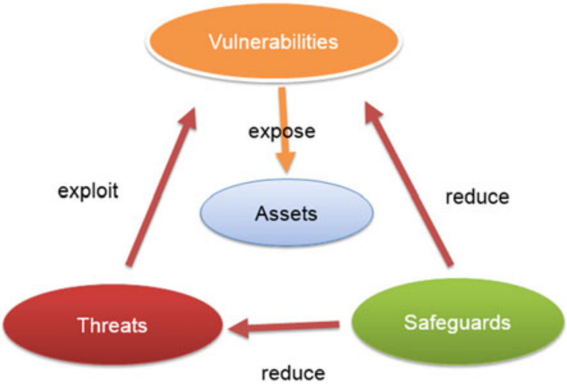
In NS3 the term node is used to name an abstract device connected to a network such as end-users hosts, end-systems, routers, switches, hubs etc. Since NS3 does not focus on Internet technologies only, it is the responsibility of simulation creator to define nodes properly by adding applications, protocols stack, etc. In NS3 the concept of application is defined as an element that runs the simulation. It is the basic abstraction of a user program, which generates some network traffic. The NS3 allows the user to use additional tools to visualise simulation at a runtime (see PyViz in Fig. 10) and to prototype the network topology with GUI-enabled software.

5.2 Cyber Risk Assessment

The goal of the tools and methods used for the modelling the cyber risk is similar to the previous approach, however the approach is substantially different. For instance, the aim of tools like Haruspex [28], is to evaluate the probability that an adversaries can implement successful cyber attack against a system. Haruspex implements the simulation as model comprising of threat agents and the attacks they convey. The system is modelled as a set of components interacting through channels. As a final result, the tool collects relevant statistical data from the simulations.

Similar approach to probability-based risk evaluation is presented in [29]. The authors have adapted an ontology to model the system, its key components and interaction between them. Main concepts, which compose main classes of proposed

Fig. 11 High-level overview of key classes in the ontology



ontology (see Fig. 11) are Assets (anything that has value to the organization), Vulnerabilities (include weaknesses of an asset or group of assets which can be exploited by threats), Threats (potential cause of an unwanted incident which may result in harm to a system or organization), Safeguards (practices, procedures or mechanisms that reduce vulnerabilities).

As argued by the authors, the ontology-based data models allows for addressing the complexity, diversity, and sparsity of dependencies. An example of instantiated ontology classes is shown in Fig. 12.

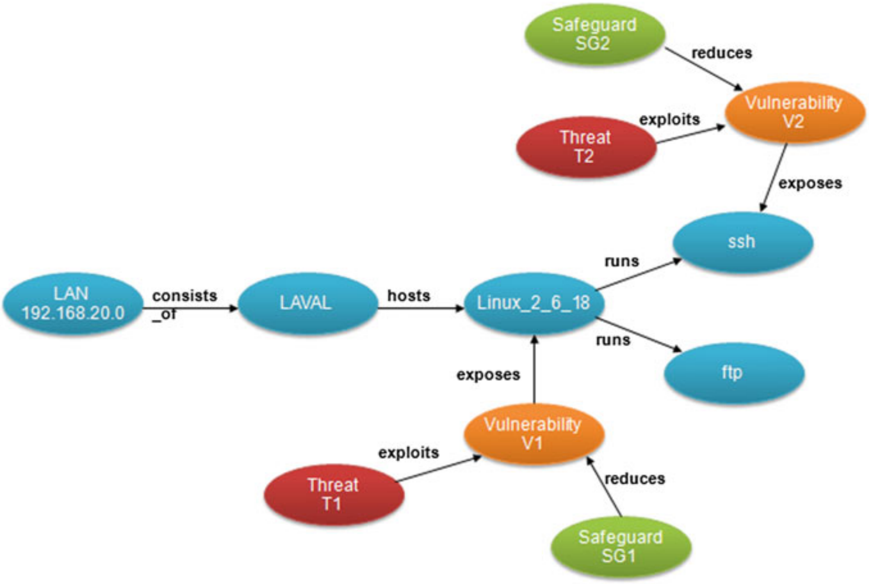
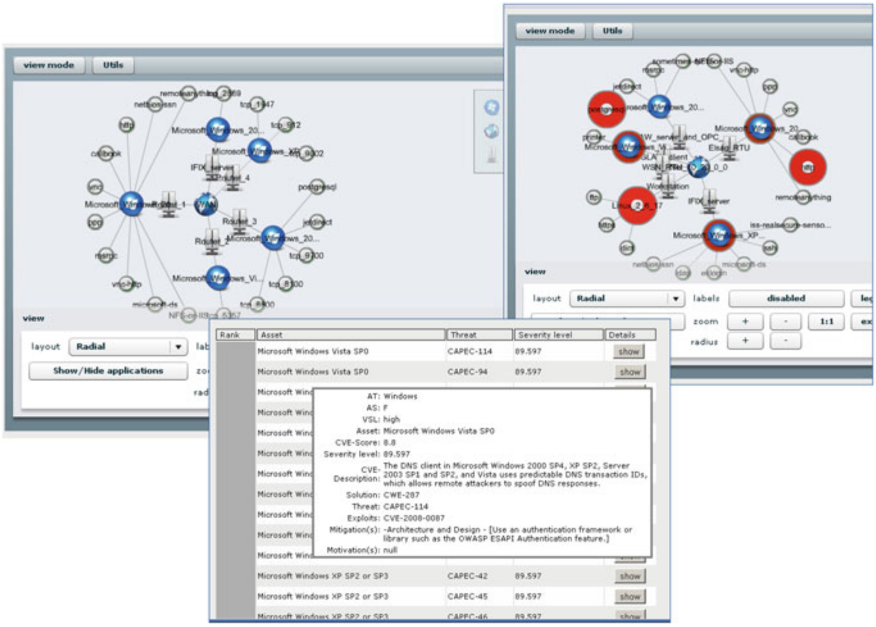


Fig. 12 Ontology-based data model describing elements and dependencies between elements



Rank	Asset	Threat	Severity level	Details
	Microsoft Windows Vista SP0	CAPEC-114	89.597	show
	Microsoft Windows Vista SP0	CAPEC-94	89.597	show
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Win			
	Microsoft Windows XP SP2 or SP3	CAPEC-42	89.597	show
	Microsoft Windows XP SP2 or SP3	CAPEC-45	89.597	show
	Microsoft Windows XP SP2 or SP3	CAPEC-46	89.597	show

AT: Windows
AS: F
VSL: high
Asset: Microsoft Windows Vista SP0
CVE-Score: 8.8
Severity level: 89.597
CVE-Description: The DNS client in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, and Vista uses predictable DNS transaction IDs, which allows remote attackers to spoof DNS responses.
Solution: CWE-287
Threat: CAPEC-114
Exploits: CVE-2008-0087
Mitigation(s): -Architecture and Design - [Use an authentication framework or library such as the OWASP ESAPI Authentication feature.]
Motivation(s): null

Fig. 13 Example of analysis conveyed by DAT tool [29]

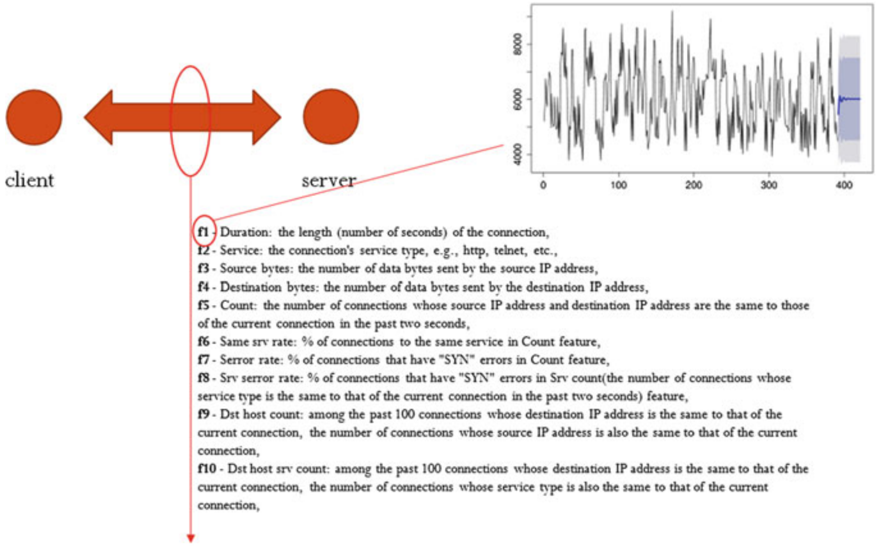
The results of the analysis conveyed with this tool is an interactive security report (see Fig. 13). It allows the operator to go through the list of identified threats and get the detailed description accompanied with security counter measure that is likely to eliminate (or decrease) given risk.

5.3 System Behaviour and Attacks Modelling

The underlying motivation for system and attack modelling is the evolvement of tools and techniques in the area of artificial intelligence, data mining, and classification. Those techniques allow for automated data analysis, novelty and anomaly detection without extensive understanding of the underlying data content. The anomaly-based methods for a cyber attacks detection build a model that is intended to describe normal and abnormal behaviour of network traffic.

The approach to adopt these techniques is in many cases similar. Firstly, sensors collecting relevant data are deployed across network. Typically, these data require further processing in order to extract relevant information (average value of measured physical property or number of packet transmitted, see Fig. 14).

Commonly such methods uses two types of algorithms from machine learning theory, namely unsupervised and supervised approach.



f1 - Duration: the length (number of seconds) of the connection,
f2 - Service: the connection's service type, e.g., http, telnet, etc.,
f3 - Source bytes: the number of data bytes sent by the source IP address,
f4 - Destination bytes: the number of data bytes sent by the destination IP address,
f5 - Count: the number of connections whose source IP address and destination IP address are the same to those of the current connection in the past two seconds,
f6 - Same srv rate: % of connections to the same service in Count feature,
f7 - Serror rate: % of connections that have "SYN" errors in Count feature,
f8 - Srv serror rate: % of connections that have "SYN" errors in Srv count(the number of connections whose service type is the same to that of the current connection in the past two seconds) feature,
f9 - Dst host count: among the past 100 connections whose destination IP address is the same to that of the current connection, the number of connections whose source IP address is also the same to that of the current connection,
f10 - Dst host srv count: among the past 100 connections whose destination IP address is the same to that of the current connection, the number of connections whose service type is also the same to that of the current connection,

Fig. 14 A conceptual overview of on-line analysis

For unsupervised learning commonly clustering approaches are used that usually adapt algorithms like k-means, fuzzy c-means, QT, and SVM. The clustered network traffic established using mentioned approaches commonly requires decision whenever given cluster should be indicated as a malicious or not. Pure unsupervised algorithms uses a majority rule telling that only the biggest clusters are considered normal. That means that network events that happens frequently have no symptoms of an attack. In practice, it is a human role to indicate which cluster should be considered as the abnormal one.

The supervised machine learning techniques requires at least one phase of learning in order to establish the model traffic. The learning is typically off-line one and is conducted on specially prepared (cleaned) traffic traces. One of the exemplar approaches to supervised machine learning for cyber attack detection use auto regression stochastic process (AR). In literature there are also methods using Kalman filters. Recently, more gaining in popularity are solutions adapting SVM, neural networks, and ID3-established decision trees.

6 Ongoing Efforts

6.1 H2020 Work Program View on CPS Aspects

The research topics defined for the security call in Horizon 2020 programme reflect the need for securing Critical Infrastructures—both physically as well as in digital domain, preventing them from cyber-attacks. For example, the topic CIP-01-2016-2017 entitled "Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe" addresses aspects of cyber and physical security convergence to protect installations of the critical infrastructure of Europe. The challenge related to such protection is not only addressing separately physical threats to CI (such as bombing and other terrorists acts and natural-born threats as seismic activities or floods) and cyber threats, but establishment of security management paradigms that include the combinations of both group of threats, analysis of their interconnections and cascading effects resulting from cyber or physical damages. Also, it is expected that research initiatives acting under this topic will pursuit solutions related to sharing information with the public in the region of affected installations, and the protection of rescue teams, security teams and monitoring teams. The main expected results of the research in short- and medium-term perspectives include analysis of physical/cyber detection technologies and risk scenarios in the context of a specific critical infrastructure, analysis of physical-cyber vulnerabilities of a specific critical infrastructure, development of tools, concepts, and technologies for combating both physical and cyber threats to a specific critical infrastructure. These tools should be innovative, integrated, and dedicated to prevent, detect, respond and mitigate physical and cyber threats and enabling monitoring of the environment, communication with the inhabitants in the vicinity of the critical infrastructure. In long-term perspective, achievement of convergence of safety and security standards, and the establishment of relevant certification mechanisms are expected in this area.

Another example of topic in which the importance cyber-physical security is emphasized is DS-01-2016: "Assurance and Certification for Trustworthy and Secure ICT systems, services and components". In particular, specific nature of CPS systems (that smart meters are highly connected to) as evolving, complex and dynamically changing environment makes critical security-related decisions very challenging and demanding a technology-based support.

Moreover, topics from past security call (H2020 WP2014-15) also addressed problems of cyber-physical security convergence. One of examples was DRS-12-2015 topic, entitled "Critical Infrastructure smart grid protection and resilience under smart meters threats", under which physical safety (threat of undesired physical access to smart meters) was examined alongside other cyber threats.

6.2 Security Standards for Critical Infrastructures

In this section we provide the short overview of wide spectrum of different standards that address the cyber (as well as physical) security aspects of critical infrastructures.

The ISA99 committee addresses the cyber security of industrial automation and control systems by its ISA/IEC-62443 series of standards. The scope of the ISA99 standards is very broad, i.e. the committee does not limit application of its standards to the specific type of plants, facilities or systems. Manufacturing and control systems to which the ISA/IEC-62443 can be applicable include hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, monitoring and diagnostic systems as well as associated interfaces used to provide control, security, and continuity of industrial processes. In the ISA/IEC-62443 series of standards physical security is not directly addressed, despite the fact that physical security highly impacts the integrity of any control system environment [30].

The NERC (North American Electric Reliability Corporation) CIP plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system. This set includes 9 security standards and 45 requirements and addresses security of electric systems and the protection of the critical cyber assets operating within these systems. Cyber security training, management and crisis recovery are also included. Physical security of Critical electric systems is covered by the CIP-006-1: Physical Security of Critical Cyber Assets sub-standard [31, 32].

The IEC 62210 technical report on "Data and Communications Security" can be applied to supervision, control, metering and protection systems in electrical utilities. The report covers a broad range of security related aspects such as definitions, prioritization of threats, consequence analysis, attacks, policies and "Common Criteria" protection profile. Communication protocols used within and between systems, secure use of the systems and access to them are also discussed. Consequence analysis was adopted in the report as the security methodology for prioritization of assets and threats to the security of the some industrial protocols e.g. TC 57 protocol used for power systems management and exchange of associated information. However, as it is stated in the report, the document does not include recommendations or criteria development related to physical security of critical systems [33]. In addition, IEC 62351 is a series of technical specifications covering aspects of information security for power system control operations. Selected aspects that are discussed in IEC 62351 are authentication of data exchange (digital signatures, certificates), security of TCP/IP (e.g. encryption), networks and systems security management and key management.

Also the IEEE 1402 standard applies to the power distribution and critical energy infrastructures protection, however in a contrary to above described IEC documents, this standard addresses aspects of physical security, especially in a context of unauthorized access to electric power substations. The document describes and guides a variety of methods to prevent such substations from human intrusion [34].

7 Conclusions

In this paper we have described various cyber security aspects related to the cyber-physical systems and critical infrastructures. We have described current challenges related to the technical aspects as well as the European vision on that matters. As we currently observe, due to the evolution of Internet and the wide adoption of the Internet of Things concept, we may expect that in the near future the cyber security of cyber-physical systems will become of even higher importance. As gradually increasing number of elements and aspects (smart devices, homes, cars, etc.) of our lives becomes connected to the Internet, it gives new opportunities and motivations for the cyber criminals to research and to exploit technological vulnerabilities in order to gain economical profits. Those attempts cannot be successful with regards to critical infrastructures and homeland security.

Therefore new technological and organizational solutions are needed for cyber physical systems protection. There are also many urgent questions and aspects to be addressed by nations and companies, such as if the standards and guidelines for cyber security should be obligatory and mandatory (which also involved controlling organizations and possible penalties), or if those should rather be voluntary. Moreover, the minimal security standards have to be defined. Another difficulty is to find the right balance for the appropriate level of details of recommendations and standards. Should those be rather general, universal and high level (for further customization for each organization), or should those be as detailed as possible mentioning particular technologies and solutions to be applied. At the nations level, the decision should be also made who (which organizations) should issue such standards and guidelines. Should those be sectorial organizations (e.g. for standards for energy, healthcare, financial sector etc.) or rather ministries covering wider range of applications?

However, the most crucial aspects now for protecting critical infrastructures is the awareness building. Without the understanding and awareness of all the actors (private CI owners, governments, managers, employees at all levels etc.) our critical infrastructures will be still endangered by the cyber and physical attacks.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450. The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

The work is also funded by Polish National Centre for Research and Development (NCBiR) from funds for science in the years 2013–2016 allocated for the international projects.

References

1. Lemos R (2015) Internet of things security check: how 3 smart devices can be dumb about the risks. PCWorld. IDG Consumer
2. Akhgar B, Choraś M, Brewster B, Bosco F, Vermeersch E, Puchalski D, Wells D (2016) Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism. In: Akhgar B, Brewster B (eds) Combatting cybercrime and cyberterrorism—challenges, trends and priorities. Advanced sciences and technologies for security applications. Springer, Switzerland, pp 295–321
3. Stuxnet. http://security.blogs.cnn.com/category/middle-east/iran/stuxnet/

4. Stuxnet computer worm. http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare
5. Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned. http://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266
6. Attack targeting Health Care. http://www.ucdmc.ucdavis.edu/welcome/features/2010-2011/08/20100811_cyberterrorism.html
7. Cyber attack on Health Care institution. http://www.bakersfieldcalifornian.com/local/x534570019/Kern-Medical-Center-battling-virus
8. Financial institutions on high alert for major cyber attack. http://www.computerweekly.com/news/4500272926/Financial-institutions-on-high-alert-for-major-cyber-attack
9. How cyber criminals targeted almost $1bn in Bangladesh Bank heist. http://www.ft.com/cms/s/0/39ec1e84-ec45-11e5-bb79-2303682345c8.html
10. Emerging Cyber Threats Report (2016) Georgia Institute of Technology
11. Choraś M, Kozik R, Churchill A, Yautsiukhin A (2016) Are we doing all the right things to counter cybercrime? In: Akhgar B, Brewster B (eds) Combatting cybercrime and cyberterrorism—challenges, trends and priorities. Advanced sciences and technologies for security applications. Springer, Switzerland, pp 279–294
12. Furnell SM (2001) The problem of categorising cybercrime and cybercriminals. In: 2nd Australian information warfare and security conference 2001
13. Audit Commission (1998) Ghost in the machine: an analysis of IT fraud and abuse. Audit Commission Publications, London
14. Gordon S, Ford R (2006) On the definition and classification of cybercrime. J Comput Virol 2:13–20
15. Report Cyber Crime homepage. Cyber crime classification. http://www.reportcybercrime.com/classification.php
16. Walden I (2007) Computer crimes and computer investigations. Oxford University Press, USA. Wall DS (ed) (2001) Crime and the internet. Routledge, London (ISBN 0415244293)
17. Ngafeeson M (2010) Cybercrime classification: a motivational model. College of Business Administration, The University of Texas-Pan American. 1201 West University
18. Directorate General for Enterprise and Industry European Commission (2009) VITA—Vital infrastructure threats and assurance
19. Luiijf HAM, Nieuwenhuijs AH (2008) Extensible threat taxonomy for critical infrastructures. Int J Crit Infrastruct 4(4):409–417
20. Luiijf HAM (2012) Threat analysis: work package 1.2—expert group on the security and resilience of communication networks and information systems for smart grids, report, 2012
21. Buldyrev SV et al (2010) Catastrophic cascade of failures in interdependent networks. Nature
22. ENISA (2011) New guide on cyber security incident management to support the fight against cyber attacks
23. Threat Risk Modeling. https://www.owasp.org/index.php/Threat_Risk_Modeling
24. CERT. ENISA homepage. http://www.enisa.europa.eu/activities/cert
25. ICS-CERT. http://ics-cert.us-cert.gov/
26. LIMA2 tool. http://www.proceed.itti.com.pl/?p=218&lang=en
27. Ciancamerla E, Minichino M, Palmieri S (2013) Modeling cyber attacks on a critical infrastructure scenario. In: 2013 fourth international conference on information, intelligence, systems and applications (IISA), Piraeus, pp 1–6
28. Haruspex-Simulation-driven Risk Analysis for Complex Systems. http://www.isaca.org/Journal/archives/2012/Volume-3/Pages/Haruspex-Simulation-driven-Risk-Analysis-for-Complex-Systems.aspx
29. Choraś M, Flizikowski A, Kozik R, Renk R, Holubowicz W (2009) Ontology-based reasoning combined with inference engine for SCADA-ICT interdependencies, vulnerabilities and threats analysis. In: Pre-proceedings of 4th international workshop on critical information infrastructures security, CRITIS'09, Bonn, Germany. Fraunhofer IAIS, pp 203–214
30. https://www.isa.org/isa99/

31. http://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection
32. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
33. IEC TR 62210 (2003) Power system control and associated communications—data and communication security. IEC technical report
34. IEC TS 62351 (2007) Power systems management and associated information exchange—data and communications security. IEC technical specification
35. ITIL Incident Management. http://www.bmc.com/guides/itil-incident-management.html