CyberROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D5.2 - Preliminary Best Practices Analysis Document

Date of deliverable: 31 / 05 / 2015
Actual submission date: 31 / 05 / 2015

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.0

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	no
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	✓

Revision history

Version	Object	Date	Author(s)
0.1	Creation	23 Jan 2015	MELANI
0.2	Revision	4 March 2015	MELANI, SM
0.3	Revision	23 April 2013	MELANI, SUPSI
0.4	Revision	4 May 2015	MELANI, SM, SUPSI
0.5	Revision	11 May 2015	NASK, MELANI
0.6	Preliminary review	20 May 2015	SUPSI
0.7	Revision	26 May 2015	NASK, CYBERDEFCON
0.8	Review	28 May 2015	MCAFEE
1.0	Final for submission	30 May 2015	CYBERDEFCON

D5.2 Preliminary Best Practices Analysis Document

Responsible
MELANI

Contributor(s)
INDRA
SM
INOV
NASK
PJ
CEFRIEL
SUPSI
CYBERDEFCON
HMoD

Reviewer
MCAFEE

Summary:

While it is incontestable that 'best practices' represent a way to find practical solutions to a problem, the methodology raises three concerns, which cannot be easily overlooked: it uses the particular to generalise; it is prone to biases to set criteria and their value to compare cases; and alternative hypotheses explaining success are often poorly investigated. On top of this, cyber security best practices are largely understood differently by small-and-medium enterprises, as they are by critical infrastructures. Yet, delving into the latter sector shows the scale and depth of initiatives being undertaken at different national and international levels to define 'best practices' regardless of mentioned methodological problems. Going beyond state-sponsored initiatives, the project also investigated via a survey how cyber security professionals currently implement 'best practices'. It found unsurprisingly that organisations, which perceive cyber attacks as a substantial threat, tend to invest heavily in cyber security solutions; and when they do so, they implement a wide range of solutions across the full range of possibilities. The project concludes by investigating a few possible future developments for the 'best practices' in cyber security.

Keywords: best practices, methodology, critical infrastructure, current and future practices, standards, measurement, metrics, consumer, end user, smart grids,

TABLE OF CONTENTS

'Best practices' is a term, while often branded around, difficult to narrowly define. To some, it may come as a self-evident universal truth, almost as part of common sense. And when this common sense is patently not being applied can come the question: how was this practice left for so long unchanged? A case in point is with a bank fraud happening in late 1978 – probably one of the earliest cases involving computers.

At that time, the Security Pacific National Bank was issuing every day a new code to his bank officers. The bank officers would have to give the code to the wire room in order for their transaction to perform successfully. Mark Rifkin, a then 32-year-old computer consultant, was passing almost every day by the wire room to check on their systems. And during his coming-and-going, he noticed that the clerks in the wire room would merely write the new verification code on notices. On 25 October 1978, he read the daily password while making other operational procedures due for the day. He then exited the building, phoned the wire room pretending to be a bank officer, gave the clerk the correct code, and proceeded to wire $10.3 million.[1] The bank did not even notice the fraudulent transaction before the Federal Bureau of Investigation contacted them to verify their books on suspicions that they had had based on an unrelated large purchase of diamonds.[2] Rifkin was eventually arrested on 6 November 1978, and sentenced on 26 March 1979 to eight years in prison.[3]

It is nowadays common sense that writing a password on a notice is bad practice. Informed by many similar cases, our collective conscience seems to have evolved to the point where we now judge this idiosyncrasy as plainly 'stupid'. But it was not always the case, and this incident fleshes out a few important questions to consider:

How can we define 'best practices'? How do they evolve, and are they really such 'universal' truth? Can we assess what 'best practices' will look like in the future?

To review all 'best practices' in the field of cyber security, is a research project in its own right and beyond the remit of the CyberROAD project. For this body of work the focus is on particular points of interest or concern. The limitations of the report stem mainly from the wide variety of meanings 'best practices' in cyber security can imply. This alone suggests that even an overview of this topic may point to several research gaps in this area.

Operators of industrial control systems, banks or even social media websites all cherish different aspects of security (e.g. the confidentiality of personal information is arguably more important to a bank than to Facebook) and have a different understanding of the terms 'best practice'. A crucial viewpoint, too, should belong to the consumer which is sometimes hidden beneath the need for entities to attain compliance. Best practice, afterall, should be of benefit to end-users, as well as the organisation implementing the process, via a top-down approach which, in terms of cyber security, contributes to the protection of the consumer from products or services that are not fit-for-purpose.

This report is split into five parts. Firstly, it will look at possible ways to approach the term 'best practices'. Secondly, it will show for one specific sector – critical infrastructures – what 'best practices' in cyber security practically speaking means. Thirdly and similarly to the second part, it

[1] Bill Gardner, 'AM cycle', *The Associated Press*, 3 November 1978.
[2] The Washington Post, 'Bank Was Unaware of Swindle', *The Washington Post*, 11 November 1978.
[3] Facts on File World News Digest, 'Rifkin Sentenced in Bank Theft', *Facts on File World News Digest*, 30 March 1979.

will delve into a second specific and practical example of what 'best practices' mean for cyber crime in Poland. Fourthly, based on a conducted survey, the report will delve into what different types of organisations currently apply and regard as 'best practices'. It will notably focus on interpreting what may have influenced the organisations' different choices. Fifthly and lastly, it will conclude by laying down key themes for the next part of this deliverable 'D5.3 Best practices analysis document' where the topics highlighted here will undergo further analysis.

There are plenty of standardisation agencies in the field of (but not only) cyber security, publishing what they brand as 'best practices'.[4] Yet there has been little critical reflection on definitional and methodological issues the term may raise.[5] From a cursory look, it is uncertain if they constitute opinion (even concerted ones), or have a proper scientific value to account for. 'At best, "best practices" are best guesses' as an academic article unrelated to cyber security suggests.[6] If this view is taken as being an accurate reflection, the value of identifying 'best practices' can be close to zero. But the way research is conducted can have important implications as to whether the outcome is only a 'best guess' or is supported by evidences.

Generally conceived, "best practices" aim at improving performance (e.g. the cyber security posture of an organisation) by identifying and codifying factors which have achieved the sought results in another environment. A more formal definition can be put as such: it is 'the selective observation of a set of exemplars across different contexts in order to derive more generalizable principles and theories of management'.[7] Often, documents showcasing 'best practices' are rather in the form of a checklist of points to comply with, and detail what has been implemented and proved to work somewhere else without much thought given to the process of translating case specific conclusions to general theory.[8] But 'best practices' have an undeniable particular appeal, and this is twofold: it provides a practical and seemingly straightforward solution with the implied promise that the solution will apply to many different situations; and it has a rather simple methodology. This simplicity comes however with a set of flaws. The methodology comprehends elements of generalisation and of comparison. And both present their own set of issues.

Before generalising, it is necessary to have a defined and comprehensive set of cases to study. For instance, if a research seeks to investigate the 'best practice' for Swiss banks to protect their computer systems from malware, one has to look at *all* the banks in Switzerland. The outcome of the research would then be applicable only to the elements of the set. Often however, the outcome will be interpreted to imply that the best practice can also work for a case outside the original data set. In the above example, this would mean wrongly applying the solution that worked for a Swiss bank to any bank outside Switzerland. This is a logical fallacy. Universality cannot be derived from empirical observations. One of the reasons beyond logic is that the environment and the social constructs associated with a case are inherent to one case and cannot be simply translated onto another one. Norms regulating the banking industry in Switzerland and in the rest of the world differ, as much as the working culture within organisations, for instance.

Defining what and how to compare represents a second challenge. Defining comparison criteria as well as ascribing a value to the criteria relies on human judgement. And human judgement is biased,

[4] For an extensive list, see: ITU, 'Part 5: Security best practices', http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part05.aspx [1 May 2015].
[5] This is also the case for 'best practices' in other fields, see for instance Stuart Bretschneider, Frederick J. Marc-Aurele Jr., and Jiannan Wu, '"Best Practices" Research: A Methodological Guide for the Perplexed', *Journal of Public Administration Research and Theory* 15, no. 2 (2004).
[6] Alexandra Kalev, Frank Dobbin, and Erin Kelly, 'Best Practices or Best Guesses? Assessing the Efficacy of Corporate Affirmative Action and Diversity Policies', *American Sociological Review* 71, no. August (2006): p.590.
[7] E. Sam Overman and Kathy J. Boyd, 'Best Practice Research and Postbureaucratic Reform', *Journal of Public Administration Research and Theory* 4, no. 1 (1994): p.69.
[8] Arnošt Veselý, 'Theory and Methodology of Best Practice Research: A Critical Review of the Current State', *Central European Journal of Public Policy* 5, no. 2 (2011): p.99.

if not fallible. Judgement is particularly needed when there is an acute lack of information, and when action needs to be taken as a consequence of the judgement.[9] Going back to the example from above, the lack of information is the motive for undertaking the research in the first place, namely that one does not know how to protect the bank's computer system. On the other hand, as a result of the research, the action that will have to be taken is to implement specific measures. But when looking at other banks' implemented solutions, one will invariably fall to biases. Biases are inevitable because human beings' observations form the basis of judgements.[10] Several psychological studies have shown the saliency of expectation biases at the level of individuals and organisations.[11] 'We tend to perceive what we expect to perceive', writes Richard Heuer, an intelligence study scholar.[12]

Further to these two fundamental methodological flaws often comes another avoidable one: the internal validity of the results even within the chosen set.[13] Alternative hypotheses explaining the success of a case need to be thoroughly tested, using yet another methodology than the case study one. Process tracing, a now very popular methodology within the social science, would come handy in many research settings.[14] Process tracing aims at looking at 'the decision process by which various initial conditions are translated into outcomes'.[15] It garners the different variables that may have led to the outcome, considers them as dependent, and then looks carefully for evidence linking the variable to the outcome of the process. Conscientiously fleshing out the process, the variable, and the evidence helps alleviate biases and makes for a more robust and importantly, reproducible analysis. In other words, the research acquires a scientific character.

Similarly, another remedy to the generalisation problem is to understand and explicitly spell out how organisations differ. This does not remove the logical fallacy, but may tame the problem. It is to be noted that 'any "best practice" [research] design will be, by its very nature, less generalizable than standard social science research design'.[16] One of the very reasons is that the method focuses on extremes ('best practices') and not on mean values applicable to most cases.

By following a strict methodological approach, it appears that it is however possible to gain from discerning 'best practices' in cyber security. Specifically to this field, there seems to be a prevailing assumption that an organisation that applies 'best practices' will avoid falling easily prey to attackers, and especially to opportunistic ones. Any organisation can become the victim of a cyber attack. There is nothing much an organisation can do against well-resourced and persistent adversary, such as certain intelligence agencies (e.g. NSA or the Russian FSB) – and even applying any 'best practices' will not help.[17] Incentives for organisations to apply 'best practices' reside more in avoiding

[9] Raymond Geuss, 'What is political judgement?', in *Political Judgement : Essays for John Dunn*, ed. Richard Bourke and Raymond Geuss (Cambridge: Cambridge University Press, 2009), p.40.
[10] Ronald Beiner, *Political Judgement* (Illinois: Univeristy of Chicago Press, 1984), p.148.
[11] See for instance: Peter C. Wason, 'On the Failure to Eliminate Hypotheses in a Conceptual Task', *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960); Richards J. Heuer, 'Limits of Intelligence Analysis', *Orbis* 49, no. 1 (2005).
[12] 'Limits of Intelligence Analysis', p.79.
[13] Bretschneider, Jr., and Wu, '"Best Practices" Research: A Methodological Guide for the Perplexed', p.309.
[14] See for instance Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry* (Princeton, New Jersey: Princeton University Press, 1994).
[15] Timothy J. McKeown and Alexander L. George, 'Case Studies and The- ories of Organizational Decision Making', *Advances in Information Processing in Organizations* 2(1985): p.35.
[16] Bretschneider, Jr., and Wu, '"Best Practices" Research: A Methodological Guide for the Perplexed', p.312.
[17] Bluntly, this is captured by how the FBI director puts it: 'There are two kinds of big companies in the United States: There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese'. Dexter Roberts, 'Chinese Hackers Like a 'Drunk Burglar,' 'Kicking Down the Door,' Says FBI Director', *Bloomberg*, 6 October 2014.

embarrassment by opportunistic hackers, which tend notably to be more vocal about their exploits than state sponsored hackers would. Counter-intuitively, this also implies that organisations, which apply 'best practices' can use them as a way to deflect responsibility when successfully attacked. The underlying text seems to be: 'there is nothing else that we could have done to prevent the attack from happening'.

Another issue inherent to the field of cyber security is what 'best practices' can possibly mean for each sector. For operators of critical infrastructure, applying guidelines for 'best practices' are part of a risk mitigation strategy to avoid the worst-case scenario. Notably, one of the challenges important to them is to bring together the so many different existing standards. For law enforcement agencies on the other hand, 'best practices' are more about enhancing information sharing processes, and meandering through at-times unnecessary lengthy bureaucratic processes. For an intelligence agency like the NSA, 'best practices' in cyber security may rather concern information assurance. Tackling the problem of insider threats may be the priority of 'best practices' – notably after the leak they experienced with Edward Snowden. For instance, only a month after the first Snowden's revelation, the NSA decided to implement a two-person rule to access or move information.[18]

For owners of small-and-medium enterprises, 'best practices' can represent first indications of what to do, if anything at all. A set of such guidelines can look as following: not only technical measures, but also organisational ones should be in place so that it is clear for employees who they have to approach when they receive a mere suspicious looking e-mail; each computer has to have an up-to-date antivirus, firewall, and anti-spam filter; regular backup of the data (preferably not with a cloud solution) needs to be carried out; network activity has to be logged; access rights should be set to the minimum and the network segmented; emails with specific extensions should be automatically filtered out; a password policy should be in place; and lastly, sensitive data should be encrypted.[19]

Although the 'best practices' may well be pertinent for small-and-medium enterprises, they may not be of much value to experts working in protecting the systems of an intelligence agency, or of critical infrastructure. This research report focuses on the latter to offer an in-depth example of what 'best practices' can look like, and how they are actor-centred.

[18] AP, 'Officials say new anti-leak measures set at NSA', *CBS News*, 18 July 2013.
[19] MELANI and GovCERT, 'Sécurité informatique: aide-mémoire pour les PME [IT security: a help for SMEs]',(Bern: MELANI, 2015).

Control and monitoring systems are essential operational processes used in today's critical infrastructures such as electricity generation plants, transportation systems, and manufacturing facilities. The generic term, Industrial control systems (ICS), includes many different control and monitoring systems, including SCADA (Supervisory Control and Data Acquisition), programmable logic controllers (PLC), Distributed Control Systems (DCS) and embedded control systems that eliminate or reduce the need for human interaction.

It is common practice today for IDCs to make use of standard embedded system platforms, often commercial off-the shelf software which helps reduce cost and promotes ease of use but, at the same time, introduces additional risk from computer network-based attacks on inherent vulnerabilities found in standardised systems.

The potential for significant disruption to critical infrastructures and services from cyber attacks was highlighted after deliberate attempts to infiltrate these systems. Successful intrusion could lead to untold consequences in the public arena as well as for national security.

As a result of bringing this subject to widespread attention, cyber security experts, governments, academics, critical infrastructure operators and other interested parties have formed working groups and iniatives to research into associated issues. ENISA (European Union Agency for Network and Information Security) is proactive in this area supporting research via a survey that investigates industrial control systems security-related working groups, standard bodies and initiatives.[20] This study provides useful information on standards and guidelines aimed at protecting critical infrastructures in different countries.

The working groups identified by the survey are summarised below in *Table 1*. The information provided here suggests that the European Union may be lacking in leadership regarding the creation and implementation of standards and guidelines. The US and international bodies appear to be further advanced in this area.[21] As a result European companies are tending to gravitate towards international standards for guidance and direction. This observation is of importance for deliverable and should be a topic for further investigation.

[20] ENISA, 'ICS Security Related Working Groups, Standards and Initiatives',(Heraklion: ENISA, 2013).
[21] 'Protecting Industrial Control Systems - Recommendations for Europe and Member States',(Heraklion: ENISA, 2011).

.

	Name	Acronym
International Working Groups	UCA International Users Group	UCAIUG
	Department of Energy	DOE
	ISA and ISA99 committee	ISA and ISA99
	National Institute for Standards and Technology	NIST
	NIST Smart Grid Interoperability Panel & Cyber Security Working Group	SGIP/CSWG
	Smart Grid Testing & Certification Committee	SGTCC WG
	Critical Infrastructure Security Working Group	CISSWG
	DETER Enabled Federated Testbeds consortium	DEFT
	Information Trust Institute	ITI
	ISA Security Compliance Institute	ISCI
	Anerican Gas Association Task Group	AGA 12
European Working Groups	Deutsches Institut für Normung	DIN

Table 1: ICS Security Related Working Groups

3.1 INITIATIVES FOR CRITICAL INFRASTRUCTURE PROTECTION

Improving critical infrastructure protection and resilience is of outmost importance in order to be able to withstand potential emerging cyber threat scenarios. A sample set of initiatives are analysed in this section to give an overview of the current landscape.

The European Programme for Critical Infrastructure Protection is a specific European program that aims at identifying and protecting the critical infrastructures of the European member states. The Programme defines the main activities that are necessary to maintain a safe environment for each of the EU States and across all relevant sectors of economic activity.

One of the main goals is identified as the need to improve protection from major threats such as cyber terrorism which, in itself, is difficult to define.[22] In 2012, a review of the first version of the Programme took place, and analysed the extent to which the program has been adopted.[23] Based on

[22] European Commission, 'European Programme for Critical Infrastructure Protection',(Brussels: European Commission, 2006).
[23] 'Review of the European Programme for Critical Infrastructure] Protection (EPCIP)',(Brussels: European Commission, 2012).

the results of this review the Commission approved and adopted a new approach, which sets a more practical implementation of the first version of the programme.[24] In this new approach the interdependencies between critical infrastructures, industry, and state actors is observed. When a single critical infrastructure becomes the target for attack the impact on a wide range of actors in a number of diverse infrastructures can be considerable. Another outcome of the review was finding that there was a lack of attention to, and understanding of, the connections between critical infrastructures and different sectors, which may extend across national boundaries. In order to appropriate protect the European critical infrastructures, and enhance their resilience, this mismatch needs to be tackled. This is a finding that indicates a gap where improved practices guided through a best practices scenario may be of benefit and is a topic of note for this deliverable.

Figure 1 shows how different sectors in the critical infrastructure industry depend on each other. For example, the electric power (or power grids) infrastructure is central to numerous other sectors including telecommunication, water, natural gas, oil, etc.

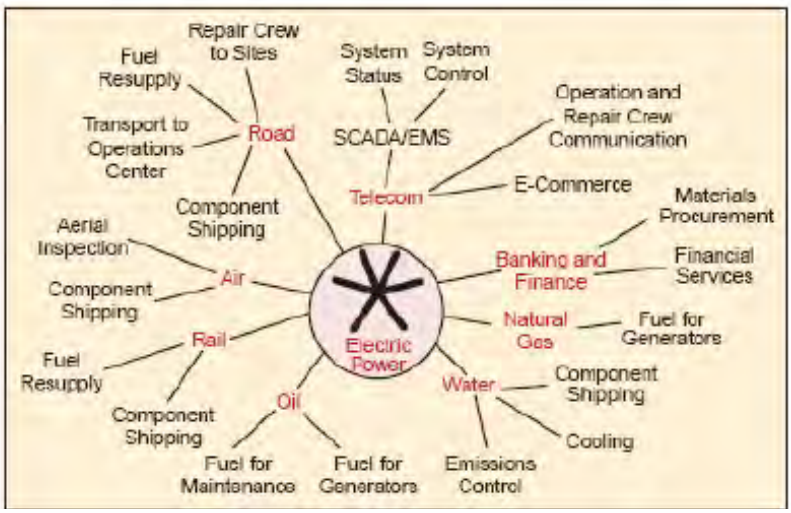

Figure 1: Interdependence between different critical infrastructures[25]

On March 30 2009, the European Commission also adopted a Communication on critical information infrastructure protection with the aim of intorducing a plan that would involve both the private and the public sector.[26] The plan proposes five categories of support: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for European Critical Infrastructures in the field of information and communication technology. The plan was revisited in 2011 when the Commission concluded that there was insufficient support at a pure national level and that a joint effort across the European Union was needed. The requirement was for a system that integrated cooperation between member states which would enhance the

[24] 'A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure',(Brussels: European Commission, 2013).
[25] Ibid.
[26] 'Protecting Europe from large scale cyber-attacks and] disruptions: enhancing preparedness, security and resilience (COM(2009) 149 final)',(Brussels: European Commission, 2009).

resilience and security of information systems and networks and improve the level of protection from all manner of disruptions, deliberate or accidental..[27]

These considerations led to the establishment of the European Union Agency for Network and Information Security (ENISA) *Critical Information Infrastructure Protection (CIIP) and Resilience Unit*. The main goals of this unit are to:

- Collaborate with the EU to enhance understanding of the threat landscape that networks such as Smart Grids and ICS-SCADA have to face;
- Develop good practices in the area of cyber security strategies and national cyber exercise;
- Offer training and seminars to individual member European Union States on areas of its expertise such as national exercises, contingency plans, incident reporting;
- Aid National Telecom Regulatory Authorities in the implemention of a coordinated exercise in mandatory incident reporting;
- Co-manage with the Commission for the Pan European Public Private Partnership for Resilience (EP3R) to imrpove fragmentation of the public and private stakeholders on emerging critical information infrastructure protection issues.

An important influence in this programme is the 2008 Directive on European Critical Infrastructures.[28] The aim of the program is to establish a standard approach towards determining if there is a need for better protection of European Critical Infrastructures. Directive 2008/114/EC9 applies specifically to the energy and transport sectors and urges member states to pinpoint which critical infrastructures may be at risk. As at 28 August 2013 fewer than 20 had been designated which is most likely not a comprehensive assessment when considering the number of European critical infrastructures that exist. The conclusion of the analysis is that a number of very critical infrastructures, including main energy transmission networks, that have not been included.

The Smart Grid Coordination Group (SG-CG), formed by three European organization: CEN (a major provider of European Standards and technical specifications), CENELEC (the European Committee for Electrotechnical Standardization) and ETSI (the European Telecommunications Standards Institute) [29], is another important initiative that co-produced a report on standardisation across the smart grid industry.

This working group formed as a result of the Smart Grid Mandate M/490 issued by the European Commission and European Free Trade Association.[30]. This mandate remit is to recommend a framework for standard enhancement in the smart grid sector be developed that outlines the European picture within the context of global activities[31]. The brief extends from generators to households appliances which covers a wide range apparatus and devices and, as a consequence, the

[27] 'Policy on Critical Information Infrastructure Protection (CIIP)',(Brussels: European Commission, 2013).
[28] 'Directive on European Critical Infrastructures 2008/114/EC',(Brussels: European Commission, 2008).
[29] SmartGrids, 'CEN / CENELEC / ETSI: Smart grids and standardization', http://www.smartgrids.eu/CEN-CENELEC-ETSI [1 May 2015].
[30] European Commission and European Free Trade Association, 'M/490 EN - Smart Grid] Mandate - Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment',(Brussels: EC, EFTA, 2011).
[31] CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)',(2014).

standards required would also be diverse. For this reason the bodies involved in the working group come range a range of industry types.

The working group has made some interesting observations, such as:

- A report highlighting existing standards and verifying if, and how, European standardization fit the requirements for smart grids.[32] The report provides a selection guide for Smart Grid systems for consideration of the most relevant existing and upcoming standards, from CEN, CENELEC, ETSI and further from IEC, ISO, ITU and including, as well, other bodies when needed. The report also outlines how, and when, these standards can be used.[33]
- The Smart Grid Architecture Model (SGAM), a reference model to analyse and visualize smart grid use cases in respect to interoperability, domains and zones.[34]
- The SGIS - Security Levels (SGIS-SL), a framework to bridge the divide between electrical grid operations and information security for the purpose of enhancing the grid resiliency and for guidance on Smart Grid information security.[35]

The work carried out by the working group only focuses on smart grids. This is a notable research gap as a similar level of ananlysis and detail is lacking for other kind of critical infrastructures (e.g. communication, oil and gas, water).

By comparison, initiatives in critical infrastructure protection in the United States are part of a nationwide program to ensure uniformity of security for vulnerable and interconnected infrastructures. The Homeland Security Presidential Directive HSPD-7 for Critical Infrastructure Identification[36] was first introduced by President Bill Clinton in May 1998 and was updated by President Bush in December 2003. Specific parts of the national infrastructure were identified as critical to national and economic security and, additionally, to the well-being of US citizens.

Directive HSPD-7 lists the various steps that are necessary to secure the infrastructures identified that have been defined, "...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety'.[37]

In the same directive, the US establishes a national policy that enhances the security and protection of US critical infrastructures and the identified key resources against terrorist acts. Additionally, in the Presidential Policy Directive/PPD-21 the importance of protection from cyber threats is explicitly stated.[38]

[32] CEN/CENELEC/ETSI Joint Working Group, 'Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids',(2011).
[33] CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)'.
[34] 'Smart Grid Reference Architecture',(2012).
[35] 'Smart Grid Information Security',(2012).
[36] White House, 'Homeland Security Presidential Directive/HSPD-7', 17 December 2003.
[37] Ibid.
[38] 'Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience', 2013.

3.2 *STANDARDS AND 'BEST PRACTICES' FOR CRITICAL INFRASTRUCTURE*

Critical infrastructure vulnerability reduction and enhanced resilience to cyber attack is a major, but complex, goal for the European Union. Securing industrial systems is in the interest of organisations and citizens alike, both for EU member states and further afield. This is not an easy challenge for standardisation bodies as new cyber threats constantly tax established procedures and processes.

Innovative solutions are needed to protect industrial networks operting utility networks. Interesting approaches are those that combine the 'best practices' in security management and the methods of governance of enterprise IT infrastructure. Although most of the current IT security policies and methodological frameworks have been designed to prevent and protect the Internet, a few steps ahead have been done in the last ten years towards the development of security techniques and standards that are specific for critical infrastructure networks.

In the United States, for example, the North American Electric Reliability Corporation is developing a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management.

In the European Union, there are several initiative for the protection of critical infrastructure, as has been mentioned in the above sections. Additionally, the Cyber Atlantic 2011 exercise is an initiative of note.[39] This took place in Brussels, and tested the responses to cyber incidents and cyber-attacks. The exercise was based on the hypothetical scenarios of SCADA system failure in a European wind turbine.

ENISA provides another example of an interesting activity promoting best practices in critical infrastructure through its recommendations for the Europe and member states concerning the protection of industrial control system.[40] As well, ENISA published a report with an in-depth analysis of existing standards, regulation and guidelines for critical infrastructure protection.[41] The study points out how the energy sector (including oil, gas and electricity subsectors) has the largest number of specific guidelines, standards and regulatory documents. On the other side, sectors like transportation and water supply or agriculture lack this information (the Annex A also contains a summary of the most important standards for security recommendation for industrial control system).[42]

[39] ENISA, 'Cyber Atlantic 2011', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 [1 May 2015].

[40] 'Protecting Industrial Control Systems. Recommendations for Europe and Member States',(Heraklion: ENISA, 2011).

[41] 'Protecting Industrial Control Systems - Recommendations for Europe and Member States'; 'Protecting Industrial Control Systems - Annex IV. ICS Security Related Initiatives',(Heraklion: ENISA, 2011).

[42] For a more extensive list please refer to: CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)'; E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (Waltham: Elsevier, 2014); IEC TC57 WG15, 'List of Cybersecurityfor Smart Grid Standards and Guidelines', http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf [4 March 2015].

Another example of a specific approach to 'best practices' for cyber security is on the topic of cyber crime, and especially by Poland. There are few technical or academic Polish articles that deal with the subject. The academic papers written in Polish or by Polish authors that exist on the topic tend to focus on the relevant laws that can be applied to cases that involve cyber crime. They do not however provide any context or analysis of actual cases that have been handled and constraints faced.[43] Non-security vendor driven research on the other hand tends to focus on compliance with EU regulation, usually in the broader cyber security context (a list of such research is presented below).

Foreign – and often vendor driven - research tends to focus on technical observations (for example, malware infection levels in the Microsoft Security Intelligence Report) or makes assumptions about the cost of cybercrime in a specific given country.[44] Especially in the latter case, it is very unclear how accurate this is, and an issue that does not only apply to Poland.[45]

4.1 CERT STATISTICS

CERT Polska - operating as part of the NASK Institute (Naukowa i Akademicka Sieć Komputerowa, a CyberROAD project partner) provides a broad number of security statistics based on actual observation of security incidents in Poland in its annual 2014 report.[46] For instance it estimated that on an average day in 2014, there were 280,000 computers infected with malicious bots. Over 50,000 of these were infected with a type of a banking Trojan written to facilitate financial fraud. As part of its mission, CERT Polska regularly publishes information on specific mechanisms of cybercrime, including statistics regarding malware on Polish networks, malicious URLs, phishing, spam, distributed denial-of-service attacks and their associated and command & control servers.[47] Other similar reports – specifically focused on government administration in Poland – are published by the Polish Internal Security Agency (ABW), which operates the CERT.GOV.PL.[48] Other Polish entities exits that publish cybercrime related statistics but from an Internet safety aspect (such as child safety online, child pornography and hate material).[49]

4.2 POLICE & GOVERNMENT STATISTICS

The Polish Police does not provide detailed statistics relating to cybercrime in their public reports.[50] More information can be gleaned from the MSW (Ministry of the Interior) reports that include

[43] Nicolaus Copernicus University, 'Cybercrime Research Centre: Publications', http://www.cybercrime.umk.pl/publications,7,en.html [12 May 2015].
[44] Microsoft, 'Microsoft Security Intelligence Report ', http://www.microsoft.com/sir [12 May 2015]; Norton, 'Norton Cybercrime Report 2012', http://us.norton.com/cybercrimereport [12 May 2015].
[45] Andy Greenberg, 'McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim', *Forbes*, 3 August 2012.
[46] NASK, 'Cert Polska: Rapport 2014',(Warszawa: CERT Polska, NASK, 2014).
[47] See for a full list of publications: 'Papers', http://www.cert.pl/raporty/langswitch_lang/en [12 May 2015].
[48] CERT.GOV.PL, 'Publikacje', http://www.cert.gov.pl/cer/publikacje [12 May 2015].
[49] Polish Safer Internet Centre, 'saferinternet.pl: Keeping children and young people safe online', http://www.saferinternet.pl/en/ [12 May 2015]; Dyzurnet.pl, 'Dyzurnet', http://www.dyzurnet.pl [12 May 2015]; Fundacja Dzieci Niczyje, 'The Nobody's Children Foundation', [12 May 2015].
[50] Policja, 'Statystyka', http://www.statystyka.policja.pl/ [12 May 2015].

general statistics in terms of the amount of cases and (selected) laws applied.[51] This also includes data from other parties, such as the Ministry of Justice.

The Polish Ministry of the Interior Report lists 19 articles of the penal code that specifically concern cyber crime and attacks against computer systems, and lists another 19 that can also be committed in cyberspace. It also enumerates 11 different crimes understood as cybercrime:

1. Online fraud
2. Phishing and other financial crime
3. Paedophilia and child pornography
4. Copyright and intellectual property infringement
5. Trading in unlicensed or illegal goods
6. Human and human organ trafficking
7. Illicit trade in excise goods
8. Trade of artefacts coming from crime and illegal trade of goods of national heritage
9. Extortion or threats by organized crime
10. Hacking, sniffing, breaking into systems and malware
11. Illegal gambling online

The report also summarises police statistics regarding specific violations of articles of the penal code. However, apart from the fact that there is an increase in these selected violations, numbers are difficult to make sense of. It is not always clear if the statistic really concerns cyber crime, as it is not mandatory to specify whether a crime was committed on a computer network or the Internet when reporting it. For those that clearly fall within cyber crime, the larger numbers of offenses were 'computer fraud' (26,945 cases) and 'paedophilia and child pornography' (1,648 cases). In terms of cyber crime cases that actually ended up in court, the numbers are much smaller. The top two categories concerned the destruction or damage of computer data (57 persons tried, 47 sentenced) and 'computer fraud' (33 persons tried, 18 sentenced). The only two other categories in the report 'interference in the functioning of computers or networks' and 'production, acquisition, selling, sharing, devices or computer programs to commit crimes' were at 9 (5) and 6 (4) respectively.

As part of the CyberROAD, Cert Poland submitted two requests for public information. One request was sent to the Polish police, and another one to the Ministry of Justice. The request asked the police for the number of initiated investigations concerning crimes against information security and other crimes committed with the use of Internet, as well as numbers of cases where investigations were discontinued and reasons for the decision. The results showed that an overwhelming majority of investigations is discontinued due to an impossibility of establishing the perpetrator. Most crimes against information security are related to unauthorised access to information (Art. 267 of Polish Penal Code, which unfortunately does not differentiate between physical and electronic access). Other crimes in which the Internet was used are mostly frauds, in particular during online transactions. These findings are in line with statistics of the Ministry of Justice. Only one in about fifty crimes identified by the police resulted in a final conviction, with an average sentence of less than 9 months (using the same Art. 267 as an example).

[51] Ministerstwo Spraw Wewnetrznych, 'Raport MSW o stanie bezpieczeństwa [Polish Ministry of the Interior reports on security in Poland]', [12 May 2015].

4.3 *NATIONAL CYBERSECURITY STRATEGY WITH REGARDS TO CYBERCRIME*

Two major documents exist in regards to Poland's approach to cyber security. The first document is the "Cybersecurity Doctrine of the Republic of Poland 2015" (currently only available in Polish).[52] While the document is broad in terms of discussing different cyber security issues, it essentially glosses over the topic of cybercrime, referencing it only twice and mentioning that it should be addressed, failing to mention the role of the police in doing so. The second document, the 'Cyberspace Protection Policy', introduces the concept of cyber crime, even provides a definition as 'an offence committed in cyberspace', but fails to elaborate on the topic.[53]

It should be noted that none of these documents are legally binding. It is expected that official legal acts in this area will be implemented once a directive from the European Union called the 'Network and Information Security' is established. Globally, it can be said that Poland currently lacks a comprehensive programme in com

4.4 *A COMPARISON OF STATISTICS*

Reports in the statistics published by different parties signal a large disparity between the number of observed security incidents (including cybercrime) by CERT Polska and government statics regarding cyber crime cases. Based on the surveys carried out in the CyberROAD project (more in the next section), it would appear that most cases are simply not reported to the police. Subsequent police investigations into cases appear not to be very effective, with only few going to court. The situation is best summed up in the words of Jerzy Kosinski, a researcher at a Polish police school:

> "It can be said, that computer piracy has become one of a few areas of computer crime where the police are effective."[54]

This may be because the affected companies are determined to fight with this problem, and have the resources to hire law firms and push cases. The conference paper also makes another point in the paper worth noting:

> Computer frauds such as interfering with input data, program or output are often a black number. Afraid of having their reputation undermined, banks, offices and companies often fail to inform the police and the public about them.[55]

The Eurobarometer survey conducted in October 2014 on cyber security highlights another aspect of the problem:

> Whilst the value of the cybercriminal economy as a whole is not precisely known, the losses are thought to represent billions of euros per year. The scale of the problem is itself a threat to law

[52] Biuro Bezpieczeństwa Narodowego [National Security Bureau], 'Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej [Cybersecurity Doctrine of the Republic of Poland]',(Warszawa: BBN, 2015).

[53] Internal Security Agency Ministry of Administration and Digitisation, 'Cyberspace Protection Policy of the Republic of Poland',(Warsaw: MAIC, 2013).

[54] Jerzy Kosinki, 'Cybercrime in Poland 2011-2012', in *International Scientific Conference Archibald Reiss Days III*(Belgrade2015), p.1.

[55] Ibid., p.2.

enforcement response capability – with more than 150,000 viruses and other types of malicious code in circulation and a million people victims of cybercrime every day.[56]

4.5 *THE CYBERROAD SURVEY*

As part of the CyberROAD project, the project consortium decided to carry out a three-step survey into cybercrime to get a better understanding of the phenomenon and end user perceptions.[57] This survey was aimed at respondents from the entire world with an English language version and specifically at Poland with a Polish language version. The consortium members decided to pick Poland as a specific example country to compare with others. Poland was selected because it is one of the larger EU countries and is also represented by a national CERT team (CERT Polska) in the CyberROAD consortium. The initial results of the first survey are summarised below with an attempt to highlight the main differences between Polish and English speaking respondents (data based on responses collected until May 11, 2015):

- Polish respondents stated that cybercrime was a lesser concern for their organisation compared to the English language respondents (39.2% of the respondents said that cybercrime was only a slight concern or none at all while this represented 16% of the respondents of the English survey). This is despite that fact that individually, respondent concern was at similar, if not slightly higher levels.
- Security training levels of respondents were slightly lower than the English language survey respondents, with 73.1% of respondents receiving no training or only after a problem is identified in comparison to 63,2% for the English survey.[58]
- Education was pointed out as the main area of improvement (74.6% of respondents with a similar number of English survey respondents, 72.3%, stated that it was a 'very important' element to improve).

Also notable was that there was:

- A higher percentage of Polish respondents had experience cyber crime in the last 5 years in a personal capacity (43% vs. for 26.7% English language survey respondents).
- A low impact of cyber crime for Polish respondents as victims: 'inconvenience' or 'no effect' of cyber crime obtained the most responses (41% and 42.6% respectively). The English survey responses were 46.8% and 33.3% respectively.
- A low reporting rate of cybercrime cases to the Police (31%), similar to the English survey responses (30.4).
- A low successful Police action and prosecution rate (5.3%), similar to the English survey responses (7.2%).
- Low reporting rates to CERTs - similar to English survey respondents (not reported by 84.4% of Polish survey respondents and by 80.3% English survey responses).

[56] European Commission, 'Special Eurobarometer 423: Cyber Security',(Brussels: European Commission, 2015), p.2.
[57] CERT.PL, 'CyberROAD Invitation to participate in the project survey', http://www.cert.pl/news/9671/langswitch_lang/en [12 May 2015].
[58] A 'Don't know' as a de facto no training answer was included here as well

- A low tendency to share information on attacks with other organizations – lower than that of respondents of the English language survey (21.1% vs 35.4%)

It is of note that Polish survey respondents tended to come from a younger group, more consumer oriented or involved in a commercial business than their English language counterparts who included more academics and security specialists.

4.6 THE EUROBAROMETER SURVEY ON CYBER SECURITY

The aforementioned Eurobarometer survey on Cyber Security for the European Commission gives much insight into perceptions and experiences of EU citizen with cyber crime. It is also very useful in providing a more in-depth comparison of Poland versus the rest of Europe.

- The most basic conclusion is that the average Pole is not very concerned with cyber crime. Responses to concerns regarding online banking payments were the second lowest in Poland out of all the EU countries surveyed (29% of respondents) and lowest when it came to potential misuse of personal data (25% of respondents).
- Polish respondents were least likely to say that they have changed the way they use the Internet due to security concerns.
- Polish respondents were among the least likely to say that they have installed anti-virus software (only 43%), least concerned about opening emails from people they do not know (29%), least regularly changing their passwords (14%) and one of the least likely to use different passwords for different sites (17%) or to change settings (8%).
- Despite these not very positive statistics, there was a general improvement of security issues, at least declared by the respondents, up 21% compared to a similar study in 2011.

In terms of cybercrime concerns, there are also some different perceptions compared to other EU countries:

- Poland declared one of the highest concerns of online fraud.[59]
- Encounters with online child pornography was the second highest in the EU, concerns with hatred materials were also above average.
- Denial of access to services is an area of concern for respondents, but not experienced by most.
- Personal data security concerns (having their e-mail account or social account hacked) was an area of lower concern and personal experience than in most other EU countries.
- Banking fraud, was slightly less personally experienced by Polish respondents compared to the EU average, as well as slightly less an area of concern.

The authors of the survey made an interesting observation: 'the survey findings suggest that a greater knowledge of cybercrime leads to a preference to contact organisations such as the website or vendor rather than the police'.[60] Polish respondents often quoted the Police as appropriate contact

[59] Defined as 'goods purchased were not delivered, counterfeit or not as advertised'

[60] European Commission, 'Special Eurobarometer 423: Cyber Security', p.94.

for cyber security issues, although compared to police statistics, it appears that there is little reporting actually carried out. On the other hand, a PwC Crime Survey 2014 study noted a drop in cyber crime as a problem for survey respondents from 24% in 2011 to 19% in 2014.[61] This is below worldwide average (24%), and also contrary to CERT Polska reports and statistics.

4.7 BSA REPORT ON LEGISLATION

In comparison once more with another survey, a recent 'EU Cybersecurity Dashboard' study by a software non-commercial group called BSA released in March 2015 provides an overview of the cyber security landscape in Europe. The survey takes a legal and policy perspective, covers particularly aspects such as: legal foundations for cyber security, operational capabilities, public-partner partnerships, sector-specific cyber security plans and education.[62] Poland was found to have a 'comprehensive cybersecurity strategy with clear goals' but many were viewed as not yet implemented, and the legal cyber security framework not fully developed.

A few missing elements to the current framework, according to the BSA studies, included that:

- There is no legislation or policy in place in Poland that requires the establishment of a written information security plan.
- There is no legislation or policy in place in Poland that requires an annual cyber security audit.
- There is no legislation or policy in place in Poland that requires an annual cyber security audit.
- There is no legislation or policy in place in Poland that requires each agency to have a chief information officer or chief security officer.
- There is no defined public-private partnership for cyber security in Poland.
- There are no new public-private partnerships being planned in Poland.
- Poland does not have sector-specific joint public-private plans in place.
- Sector-specific security priorities have not been defined.
- Sector-specific risk assessments have not been released.

4.8 OBSERVED GAPS

In terms of the overall conclusions regarding cybercrime in Poland, the following gaps have been observed as part of this study:

- There are sufficient cyber crime penal laws in place, but there appears to be a lack of adequate enforcement. Even if cases are reported, most do not lead to prosecution or sentencing.

---

[61] PwC, 'Economic Crime Survey Poland 2014',(Warsaw: PwC, 2014), p.6.

[62] BSA, 'Country: Poland',(BSA, 2014).

- Reporting rates of cyber crime incidents to authorities appear to be low. Most Polish users report cyber crime effects as a mere 'inconvenience', which may also result in the relative absence of Police reports.
- There is no national plan to tackle cybercrime. Existing documents that attempt to establish cyber security policies at the national level do not devote sufficient attention to the problem or recognise the complexity of the problem.
- There is a lack of good statistics and metrics to measure cyber crime levels and costs resulting from cybercrime - a problem that applies not only to Poland but also almost everywhere else. There is a need to move beyond the technical observations of the tools used to commit the crime (like malware or malicious pages) in order to focus more on cyber crime itself.
- There is no established link between cases reported to the Police, successful prosecution in court and technical measurements and statistics from CERT reports.

Work on exploring these gaps and looking for possible solutions will be the subject of further research under the CyberROAD Project.

Critical infrastructures and cyber crime are only one part of how 'best practices' for cyber security are being considered by various international agencies and national governments. As the initial research question did not focus on any specific industry for cyber security, there was an interest in trying to obtain a broader picture. As part of the CyberRoad WP5.1, a survey was designed and made available on the CyberROAD website with the target being professionals working in the field of cyber security and other interested parties. The survey was offered to participants worldwide but with a specific focus towards Europe to gain a macro viewpoint. The survey was also translated in Polish to garner a micro perspective. Poland was chosen as the survey could be pushed via CERT (Computer Emergency Response Team) Polska, a participant of the CyberROAD project.

Several questions within the survey pertained to 'best practices', the theme of WP5.2. The survey would provide a snapshot of the current best practices landscape, through assessment of the practices companies are applying. The survey included questions pertaining to personal and organisational cyber security practices as well; only the organisational ones have been taken into consideration here. By looking at specific correlations, it is possible to extract interesting information.

The number of respondents obtained was N=679, and the survey questions can be consulted in Annex B. Correlations values and p-values were computed using the 'Data Analysis Tool Pack' from Excel. More specifically, the p-values are computed following a two-tail Student t-distribution. Only p-values inferior to 0.05 have been considered. The significant correlations, which made sense regarding the context of the research questions, are presented below. Note, however, that some of the correlations were rather problematic and did not provide definitive outcomes.

The survey shows that respondents who have risk management policies also have policies about Bring-Your-Own-Devices (BYOD) best practices. As the latter is often comprised within the former, such a result is not very surprising. Similarly, having risk management policies and having certifications in information security management also showed correlation – again, the two being in any case often associated with one another. Having a risk management policy also strongly correlated on the one hand with concerns respondents had about cybercrime, and on the other hand, with how often the organisation decided to give its staff training about cyber security risk.

In turn, organisations, which often give security trainings, also have best practices policies for BYOD. But giving security training is not a best practice for cyber security that comes on its own. Noteworthy, those who give regular security trainings to their employees also have in place a range of other security measures: they use firewalls, antivirus software, share information about cyber attacks with other organisations, and some of their staff hold information security management certificates. Participation in security trainings is also strongly correlated with the perception of high costs of cybercrime to the local and the global economy.

These points make intuitively sense, and the survey comes as evidence to support them. The conclusions of the many correlations can be summarised with two arguments. Firstly, the more an entity perceives cyber crime as being a salient problem to be wary of, the more it will invest in solutions to tackle the problem. Training is one of these solutions. But the correlation between spending on cyber security and perception of cyber crime also comes up in other places. For instance, the more prominent companies are concerned about cybercrime in their country or even in

the world, the more they are allocating financial resources for it. The second takeaway is that companies, which apply at least one security measure, have a strong tendency to apply many others. There are therefore noticeable cross-correlations between having in place the followings: firewalls, antivirus, spam blockers, secure email gateways, data encryption, and back-up systems.

The analysis of the survey data does not hence show ground-breaking or unexpected results. In parts it confirms some pre-conceived assumptions. It is as well very plausible that many of the professionals who took the survey share the same pre-conceived assumptions, which influenced how they answered the questions. As already mentioned in the methodological section, biases come along with any experiment involving human observations and cannot be removed. It would be interesting to compare the results of the survey against another population, this time constituted of fewer cyber security professionals.

Lastly, the aforementioned correlations are shown more comprehensively below. Most interesting correlations can be shown with two disconnected graphs. The number above the vertices are the absolute correlation values, and the p-values are all within the confidence interval ($p<0.05$).

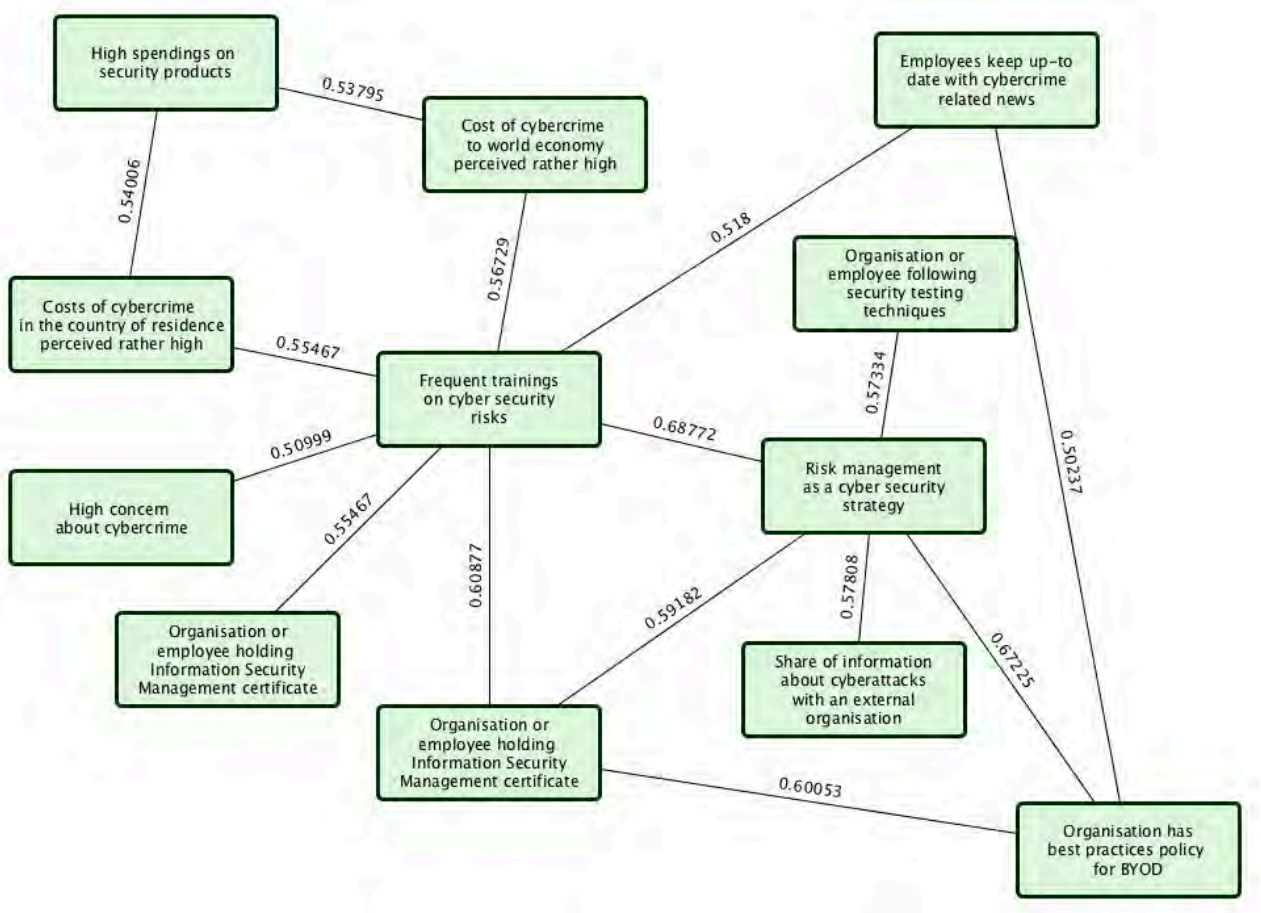

Figure 2 Relevant correlations from the survey (1/2)

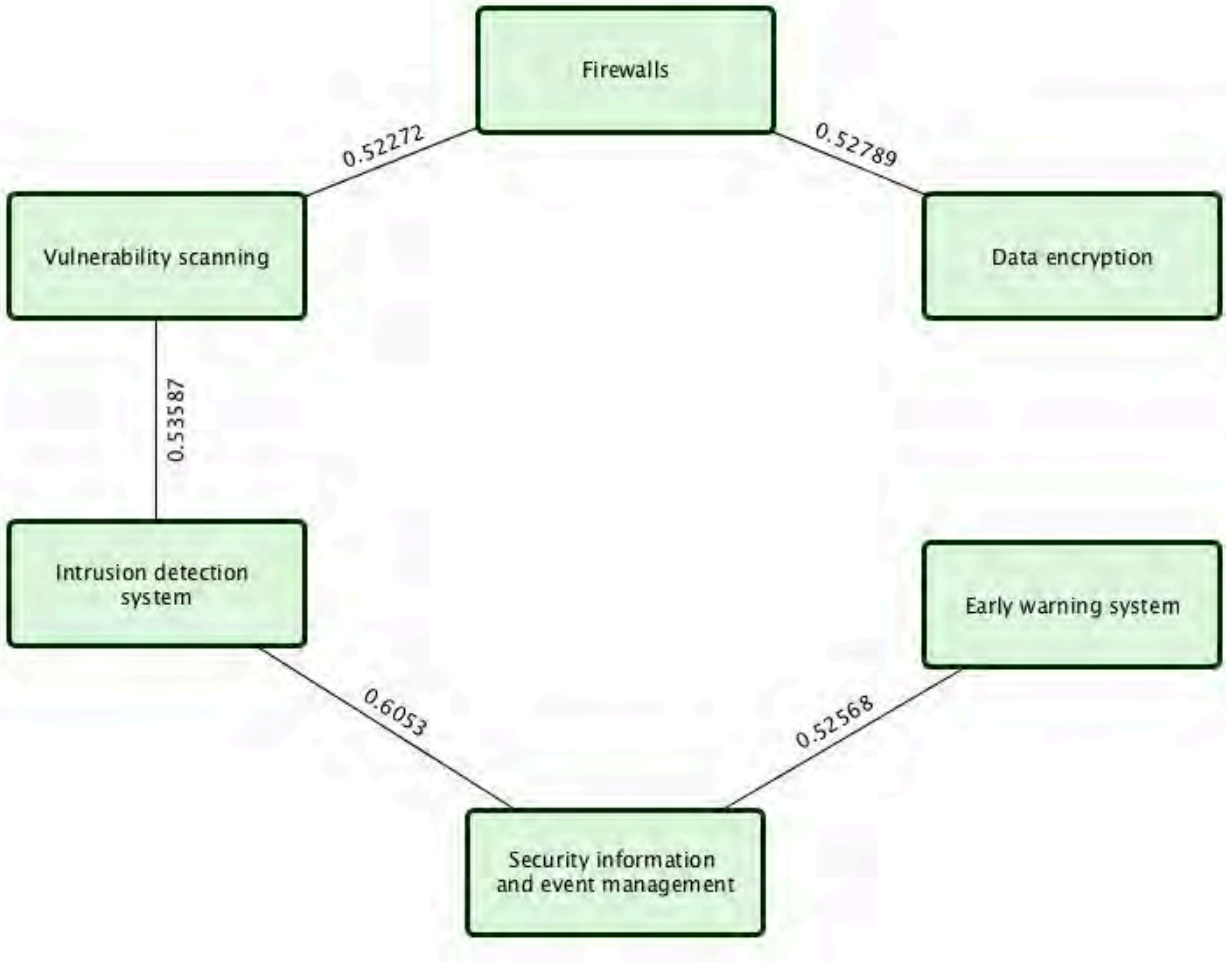

Figure 3 Relevant correlations from the survey (2/2)

Predicting the future is not only often fraught with failure, but also lacks scientific and academic basis to do so. Yet it is a predominant question of interest for policy makers to know where to expect future threats and to direct accordingly the state security apparatus. It is similarly of interest to many companies' executives looking ahead at the risks they may soon face and at how they can adapt their strategies to best tackle them. This interest explains the recurrence of the theme and its own importance for cyber security.

At least two schools of thoughts almost opposite to each other exist on the topic. On the one hand, one school holds that it is possible for certain people to garner enough knowledge to be able to make certain predictions correctly. More precisely, the psychology researcher Philip Tetlock advances the two-pronged empirically tested argument that: "how you think matters more than what you think"; this in turn implying that generalists fare better at predictions than experts. The type of knowledge to acquire would hence rather have to be broad than in-depth.[63] On the other hand, the much-publicised 'theory of the Black Swan' holds that the most impactful events in our society are outliers and cannot be predicted.[64] This holds true for 9/11, the success of Harry Potter, or the invention of Google and Facebook.

With this in mind, a middle ground would have to be considered, while staying very modest: What would best practices look like in the near future? What will be the questions to arise in the near future?

Tetlock's theory, and even less so with the 'Black Swan' one, does not lend a very workable methodology to approach these questions. But Google's chief economist, Hal Varian, puts forward an elegant solution. According to him, 'to predict the future, we just have to look at what rich people already have and assume that the middle classes will have it in five years and poor people will have it in 10'.[65] Applying this rule, which best practices can the richest companies of the moment afford that others cannot?

Firstly, there are the concerns within the field of intelligence. With good intelligence on cyber threats, companies are able to know what they need to focus on to prevent adversaries getting into their network. Acquiring intelligence feeds does not come cheap, and especially if one wants to acquire very specific intelligence about sophisticated and persistent threat actors. An intelligence feed from one provider can cost in the hundreds of thousands of dollars yearly. Regarding that each provider can have an area of specialisation with specific sensors in a part of the world able to catch interesting pieces of malware, a well-off company is able to acquire several of them and have a very specific picture of the threats.

This leads to the second point. Intelligence feeds represent only one source of information. Ideally, many sources need to be brought together in order to be able to see patterns and where the sources

[63] Philip E. Tetlock, *Expert Political Judgement: How Good Is It? How Can we Know?* (Princeton: Princeton University Press, 2005).

[64] Nassim Nicholas Taleb, *The Black Swan: the impact of the highly improbable* (New York: Random House, 2007).

[65] Evgeny Morozov, 'Facebook isn't a charity. The poor will pay by surrendering their data', *The Guardian*, 26 April 2015.

correlate. To do so, one also needs a specific product. And products in the field of 'big data' which are able to draw correlations between different sources of data – for example what the company Palantir does – also easily cost one million dollars or more per year.

Thirdly, once a company is able to receive actionable intelligence to defend its network, a next step may be to elaborate a strategy to completely take the adversaries out by incapacitating them – this would mean putting instigators of attacks behind bars. And this requires working closely with law enforcement agencies. Arguably, only large companies forward cases (and possibly receive intelligence back from authorities) to law enforcement agencies. Smaller companies or those with less resources may still think that it may not be worth the trouble, and that the reputational damage coming out of such a procedure could be greater than the return. With time, as processes develop, companies may be increasingly comfortable in coming out about attacks they have undergone, and in working hands-in-hands with authorities to try to work out the diplomatic challenges foreign-based attackers can represent.

Taking this view, it means that in the short-run, technology making sense of 'big data' will become more and more available, while technical data on cyber-threat may become less politicised, and henceforth more easily exchanged between entities. This would ensure a better flow of information between different entities ensuring that attacks are detected and thwarted early. The legal basis for this type of exchange, as well as the bureaucratic hurdles would have been mostly overcome. People would then know what the process looked like and would follow it timely, for instance when an intelligence agency detects that a company could be a potential victim.

Intelligence as a best practice is a long shot from the current situation. As the result of the survey presented in the earlier section showed, the current focus is rather on 'bring-your-own-devices' or applying at times conflicting standards issued by international organisations. But the approach to cyber security may be slowly moving to that direction – given that no other revolutionary breakthrough of 'Black Swan'-type occurs.

From observations of the issues highlighted in this body of work the next stage is investigate at a deeper level into the the possible research gaps. Other themes will also be explored, for example the impact of best practice implementation on consumer services. Could this be a neglected option in ensuring that end-users are kept safe from cybercrime? Imposing heavy fines on service providers, device designers, etc who failed to provide a service or product that was fit for service can act as a stimulus to make certain all possible loopholes have been closed, i.e. hosting providers are not allowing cybercriminals to host malicious traffic from their networks.

One of the challenges is how to bring about the different existing standards in diverse sectors within a large industry area, for example, critical infrastructures. Standardised best practices need to be flexible enough to be appropriate without being so generic to render them practically useless. Again, what works for large multi-national corporations with large resources may tie down SMEs.

Best practices can apply to technical measures as well as organisational ones. As the CyberROAD survey shows there is a mismatch between the number of organisations who allow BYOD and those with best practice policies for these devices. This may be more than a purely technical problem but also an organisational one too? How can the uptake for best practices be further improved?

One potential problem area requiring more research is the apparent mismatch between the creation and implementation of standards and quidelines in the EU and the US as the latter has a more established track record in this area. One possible reason is an historic preference in the US for consumer rights groups which are self-regulating whereas in Europe the tendency is for governmental regulatory consumer support systems. Or it could simply be that strong leadership has lacking on the European side to push these concepts forward.

Understanding the connectivity between critical infrastructures and related sectors is crucial if vital ntional and interntational services are to be protected from cyber attack. These calls for collaboration and a great deal of transparency if initiatives in this area are to be successful. More research here is needed.

There exists a functioning working group overseeing the processes that that are need to keep smart grids safe but this is not the case in all the other sectors (e.g. communication, oil and gas, water). This indicates that there may be a rsearch gap that needs attention.

For escalation to D5.3, there are many considerations for further work that will be drawn from this body of work along with new themes that may arise. More results from the ongoing CyberROAD survey(s) from T5.1 will facilitate this process.

7 ANNEX A: MOST IMPORTANT SECURITY STANDARDS FOR INDUSTRIAL CONTROL SYSTEMS

Name	Type	Brief Description
IEC 62351 Parts 1-8 Information Security for Power System Control Operations	(family of) Standard	It defines security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation and protection.
IEC 62210 Power system control and associated communications.	Technical Report	It applies to computerised supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems.
IEC 62443 (formerly ISA 99) Security for industrial process measurement and control: network and system security	Standard and Guidelines	A series of standards, technical reports, and related information for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.
IEC 62357 Power system control and associated communications	Technical Report	It is a technical report describing all the existing object models, services, and protocols developed in technical committee 57 and showing how they relate to each other. It also presents a strategy showing where common models are needed, and if possible, recommending how to achieve a common model. This publication is of core relevance for Smart Grid.
IEEE 1686-2007 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Standard	It define the functions and features to be provided in substation intelligent electronic devices (lEDs) to accommodate critical infrastructure protection programs. The standard also addresses security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED.
IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security	Standard	It identifies and discusses security issues related to human intrusion upon electric power supply substations. It also presents various methods and techniques that are currently used to mitigate human intrusions.
IEEE 1711 Trial-Use Standard for a Cryptographic Protocol for Cyber Security Substation Serial Links	Standard	It defines a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of serial links. This standard is independent of the underlying communications protocol.
ISO/IEC 27000 Information security standards	(family of) Standard	The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system. The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues
NISTIR 7628 Guidelines for Smart Grid Cyber Security	Guidelines	It presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.[66]
NIST SP 800-53	Guidelines	It provides a catalog of security and privacy controls for federal information

[66] Smart Grid Interoperability Panel (SGIP), 'Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security',(2010).

Security and Privacy Controls for Federal Information Systems and Organizations		systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.[67]
NIST SP 800-82 Guide to Industrial Control System (ICS) security	Guidelines	The purpose of this document is to provide guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions.[68]
NERC CIP-002-1/009-2	Standard	NERC Standards CIP-002 through CIP-009 provide a cyber-security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.[69]
Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendation for standards developer	Guidelines	This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber-attacks. This catalog is not limited for use by a specific industry sector. All sectors can use it to develop a framework needed to produce a sound cybersecurity program.[70]

[67] National Institute of Standards and Technology, 'Security and Privacy Controls for Federal Information Systems and Organizations',(2013).
[68] 'Guide to Industrial Control Systems (ICS) Security',(2011).
[69] North American Electric Reliability Corporation (NERC), 'Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification',(2006).
[70] Department of Homeland Security, 'Catalog of Control Systems Security: Recommendation for standards developer',(2011).

(This corresponds to questions 6 to 9 only)

AP. 'Officials say new anti-leak measures set at NSA'. *CBS News*, 18 July 2013.
Beiner, Ronald. *Political Judgement*. Illinois: Univeristy of Chicago Press, 1984.
Biuro Bezpieczeństwa Narodowego [National Security Bureau]. 'Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej [Cybersecurity Doctrine of the Republic of Poland]'. Warszawa: BBN, 2015.
Bretschneider, Stuart, Frederick J. Marc-Aurele Jr., and Jiannan Wu. '"Best Practices" Research: A Methodological Guide for the Perplexed'. *Journal of Public Administration Research and Theory* 15, no. 2 (2004): 307–23.
BSA. 'Country: Poland'. BSA, 2014.
CEN-CENELEC-ETSI Smart Grid Coordination Group. 'Smart Grid Information Security'. 2012.
———. 'Smart Grid Reference Architecture'. 2012.
———. 'Smart Grid Set of Standards (Version 3.1)'. 2014.
CEN/CENELEC/ETSI Joint Working Group. 'Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids'. 2011.
CERT.GOV.PL. 'Publikacje'. http://www.cert.gov.pl/cer/publikacje [12 May 2015].
CERT.PL. 'CyberROAD – Invitation to participate in the project survey'. http://www.cert.pl/news/9671/langswitch_lang/en [12 May 2015].
Department of Homeland Security. 'Catalog of Control Systems Security: Recommendation for standards developer'. 2011.
Dyzurnet.pl. 'Dyzurnet'. http://www.dyzurnet.pl [12 May 2015].
ENISA. 'Cyber Atlantic 2011'. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 [1 May 2015].
———. 'ICS Security Related Working Groups, Standards and Initiatives'. Heraklion: ENISA, 2013.
———. 'Protecting Industrial Control Systems - Annex IV. ICS Security Related Initiatives'. Heraklion: ENISA, 2011.
———. 'Protecting Industrial Control Systems - Recommendations for Europe and Member States'. Heraklion: ENISA, 2011.
———. 'Protecting Industrial Control Systems. Recommendations for Europe and Member States'. Heraklion: ENISA, 2011.
European Commission. 'Directive on European Critical Infrastructures 2008/114/EC'. Brussels: European Commission, 2008.
———. 'European Programme for Critical Infrastructure Protection'. Brussels: European Commission, 2006.
———. 'A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure'. Brussels: European Commission, 2013.
———. 'Policy on Critical Information Infrastructure Protection (CIIP)'. Brussels: European Commission, 2013.
———. 'Protecting Europe from large scale cyber-attacks and] disruptions: enhancing preparedness, security and resilience (COM(2009) 149 final)'. Brussels: European Commission, 2009.
———. 'Review of the European Programme for Critical Infrastructure] Protection (EPCIP)'. Brussels: European Commission, 2012.
———. 'Special Eurobarometer 423: Cyber Security'. Brussels: European Commission, 2015.
European Commission, and European Free Trade Association. 'M/490 EN - Smart Grid] Mandate - Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment'. Brussels: EC, EFTA, 2011.
Facts on File World News Digest. 'Rifkin Sentenced in Bank Theft'. *Facts on File World News Digest*, 30 March 1979.
Fundacja Dzieci Niczyje. 'The Nobody's Children Foundation'. [12 May 2015].
Gardner, Bill. 'AM cycle'. *The Associated Press*, 3 November 1978.
Geuss, Raymond. 'What is political judgement?'. In *Political Judgement : Essays for John Dunn*, edited by Richard Bourke and Raymond Geuss. Cambridge: Cambridge University Press, 2009.
Greenberg, Andy. 'McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim'. *Forbes*, 3 August 2012.
Heuer, Richards J. 'Limits of Intelligence Analysis'. *Orbis* 49, no. 1 (2005): 75-94.
IEC TC57 WG15. 'List of Cybersecurity for Smart Grid Standards and Guidelines'. http://iectc57.ucaiug.org/wg15public/Public Documents/List of Smart Grid Standards with Cybersecurity.pdf [4 March 2015].
ITU. 'Part 5: Security best practices'. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part05.aspx [1 May 2015].
Kalev, Alexandra, Frank Dobbin, and Erin Kelly. 'Best Practices or Best Guesses? Assessing the Efficacy of Corporate Affirmative Action and Diversity Policies'. *American Sociological Review* 71, no. August (589-617 2006).
King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry*. Princeton, New Jersey: Princeton University Press, 1994.

Knapp, E. D., and J. T. Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham: Elsevier, 2014.
Kosinki, Jerzy. 'Cybercrime in Poland 2011-2012'. In *International Scientific Conference Archibald Reiss Days III*. Belgrade, 2015.
McKeown, Timothy J., and Alexander L. George. 'Case Studies and The- ories of Organizational Decision Making'. *Advances in Information Processing in Organizations* 2 (1985): 21–58.
MELANI, and GovCERT. 'Sécurité informatique: aide-mémoire pour les PME [IT security: a help for SMEs]'. Bern: MELANI, 2015.
Microsoft. 'Microsoft Security Intelligence Report '. http://www.microsoft.com/sir [12 May 2015].
Ministerstwo Spraw Wewnetrznych. 'Raport MSW o stanie bezpieczeństwa [Polish Ministry of the Interior reports on security in Poland]'. [12 May 2015].
Ministry of Administration and Digitisation, Internal Security Agency. 'Cyberspace Protection Policy of the Republic of Poland'. Warsaw: MAIC, 2013.
Morozov, Evgeny. 'Facebook isn't a charity. The poor will pay by surrendering their data'. *The Guardian*, 26 April 2015.
NASK. 'Cert Polska: Rapport 2014'. Warszawa: CERT Polska, NASK, 2014.
———. 'Papers'. http://www.cert.pl/raporty/langswitch_lang/en [12 May 2015].
National Institute of Standards and Technology. 'Guide to Industrial Control Systems (ICS) Security'. 2011.
———. 'Security and Privacy Controls for Federal Information Systems and Organizations'. 2013.
Nicolaus Copernicus University. 'Cybercrime Research Centre: Publications'. http://www.cybercrime.umk.pl/publications,7,en.html [12 May 2015].
North American Electric Reliability Corporation (NERC). 'Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification'. 2006.
Norton. 'Norton Cybercrime Report 2012'. http://us.norton.com/cybercrimereport [12 May 2015].
Overman, E. Sam, and Kathy J. Boyd. 'Best Practice Research and Postbureaucratic Reform'. *Journal of Public Administration Research and Theory* 4, no. 1 (1994): 67-83.
Policja. 'Statystyka'. http://www.statystyka.policja.pl/ [12 May 2015].
Polish Safer Internet Centre. 'saferinternet.pl: Keeping children and young people safe online'. http://www.saferinternet.pl/en/ [12 May 2015].
PwC. 'Economic Crime Survey Poland 2014'. Warsaw: PwC, 2014.
Roberts, Dexter. 'Chinese Hackers Like a 'Drunk Burglar,' 'Kicking Down the Door,' Says FBI Director'. *Bloomberg*, 6 October 2014.
Smart Grid Interoperability Panel (SGIP). 'Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security'. 2010.
SmartGrids. 'CEN / CENELEC / ETSI: Smart grids and standardization'. http://www.smartgrids.eu/CEN-CENELEC-ETSI [1 May 2015].
Taleb, Nassim Nicholas. *The Black Swan: the impact of the highly improbable*. New York: Random House, 2007.
Tetlock, Philip E. *Expert Political Judgement: How Good Is It? How Can we Know?* Princeton: Princeton University Press, 2005.
The Washington Post. 'Bank Was Unaware of Swindle'. *The Washington Post*, 11 November 1978.
Veselý, Arnošt. 'Theory and Methodology of Best Practice Research: A Critical Review of the Current State'. *Central European Journal of Public Policy* 5, no. 2 (2011): 98-117.
Wason, Peter C. 'On the Failure to Eliminate Hypotheses in a Conceptual Task'. *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960).
White House. 'Homeland Security Presidential Directive/HSPD-7'. 17 December 2003.
———. 'Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience'. 2013.