Fachhochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Cyber Security at Nuclear Facilities: National Approaches

An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI)

FOREWORD

Ensuring the security of nuclear facilities is a critical element in preventing theft of nuclear materials and sabotage that could result in a radiological release. The international community has traditionally focused on physical threats to facilities – for example, armed militants gaining access to or damaging a facility. A newer threat has now gained attention – the threat of a cyber attack on a facility that could lead to either an act of theft or sabotage – and is presenting new challenges to facility operators as well as national authorities. Given the increasing use of digital controls, it is expected that these challenges will only continue to grow.

The Nuclear Threat Initiative (NTI) has launched several projects to (i) understand the threat and current efforts to address the cyber-nuclear threat; (ii) identify gaps in current efforts and major challenges; and (iii) consider a path forward for addressing these challenges. This research paper presents the results of one of those projects conducted in joint cooperation between NTI and ISS. The purpose of this project is to understand and characterize current national approaches to cyber-nuclear security.

Guido Gluschke

ISS

Fachhochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Cyber Security at Nuclear Facilities: National Approaches

An ISS research project in cooperation with the Nuclear Threat Initiative (NTI)

For this research report valuable contributions were made by Friedrich Holl, Guido Gluschke, Andrea Cavina, Anna-Maria Praks and Marco Macori from the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, Germany; Page O. Stoutland, Samantha Pitts-Kiefer, Michelle Nalabandian and Alexandra Van Dine from Nuclear Threat Initiative (NTI), Washington, US; and Project Consultants Dmitry Kovchegin and Hui Zhang. Additional input was received from Clifford Glantz, Guy Landine from Pacific Northwest Laboratory (PNNL), Richland, WA, US; and Julio Rodriguez from Idaho National Laboratory (INL), Idaho Falls, US

.

June 2015, First Edition

The research project has been supported with funds from the Nuclear Threat Initiative (NTI). Its contents represent the views, findings and opinions of the authors, and are not necessarily those of the Nuclear Threat Initiative.

The Nuclear Threat Initiative is a privately-funded, U.S.-based non-profit organization with the mission to strengthen global security by reducing global threats from nuclear, chemical and biological weapons and materials. NTI is led by former U.S. Senator Sam Nunn.

The Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences is an associated institution of the Brandenburg University of Applied Sciences. While Brandenburg University has expertise in cyber security and security issues, ISS was founded to provide additional competence in the nuclear area with a specific focus in working internationally.

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Cyber Security at Nuclear Facilities: National Approaches

Table of Contents

Table of Contents 1
1 Abstract 2
2 Introduction and Methodology 3
2.1 Motivation 3
2.2 Scope and Goals 3
2.3 Methodology 5
2.4 Model Framework 5
2.5 Reading Note 6
3 National Legislation 7
3.1 Tables of Characteristics 7
4 Regulatory Framework 8
4.1 Tables of Characteristics 9
5 Regulations and Guidance 11
5.1 Tables of Characteristics 12
6 Licensing 13
6.1 Tables of Characteristics 13
7 Associated Regulatory Activities 13
7.1 Tables of Characteristics 14
8 Cyber Security Education 16
8.1 Tables of Characteristics 16
9 Conclusions 17
10 Appendix 1 – List of Questions 19
11 Appendix 2 – List of Abbreviations 24
12 References 24

1 Abstract

As the threat landscape changes and as new actors – from criminal organizations to nation states – get involved, the threat to nuclear facilities from cyber attacks is increasingly perceived as a growing, real problem. Recent complex attacks have been designed to target to instrumentation and control (IC) systems with all the potential consequences for safety and security such attacks may carry. Cyber security has become an essential element of the overall security framework of nuclear facilities and it is establishing itself as a priority for facility operators and national regulators.

This study focuses on characterizing what several countries are doing at the national level and introduces a potential model for developing a national approach to cyber security at nuclear facilities. The study focused on China, Germany, Russia, South Africa and the United States.

Thematically, this study focuses on the legal, regulatory, and institutional frameworks looking—i.e., the range of measures taken at the national level (see Figure 1 below). It compares laws, regulations, regulatory frameworks, licensing and other associated regulatory activities analyzing differences and similarities across the countries surveyed. The range of activities considered in the study provides a model—or the essential elements—of a national legal and regulatory framework necessary to ensure cyber security at nuclear facilities.

As a general conclusion the study found a wide spread in the maturity of national approaches to cyber security at nuclear facilities in the five countries surveyed. Whereas in some countries (Germany, the United States) the program has been fully institutionalized and most of its components have been partially or fully developed and implemented, in other countries the implementation is still fragmented, lacking institutional backing, or is near non-existent. A similar spread is likely found in other countries outside of the study.

Given the wide spread of maturity and the growing threat posed by cyber attacks—and the possible consequences of a cyber-mediated theft of nuclear materials or sabotage of a nuclear facilities, countries with nuclear programs should take the steps needed to put in place the national and regulatory frameworks necessary to ensure effective cyber security at nuclear facilities, or strengthen existing frameworks, in line with the model framework presented in this study. Countries that have new nuclear programs or are at the early phases of developing nuclear programs may also need assistance from international organizations like the International Atomic Energy Agency (IAEA) and other countries with more advanced programs.

2 Introduction and Methodology

2.1 Motivation

The threat from cyber attacks is increasingly perceived as a problem of national and international security as cyber attacks grow in number and sophistication and as actors behind them are no longer only private hackers or organized criminals but also nation states. Likewise, attacks once confined to *networks and business* computer systems have now been extended to instrumentation and control (IC) systems with all the implications and potential consequences such attacks may carry.

Nuclear facilities – in operation or being built – have progressively become heavily reliant on digital instrumentation or digital control systems or computer based information systems (IS). This is a consequence of the disappearance from the market of analog products as the digitalization of operational functions and working processes increases in quality and efficiency. This development gives rise to new threats as has been highlighted during various international events and conferences and confirmed by the publications of security vulnerabilities in the area of process control and automation systems.

There are several current developments which focus heavily on the role of IT/cyber security in the context of nuclear security. First, after the Fukushima disaster an Ad Hoc Group on Nuclear Security (AHGNS) was established by the Council of Europe to review the safety of all nuclear power plants (NPPs) in the European Union (EU). Five themes were selected for more detailed analysis, among them "Computer Security/Cyber Security." The analysis concluded that, given the key role of information and communication technology (ICT) and IC systems in any NPP, high priority has to be assigned to cyber security. In addition, in May 2011, the European Nuclear Safety Regulators Group (ENSREG) and the European Commission (EC) agreed on a two-track process to explore relevant safety and security aspects of cyber security. At the IAEA convened International Nuclear Security Conference in July 2013 cyber security was highlighted as a relevant issue.

While writing policy, planning new measures, and devising new controls are all fundamental activities to advance the field of cyber security, being able to clearly understand and characterize the current situation around the globe is at least as important. Therefore, this study focuses on characterizing what several countries are doing at the national level and introduces a potential model for the developing a national approach to cyber security at nuclear facilities.

2.2 Scope and Goals

This research project was undertaken as a joint collaboration between the Nuclear Threat Initiative (NTI) and the Institute for Security and Safety at the Brandenburg University of Applied Sciences (ISS). ISS has been working in the area of cyber-nuclear security for some years now and is internationally recognized.

The project was funded by NTI as one of the first steps in achieving NTI's objectives for cyber-nuclear security. NTI's overall objectives include strengthening the security of nuclear materials and facilities around the world – cyber-nuclear security is an important element of this. As a first step, NTI believed that it was important to characterize how a diverse set of countries are approaching cyber security at nuclear facilities.

By cyber security we understand all processes and mechanisms by which any digital equipment, information or service is protected from unintended or unauthorized access, change or destruction. By cyber security as a component of nuclear security we mean the range of measures enacted to prevent, detect, or respond to the theft of Category I nuclear material or the sabotage of a nuclear facility that could result in catastrophic consequences through cyber-attacks, either alone or combined with physical

attacks. The scope of this study is restricted to civilian nuclear fuel cycle facilities, e.g., enrichment or fuel fabrication plants, power plants, reprocessing facilities, research reactors, etc.

The impetus for the focus on cyber security is that it is one of the most significant new key elements that have entered the nuclear security arena in the last decades, quickly gaining prominence and significance due to growing reliance on digital equipment and to game-changing events like the Stuxnet attack. After several years in which cyber security at nuclear facilities has evolved from ad hoc measures and pilot projects to a fairly established and important element of overall nuclear security, it is important and timely to try and capture a comparative snapshot of where its implementation stands in several countries.

Specifically, this study focuses on the legal, regulatory, and institutional frameworks for cyber security looking in detail at the range of measures affecting the higher levels of the hierarchy of responsibilities. The study's comparative analysis focuses on national legislation, regulatory frameworks, regulations and guidance, licensing and other associated regulatory activities; thus we left aside, in this first project, the more operational and technical aspects of cyber security and their implementation at the facility level.

The following figure shows the various tiers of cyber security needed to address the cyber threat at nuclear facilities and indicates the tiers at the nation state level, which is the focus of this study:

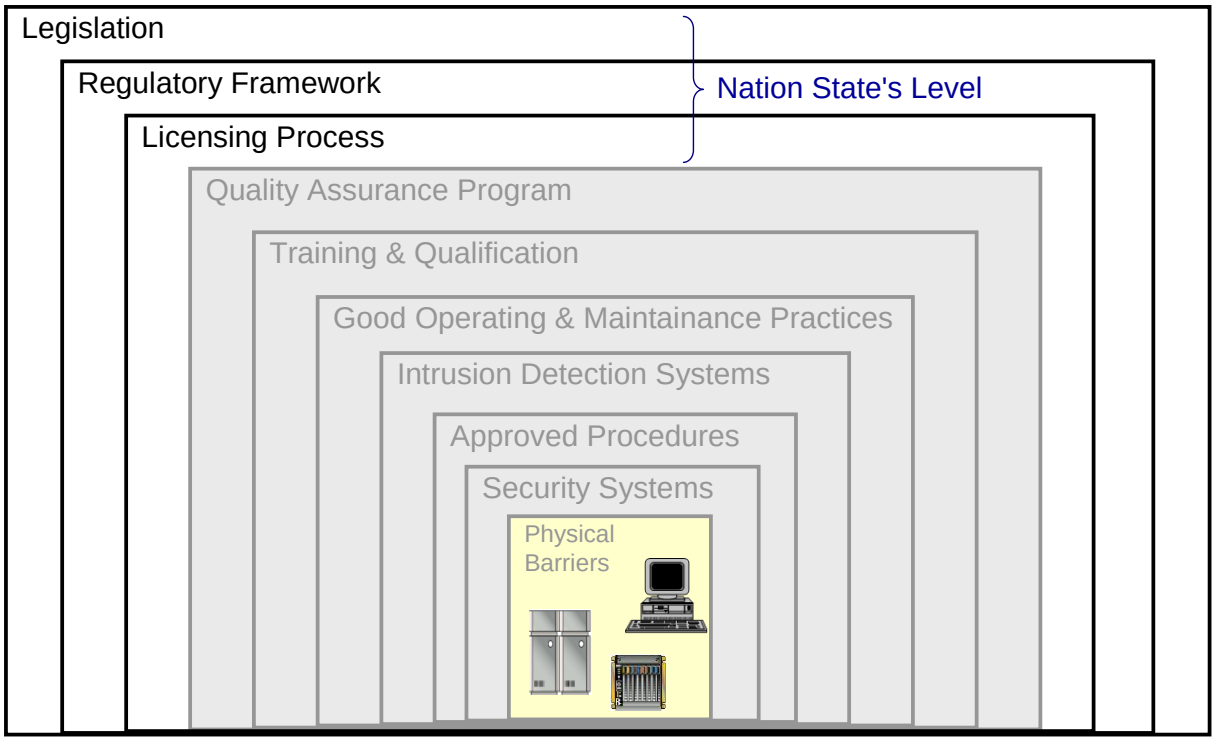

Figure 1: Defence-in-depth model for cyber security in the nuclear context

This approach allows a more direct comparison between countries as it reflects a national approach and not individual initiatives of facilities or organizations. Also an analysis of these top tiers of the cyber security programmes provides an understanding of the influence legal and regulatory instruments have on operational and facility level implementation of cyber security. Last, the fact that laws and regulations are often made available to the public permits a more thorough data collection and concurrent verification of sources.

2.3 Methodology

The methodology for data gathering combines open source analysis with a questionnaire directed at experts, officials and academics in the five countries chosen. The questionnaire was devised to not only verify the existence of specific elements within a country's nuclear security framework, but also to try and characterize the maturity and breadth of their implementation. The data was collected through a combination of questionnaires collection through email, interviews and direct feedback from key national experts. The data was then checked for consistency with available sources and contrasted with data from the other countries to obtain a comparative overview of the state of implementation of cyber security in nuclear programs. This led to conclusions on the current level of maturity of the programmes as well as a characterization of the programmes themselves. The five countries chosen (China, Germany, Russian Federation, South Africa and the United States) all have nuclear power plants and range from very large infrastructures (e.g., the US with 99 nuclear power plants (NPPs henceforth) and several other nuclear fuel cycle facilities) to very small (e.g., South Africa, with 2 NPPs) and cover a wide geographical, cultural and economic distribution.

While there are not yet recognized international standards on how the national infrastructure for cyber security should be organized, several international and national organizations have published guidance in this direction ranging from high level guidance documents (IAEA[1], WINS[2]) to detailed technical guidance (e.g., ANSI/ISA[3]). From these documents and existing best practices in the nuclear and other sectors it is possible to model a preferred scenario of how such a cyber security infrastructure could be configured; this study outlines some of the elements of such a *model* infrastructure and analytically compares them to the frameworks found in the sample countries.

2.4 Model Framework

The IAEA Nuclear Security Fundamentals document (NSS20) provides the objective and essential elements of an appropriate and effective national nuclear security regime. The NSS20 approach is broader than is needed for cyber; but most essential elements can play a role when assessing a nation state in terms of nuclear-cyber readiness, such as 'Identification and Definition of Nuclear Security Responsibilities', 'Legislative, Regulatory Framework' or 'Identification and Assessment of Nuclear Security Threats'.

The structure of the report is ordered according to the project's adapted assessment objectives and potential model, and is summarized as follows:

I. National legislation

At the highest level, legislation should ideally reflect a contemporary approach to nuclear security, i.e., reflecting the rapid evolution the field has seen since 2001 and among others, incorporating concepts expressed in the 2005 amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM)[4] as well as including or referring to the security of information (or more explicitly cyber security) as one of the key elements of nuclear security. In this context it is probably more feasible to do so in those national legislations where nuclear security is separate from *generic* nuclear laws dealing with the promotion and regulation at large of any activity involving radioactive materials or nuclear energy generation.

II. Regulatory framework

Likewise, legislation should operate at the *correct* level and avoid rapid obsolescence by steering clear from legislating specific details which are bound to evolve rapidly (like technology) and should instead focus on establishing the framework for the correct operation of a regulatory authority, on its ability to write and enforce regulation and on the criminalization and prosecution of relevant crimes.

III. Regulations and guidance

Regulations instead, are standards adopted as rules by the relevant authority to implement, interpret, or make specific the laws enforced or administered by the authority itself. These are needed so that the industry may have detailed guidance and a clear interpretation of the law. Regulations have at the same time the possibility to evolve and adapt more rapidly than legislation given a lighter approval/modification procedure involving fewer stakeholders.

IV. Licensing

Ideally cyber security should be embedded from the start into the design of nuclear facilities themselves and their associated security plans. One of the crucial instruments to ensure this happens and is maintained – as a design goal and as an element of safety and security culture – throughout the lifecycle of an NPP are the licensing process and its enforcement.

V. Associated regulatory activities

From supply chain control to personnel security to law enforcement training, many collateral issues may have a strong impact on the cyber security of nuclear facilities. We try to examine and characterize a few of those of highest relevance.

VI. Cyber Security education

Centres of higher education focussed on cyber security or nuclear security can provide research, fundamental to advance the field, as well as a highly trained workforce, necessary to ensure the adequate level of competence in the facilities.

2.5 Reading Note

The full list of questions used in the survey is found in Appendix I and questions are referenced throughout the text by their number. Bibliographical and legislative references are in the endnotes.

3 National Legislation

In this section we chose questions that verify the existence of legislation on nuclear and cyber security and how these cross-relate to each other and to international legal instruments with the aim of characterising the legal framework for cyber security at nuclear facilities.

(Q.1) It is not surprising that, with the exception of China, every country surveyed has some form of generic nuclear law (e.g. a law establishing a nuclear power programme and its related infrastructure) in place. China is drafting two nuclear related laws, one of which will cover nuclear security and currently regulates nuclear facilities through ministerial regulations and directives. Most of these generic laws are 15 or more years older as legislation on nuclear activities is a well-established, mature practice that has been continuously promoted by international organizations like IAEA.

Writing legislation specifically dedicated to nuclear security is a more recently established practice. Nonetheless, in three out of five countries surveyed we find that nuclear security has their own dedicated legislative instruments, usually promulgated within the last ten years. Of the other two countries, China is currently drafting its nuclear security related laws and South Africa has not updated its legislation beyond its generic nuclear laws of 1999 in which some references to security are found. Of note is also that in some cases safety and security are addressed within the same legislation.

As the rise to prominence of cyber security is very recent it is unsurprising that only two out of three countries, Russia and Germany, address cyber security explicitly within their nuclear laws or nuclear security laws as most of these would have been drafted earlier.

(Q.2) Generic cyber security legislation is commonly drafted independently from the nuclear or even the critical infrastructure sectors and most of these generic cyber security laws are of recent creation. Out of five countries only the US and China do not have generic national legislation on cyber security, while Russia and Germany even explicitly reference nuclear security in their cyber security laws. Some countries have more than one single legal instrument addressing cyber security, often with different pieces of legislation addressing various aspects of cyber and information security.

(Q.3) All of the five countries surveyed have issued one or more national policies addressing cyber security. None of these policies is specifically dedicated to nuclear facilities but in some cases they are specifically dedicated to the cyber security of national critical infrastructure (Germany, US).

3.1 Tables of Characteristics

Q.1 Specificity of nuclear security legislation

Characteristics	Countries
No nuclear law	China
A generic "nuclear law" dealing broadly with issues relating to the implementation of nuclear power with few or no explicit references to nuclear security	South Africa[5]
A generic "nuclear law" with explicit references or detailed sections dedicated to nuclear security	
A law specifically dedicated to nuclear security (the latter often in conjunction with more generic "nuclear laws" within the same legal system)	US[6], Germany[7], Russia[8]

Q.1.1 References within nuclear legislation to cyber security (or information security or confidentiality)

Characteristics	Countries
Nuclear or nuclear security laws with no mention of cyber security or information security or protection of confidentiality	South Africa, US
Nuclear or nuclear security laws with explicit references to cyber security or information security or protection of confidentiality	
Nuclear or nuclear security laws with specific sections dedicated to cyber security	Germany[9], Russia[10]

Q.2 Cyber security legislation

Characteristics	Countries
No legislation regarding cyber security is in place	US, China
Legislation on cyber security is in place, no explicit provisions for critical infrastructure or nuclear facilities	South Africa[11]
Legislation on cyber security is in place, and either has dedicated sections for critical infrastructure or nuclear facilities or separate laws covering the cyber security of these exist	Russia[12], Germany[13]

Q.3 Cyber security policies

Characteristics	Countries
No national policy regarding cyber security has been issued	
National policy(-ies) regarding cyber security has been issued, partially applicable nuclear facilities	Russia[14], Germany[15], US[16], China[17], South Africa[18]
National policy(-ies) regarding cyber security has been issued, and either has dedicated sections for nuclear facilities or separate policies covering these exist	

4 Regulatory Framework

This section of the study examines the regulatory frameworks with respect to nuclear and cyber security with a focus on which authorities exist, which competencies they have and how they relate to each other. The study also looked at the specific capabilities available to these authorities and at the characteristics of their cyber security programmes.

(Q.5) All countries surveyed have established some regulatory authority for (non-nuclear) cyber security. In most countries more than one agency or authority has some role or responsibility to play in regulating cyber security. It is unclear from the data gathered in most countries whether the work of these authorities is coordinated, hierarchically organized or clearly divided along topical lines, perhaps reflecting the lack of maturity of this relatively new field of regulations. The spectrum ranges from South Africa, where four entities are reported as having cyber security regulatory roles, to China where the major regulatory power on the issue is concentrated at the Ministry of Public Security and the Ministry of Industry and Information Technology. [19]

(Q.6) In a similar fashion, all countries surveyed have established authorities regulating nuclear activities. In comparison to what the study found for cyber security, these authorities have more clearly defined roles and in each of the five countries there is a clearly defined main regulatory body. (Q.7) In three countries other authorities alongside the main regulator cover more limited, specific regulatory roles or

an explicitly separate function covering military activities (three of the countries surveyed – US, Russia and China – are nuclear weapon states).

Looking at coordination among different agencies tasked with regulations (Q.8), in the case of cyber security, in countries where there is more than one body, three out of four countries have established coordinating bodies, and the South Africa being the only country surveyed lacking this function. A similar picture is found in the case of nuclear regulations where three countries have multiple responsible authorities and again only the South Africa lacks a coordinating function.

In all countries where the specific function of regulating cyber security in nuclear activities exists (Q.9) (four out of five), it is always allocated to an authority already identified as one of the nuclear regulatory bodies, and in all cases this is actually the main regulatory body. In China there is no authority yet tasked with this function but its assignment to one of the two nuclear regulatory bodies is under discussion.

The more in depth questions (Q.9.1-5) in the survey detailing the way in which cyber security at nuclear facilities is regulated were meant to highlight the maturity of the programme in the countries surveyed but have in the end limited comparative value as relevant information was only available from Germany and the US. There is limited information regarding Russia, a lack of a properly established programme in the South Africa and, as already mentioned, no regulation of cyber security for nuclear activities in China.

Only the US and Germany have a unit within their nuclear regulating authority dedicated to cyber security (Q.9.1). It follows that these two countries also have specific cyber security technical competencies available (Q.9.3) – in the US directly within the regulator, and in Germany within the Technical Support Organization (TSO). The US also reports (Q.9.5.1-3) having an independent budget and head of programme for the regulation of cyber security in the nuclear sector. Three out of five countries surveyed (Q.10) (US, Russia and Germany) have TSOs with specific competencies in cyber security that are available to regulators and/or operators and cooperation agreements with the regulator have been formalized.

4.1 Tables of Characteristics

Q.5 Competent authority (cyber, non-nuclear)

Characteristics	Countries
No competent authority regulating cyber security within the country has been established	
Cyber security regulatory activities are fragmented over multiple authorities having partial coverage of the field	South Africa, US, Russia
Either one single competent authority exists or multiple authorities with well-defined and coordinated regulatory competences	China, Germany

Q.6 Competent authority (nuclear)

Characteristics	Countries
Nuclear security regulatory activities are fragmented over multiple authorities having partial coverage of the field	
Either one single competent authority exists or multiple authorities with well-defined and coordinated regulatory competences	Russia, Germany, US, China, South Africa

Q.8 Coordinating body (cyber)

Characteristics	Countries
No council or committee has been established	South Africa
A council or committee coordinating various stakeholders for national cyber security has been established	US, Russia, Germany, China
A council or committee coordinating various stakeholders specific to cyber security for nuclear has been established	

Q.8 Coordinating body (nuclear)

Characteristics	Countries
No council or committee has been established	South Africa
A council or committee coordinating various stakeholders involved in nuclear activities has been established	China
A council or committee coordinating various stakeholders specific to nuclear security has been established	US, Russia, Germany

Q.9 Competent Authority for cyber security at nuclear facilities

Characteristics	Countries
No competent authority explicitly regulating cyber security at nuclear facilities has been established	China
Cyber security at nuclear facilities is the responsibility of the nuclear regulatory body	Germany, US, South Africa
Cyber security at nuclear facilities is the responsibility of the cyber regulatory body	Russia

Q.9.1-3 Existence of dedicated unit for cyber security at nuclear facilities

Characteristics	Countries
No unit regulating cyber security exists	South Africa, China
Cyber security regulation is performed by units dedicated to it	Germany, Russia
Cyber security regulation is performed by independent dedicated units with their own programme, budget and senior management	US

Q.9 Application of cyber security regulations to nuclear facilities

Characteristics	Countries
Cyber security at nuclear facilities is not formally regulated	South Africa, China
Cyber security of different systems at nuclear facilities is regulated by different authorities	
Cyber security regulation of nuclear facilities is unified under one body	Russia, Germany, US

Q.10 Technical support of cyber security regulation of nuclear facilities

Characteristics	Countries
No technical support is available for cyber security	South Africa
Technical support is available for cyber security on an ad hoc basis	China
Technical support is available for cyber security and regulated by formal agreements	US, Russia and Germany

5 Regulations and Guidance

In this section questions scrutinize the extent and depth of written regulations in cyber security and specifically in cyber security in the nuclear sector. These questions also look at how cyber security may be referenced in regulations pertaining to other aspects of nuclear safety and security.

All countries surveyed (Q.11) (except the US[20]) have published generic cyber security regulations covering national infrastructure (i.e., non-specific to the nuclear sector) and the entity publishing and controlling the regulations corresponds to one of those identified as regulators under question 5 (cyber security regulator); in the US some sector-wide (i.e., energy & grid) cyber security regulations are in place. Few details have been made available regarding the status of implementation of the above regulations in the five countries and they are not sufficient to derive either conclusions on the maturity of the regulations in individual countries or comparative considerations.

Three out of five countries surveyed (Q.12) possess written regulations regarding cyber security at nuclear facilities. Countries without written regulations are China (where such regulations are under consideration) and the South Africa. In the three countries where such regulations exist, the entity publishing and controlling the regulations corresponds to one of the identified regulators. In Russia the mandatory regulations are issued by the cyber regulatory body and are adapted at the agency level to provide detailed guidance for cyber security in nuclear security related systems. Also in Russia, lack of specific guidance associated with the regulations may denote a lower maturity level for cyber security in the nuclear sector. In Germany and the US, regulations have been published, are supported by guidance, are enforced and regularly reviewed, which denotes a higher level of maturity.

Regarding the extension of the coverage of cyber security regulations within the nuclear sector, in the three countries where they exist, coverage seems to extend to most of the domains (cf. Q. 13.1-14 in Appendix I for details) identified in the survey. In the interest of a comparative analysis, the following exceptions are noted:

- Germany's regulations do not cover cyber threat analysis.
- Russia is the only country covering cyber security of nuclear material accounting and control (NMAC) in the regulations.
- Russia's regulations do not cover the nuclear supply chain.

Mechanisms to enforce cyber security regulations are common to three countries and include: licensing, inspections and oversight processes.

The update of nuclear facilities' security plans in order to comply with newly published cyber security regulations (Q.14) took place in both the US as well as in Germany where it was made compulsory. In Russia the update is recommended but not compulsory for existing installations and will only take place at the time of upgrade or replacement of existing systems. South Africa reports that nuclear facilities voluntarily updated their security plans to include cyber security despite the lack of written regulations.

Regarding cross-referencing of cyber security in existing regulations relevant to nuclear (Q.15), the picture presents some patterns and some anomalies:

- In all cases (including South Africa), physical protection regulations reference cyber security.
- Safety regulations reference cyber security only in the US.
- NMAC regulations reference cyber security only in Russia.

5.1 Tables of Characteristics

Q.11 Written regulations (cyber security in national infrastructure)

Characteristics	Countries
There are no written regulations regarding cyber security in national infrastructure / only sectorial regulations exist.	US
There are published written regulations regarding cyber security in national infrastructure	Russia[21], Germany[22], China[23], South Africa[24]
There are published, enforced and regularly assessed written regulations regarding cyber security in national infrastructure	

Q.12 Written regulations (nuclear)

Characteristics	Countries
There are no written regulations regarding cyber security at nuclear facilities	South Africa, China
There are published written regulations regarding cyber security at nuclear facilities	
There are published, enforced and regularly assessed written regulations regarding cyber security at nuclear facilities	Russia[25], Germany[26], US[27]

Q.14 Enforcement of cyber security regulations at nuclear facilities

Characteristics	Countries
Regulations for cyber security at nuclear facilities do not exist	South Africa, China
Regulations for cyber security at nuclear facilities exist but are not enforced	
Regulations for cyber security at nuclear facilities exist and are enforced through regulatory oversight and inspections	Russia, Germany, US

Q.16 Cross referencing of cyber security in other nuclear regulations

Characteristics	Countries
Safety and security regulations do not reference cyber security	China
Safety regulations make reference to cyber security	US
Security regulations make reference to cyber security	South Africa, US, Russia, Germany

6 Licensing

In this section questions examine how cyber security is integrated in the licensing process for nuclear facilities.

When looking at the licensing process (Q.16), there is continuity with previously analysed regulatory activities. In fact, it is in the same three countries (Russia, the US and Germany) where considerations for cyber security are explicitly included in the licensing process and when looking at details, the coverage is broad in all three countries.

The same pattern is observed for the certification process of individual systems (Q.17) where again cyber security is only explicitly addressed in Germany, the US and Russia. Again, looking at the specific details of which systems are covered by the certification process in general there is broad coverage in the three countries and some specific differences. Of note:

- Safety systems are not included in Russia while business and NMAC systems are
- Once again, systems relevant to security are covered in all three countries.

6.1 Tables of Characteristics

Q.17 Licensing processes

Characteristics	Countries
No mention of cyber security	China, South Africa
Cyber security is part of some licensing processes	
Cyber security is integrated in most or all licensing processes	Russia, Germany, US

Q.18 Systems certification

Characteristics	Countries
No mention of cyber security	China, South Africa
Cyber security is part of some certification processes	
Cyber security is integrated in most or all certification processes	Russia, Germany, US

7 Associated Regulatory Activities

In this section the questions survey a set of regulatory activities relevant to cyber security. The purpose of these questions is to characterize how threat assessment is done, how cyber security training is integrated in the programme, whether the nuclear supply chain is regulated and whether cyber security is a component of those regulations. Questions also look at how cyber security and personnel security can constructively interact.

Three out of the five countries surveyed have a designated authority that conducts cyber threat assessments for nuclear facilities (Q.18) and in all three cases (Germany, the US and South Africa) national intelligence is involved in the preparation of the threat information and said information is made available directly to nuclear facilities. Both the South Africa and the US use the Design Basis Threat (DBT) as the instrument to communicate threats to facilities, but the US also makes use of additional instruments (Advisories) to do so.

All countries make use of the DBT (Q.18.3) in dealing with threats to nuclear facilities. In two cases (South Africa and the US) cyber is an integrated component of the main DBT while in Germany it is a separate DBT document (Cyber DBT) and in Russia and China, DBT and cyber threat assessments are done using different, separate methodologies.

In only two countries (Russia and the US) does the competent authority provide or facilitate training on cyber security issues (Q.19) and in both cases only for their own inspectors and not for operators. Topics covered are similar but it is of note that no training on I&C security is yet provided in Russia.

Again, the same constellation of three out of five countries conducts regular inspections of nuclear facilities focusing on cyber security issues (Q.20). The methodology in use includes in all cases verification of compliance with regulations but, in the case of Germany and the US, it adds also performance based assessments. The US and Russia base their inspections on a triennial cycle while Germany may run inspections several times a year, conversely the duration of inspections in Germany (1-2 days) is much shorter than those in the US (1 week) or Russia (3 weeks). Limited information has been provided on the specific competences of the inspectors. In both Russia and the US, facilities are also asked to run self-assessments.

Three (US, Russia and South Africa) countries out of five regulate the nuclear supply chain (Q.21) but of these only Russia and the US explicitly regulate the cyber component of the supply chain.

All countries perform some form of vetting or trustworthiness checks on individuals or third parties accessing or managing sensitive digital systems (Q.22); in the case of Russia the checks are performed by the intelligence/security services and happen only if the individual has to have access to confidential information, it is unclear if systems per se are classified as confidential. Additionally, South Africa and the US run compulsory trainings on cyber security for individuals or third parties accessing or managing the sensitive digital systems (Q.23).

Responses regarding the cyber security of activities outside the nuclear sector but relevant to nuclear security (Q.24) are too fragmented to allow a comparative approach but it is evident that laws and initiatives are in place at different level of maturity.

7.1 Tables of Characteristics

Q.18 Cyber threat assessment for nuclear facilities

Characteristics	Countries
No cyber threat assessment is performed	China
Cyber threat assessment is performed	Russia
Cyber threat assessment is performed, receives the input of national intelligence and is regularly communicated to stakeholders	Germany, US, South Africa

Q.18.3 Cyber DBT for nuclear facilities

Characteristics	Countries
Cyber threats are not considered in DBT or similar documents	China
Cyber threats are integrated in the DBT	South Africa, US
Cyber threats are presented separately from the DBT in a non-DBT format	Russia
The Cyber DBT is a separate complementary document to the DBT	Germany

Q.19 Cyber security training

Characteristics	Countries
The competent authority does not provide training	China, Germany, South Africa
The competent authority provides training	US, Russia

Q.20 Cyber security inspections of nuclear facilities

Characteristics	Countries
The competent authority does not conduct inspections on cyber security	South Africa, China
The competent authority conducts reactive/ad hoc inspections on cyber security	
The competent authority conducts regular inspections on cyber security	Germany, US, Russia

Q.21 Regulations of nuclear supply chain

Characteristics	Countries
The nuclear supply chain is not regulated/controlled	China
The nuclear supply chain is regulated/controlled but not its cyber components	South Africa, Germany
The nuclear supply chain is regulated/controlled including its cyber components	US, Russia

Q.22 Personnel security of digital systems

Characteristics	Countries
The competent authority does not conduct vetting of individuals accessing or sensitive systems	
The competent authority conducts vetting of individuals accessing or sensitive systems	All

8 Cyber Security Education

In this section questions survey the presence of national level initiatives in education for nuclear and cyber security.

China and Russia offer national level education in nuclear security (Q.25), in Russia even to the level of academic degrees. Comparatively, every country has educational programmes in cyber security (Q.26) available also as part (or whole) of academic degrees but not connected to nuclear facilities. The only country where a national educational program for nuclear IT and/or cyber security exist (Q.27) is Russia. There seems to be plans to establish such a programme in the South Africa.

8.1 Tables of Characteristics

Q.25 Nuclear security education

Characteristics	Countries
No national level programme exists	
Limited education/training exist	US, Germany, South Africa
Established education programme	China, Russia

Q.26 Cyber security education

Characteristics	Countries
No national level programme exists	
Limited education/training exist	
Established education programme	All

Q.27 Cyber security education for nuclear

Characteristics	Countries
No national level programme exists	South Africa, China
Limited education/training exist	US
Established education programme	Russia

9 Conclusions

The most general observation that may be derived from the study is an acknowledgement of the wide spread in the maturity of cyber security programmes within the nuclear industry in the five countries surveyed. Whereas in some countries (Germany, US) the programme has been fully institutionalized and most of its components have been partially or fully developed and implemented, in other countries the implementation is still fragmented, lacking institutional backing or near non-existent.

Another important and reassuring conclusion is to see how in two countries (again US and Germany) the programme, while not as mature as other longer established nuclear security programmes like physical protection, has progressed a long way towards formalization and institutionalization and most of the standard, formal instruments are in place and in force. The observed structure of the programmes follows logically from legislation to regulations and the regulatory bodies have been empowered with both authority and means to implement the programmes. Many of the elements of the programmes have only been recently created and they are often not backed up by significant implementation experience and will surely need to evolve as the field becomes more established; they have nonetheless started to propagate their effects onto the operational level within facilities.

In all countries surveyed, the non-nuclear cyber security institutional framework is observed to be more fragmented and complex compared to the nuclear security framework. This is possibly due to both historical considerations and the fact that cyber security touches extremely varied aspects of a country's infrastructure from telecommunication to intelligence services to national critical infrastructure protection. Also, despite its rapid rise to prominence it is still not *per se* a mature field and that is reflected in the lack of streamlining of the laws and authorities responsible for it. Paradoxically it is found to be more streamlined within the nuclear industry itself as in almost all countries (with the exception of Russia) the role of regulating cyber security in the nuclear sector is assigned directly to the nuclear regulatory authority.

Some cyber security initiatives in the nuclear industry seem to exist in all countries, but we can distinguish three main modes of operations: a well-defined and institutionalized one like in Germany and the US; a more fragmented and less formalized approach but still with multiple initiatives and competent organizations like in Russia; and finally a sporadic and ad hoc approach with little impact like in China or South Africa.

Several recommendations can arise from the observations and analysis of collected data that will apply differently according to the maturity and model within each country. At the highest level it is evident that efforts need to be made in ensuring that cyber security oversight is further streamlined in most countries: clearly defining the scope of each regulating agency as well as establishing either reporting hierarchies or coordinating bodies to ensure both full coverage of all sectors and minimizing duplication of efforts and conflicts of interest. Furthermore, coordination should not only be established among cyber security bodies but also between entities responsible for nuclear security and cyber security. Much work is left to be done to integrate cyber security in various services, industries and other aspects of civil and military processes; with a growing reliance on digital data and services, cyber security will in the long term naturally take its place as an increasingly standard and predominant element of security. We are obviously still very far from a steady-state operation as both technologies and threats evolve at a exceedingly fast pace, so fast in fact that it surpasses most institutional abilities to keep up and absorb change. The resulting danger is that this currently creates a very asymmetrical field, where institutions are always trying to catch up with unknown threats and threat agents.

However cyber security may evolve long term, it is crucial that states start gathering the momentum necessary to keep abreast of the changes and adopt a pragmatic approach towards establishing the necessary infrastructure for tackling threats. Where responsibilities for cyber security are fragmented, redundant or unclear or where it is unsure whether the legal and regulatory coverage is thorough and exhaustive, the state could commit to a rigorous review of their legal instruments and infrastructure and ensure gaps are filled and responsibilities are properly assigned and coordinated. In many of the cases we

observed, the creation of one single agency/organization overseeing the application of cyber security to all the many domains it affects seems not to be the preferred solution. Rather, the establishment of a lighter weight coordination council/body regrouping the agencies responsible for the different domains of application of cyber security seem to be a more efficient answer – definitely for the short term and possibly also as a long term solution.

Regarding cyber security in the nuclear sector, it seems also reasonable to suggest that the nuclear regulatory body (or the appropriate one among them) should be directly and primarily involved in the oversight of cyber security at nuclear facilities, whether on its own, in cooperation with a cyber regulatory body and/or with the assistance of relevant technical support organizations. The main argument for this could be that to understand the threats and the vulnerabilities associated with cyber security at nuclear facilities a thorough understanding of nuclear security is paramount and takes precedence over other considerations.

Further efforts need also to be made in ensuring that cyber security is acknowledged and fully referenced in the other domains protecting the operation of nuclear facilities (e.g., safety, physical security, NMAC). In particular in some fields – instrumentation & control and physical protection technologies come to mind – the interaction between the cyber and physical sides is so strong and inextricable that they are coming into fields of studies and analysis of their own. It is therefore crucial that these interdependences are rapidly recognized and documented at the appropriate level in guidance instruments. Where relevant, most safety and security functions may have to be reassessed with a clear understanding of possible interactions with cyber threats in mind.

In general cyber security concerns should extend to cover the full lifecycle of nuclear facilities and their components. Therefore cyber security should become a fully incorporated factor in such activities associated with the operation of nuclear facilities like the management of the nuclear supply chain, instrumentation certification procedures, personnel security issues, core training curricula or threat assessment to name a few.

Another set of conclusions derived from this first comparative analysis of cyber security at nuclear facilities points at the need for more and more comprehensive studies of the field. A most obvious and more immediate expansion of the current research would obviously involve looking at other countries that have a significant nuclear industry and extend the comparison to a more significant sample. Besides allowing the consolidation and refinement of the study's analysis it could also point to novel solutions or implementation of the nuclear-cyber security infrastructure.

Another possible expansion of the study could instead point toward other "inner layers" of the defence in depth scheme. For example it would be extremely valuable to look at how regulations are received and implemented in the industry and start looking at some of the more operational issues faced by facilities.

An initiative of more immediate application would be a more rigorous development of a cyber-nuclear security maturity model for the institutional framework. This would enable researchers to more accurately characterize and describe national frameworks against a more formally defined model. Of similar utility could be the creation of model regulations or of workshops to help states develop their own cyber security regulations.

Cyber security, despite a history now reaching almost half a century, remains a young and fast evolving discipline which will need to mature rapidly due to the growing weight – in threats and consequences – it carries as digital elements rapidly take over critical functions within our industries and our society.

10 Appendix 1 – List of Questions

The following is the list of questions that were used to gather data for the project.

Q 1. Does your country have national legislation in place for **nuclear security**?
If so,
1.1. Are there, in such laws, any provisions specific to cyber security?
1.2. Which, if any, international treaties and standards are referenced in the national legislation?

Q 2. Does your country have national legislation in place for **cyber security** (not specific to nuclear)?
If so,
2.1. Are there, in such laws, any provisions that apply to nuclear security?
2.2. Which, if any, international treaties and standards are referenced in the national legislation?

Q 3. Has the government of your country issued **non-legally binding policies** (i.e. policy papers, strategic plans, doctrines or guidelines) covering or impacting cyber security?
If so,
3.1. Is any part of those policies applicable to nuclear security?
3.2. Are those policies publically available?
If so, please send them or add a link:

Q 4. Please list any additional national **legal instruments** that regulate cyber security in the nuclear sector in your country?

Q 5. Do you have one or more established **competent authority** responsible for **regulating** (or who have oversight of) **cyber security** within the country? Which are they?

Q 6. Do you have one or more **competent authority** in the country that exert functions or have authority comparable to those defined as a ***nuclear regulatory body*** by IAEA standards? Which are they?

Q 7. If more than one exists, how are the respective **domains** of competence subdivided? By industry/activity? By type of regulations?

Q 8. Is there a **council** or committee who harmonizes the work of different agencies having responsibilities for cyber and/or nuclear security?
If so,
8.1. What is the name of the council? To whom do they report?

Q 9. Referring to the agencies/bodies identified in questions #5 and #6; which of these are tasked with **regulating cyber security** for **nuclear facilities**?
If so,
9.1. Are there **distinct** units/departments **dedicated to cyber security** within these bodies?
9.2. When were they created? Details?
9.3. Describe the **cyber security competencies/expertise** available within these units? What is the background (training or education) of the respective staff?

9.4. If more than one agency/body is identified in question 9. please specify:
  9.4.1. Which body regulates cyber security **of computer systems**?
  9.4.2. Which body regulates cyber security **of Safety Systems and Instrumentation and Control (I&C) Systems**?
  9.4.3. Which body regulates cyber security **of Physical Protection systems**?
  9.4.4. Which body regulates cyber security of Nuclear Material **Accounting and Control systems**?
9.5. Is the **oversight of cyber security** in nuclear facilities a self-standing**, independent programme** within the regulatory body?
  9.5.1. Is the head of the programme responsible **only** for cyber security?
  9.5.2. Do they **report directly** to the Director General/CEO?
  9.5.3. Is there a **distinct budget** available for cyber security regulatory activities?

Q 10. Are there government or independent **Technical Authorities or Organizations** (**TA**) with specific competences in cyber security that are available to regulators and/or operators for support?
If so,
10.1. Is TA-Regulator cooperation documented by formal agreement and processes?
10.2. Please describe any such agreements: What type of agreement does the TSO have (e.g. …)

Q 11. Are there any written **regulations** regarding **cyber security in national infrastructure** (whether or not they are specific to nuclear facilities)?
If so, specify details (links or references to regulations are welcome).
11.1. By whom are such regulations written/controlled? When were they implemented and enforced?
11.2. Characterize the status of their implementation in the nuclear sector:
  11.2.1. Have the regulations been published?
  11.2.2. Are the regulations supported by guidance?
  11.2.3. Have the regulations been implemented in most facilities?
  11.2.4. Are the regulations enforced?
  11.2.5. Are the regulations periodically assessed?

Q 12. Are there any written regulations regarding **cyber security in nuclear facilities**?
12.1. If yes, written/controlled by whom? When were they created? Details?
12.2. Characterize the status of their implementation:
  12.2.1. Have the regulations been published?
  12.2.2. Are the regulations supported by guidance?
  12.2.3. Have the regulations been implemented in most facilities?
  12.2.4. Are the regulations enforced?
  12.2.5. Are the regulations periodically reviewed?
12.3. Is the connection with regulations written for cyber security in non-nuclear sectors, if any, documented?

Q 13. Do existing regulations cover the following aspects of cyber security within nuclear facilities:
13.1. Development and review of a **Cyber security Plan**?
13.2. Identification of critical **digital assets**?
13.3. Analysis of **cyber threats**?
13.4. Protection of **computer systems** against cyber threats?
13.5. Protection of **Instrumentation and Control (I&C) and Safety systems** against cyber threats?

13.6. Protection of **Physical Protection Systems (PPS)** against cyber threats?
13.7. Protection of **Nuclear Material Accountancy and Control** (**NMAC**) **Systems** against cyber threats?
13.8. Use of **defence-in-depth** approach?
13.9. Cyber security evaluation of individual **components**?
13.10. Cyber security in the **supply chain** of (critical) digital assets?
13.11. Implementation of **cyber security incident response**?
13.12. Cyber security **awareness/training**?
13.13. Cyber security **assessment**?
13.14. Please add any additional aspects of cyber security covered by regulations:

Q 14. Have facilities' existing security plans been **updated** following the introduction of **cyber security regulations**?
14.1. Was the update **enforced/compulsory**?

Q 15. Is cyber security **explicitly cross-referenced** in (other) existing regulations covering:
15.1. Safety?
15.2. Physical protection?
15.3. Nuclear material accountancy and control?

Q 16. Do the various licensing processes for nuclear facilities contain explicit considerations for cyber security?
16.1. Is cyber security part of the **design process** of a nuclear facility?
16.2. Is licensing contingent on the development of a **cyber security plan**?
16.3. Is licensing contingent on performance of a **cyber security assessment**?
16.4. Are **standards** required/referenced?
16.5. Does it require people to be **trained** in cyber security?

Q 17. Does the certification process for **individual systems (hardware/software)** explicitly address cyber security considerations?
If so, for which systems:
17.1. Systems relevant to **safety**?
17.2. Systems relevant to **security**?
17.3. Systems relevant to **Nuclear Material Accountancy and Control**?
17.4. **Business** systems?

Q 18. Is a national competent authority designated to **conduct cyber threat assessment** for nuclear facilities?
18.1. Do the assessments receive the input of **national intelligence**?
18.2. Are these assessments made available to the facilities?
18.2.1. If so, how is threat information communicated to the facilities?
18.3. Does the State utilize a **Design Basis Threat** (**DBT**) for its nuclear facilities?
18.3.1. If so, are cyber threats incorporated into the **DBT** as an integrated component or as a separate **cyber-DBT**?

Q 19. Does the competent authority provide or facilitate **training** on cyber security issues?
19.1. For its own staff? Inspectors?
19.2. For operators?
19.3. What is the focus of training?

Are the following topics covered?

19.4. Regulatory compliance?
19.5. Generic cyber security?
19.6. Incident response?
19.7. Cyber security of Instrumentation and Control (I&C) systems?

Q 20. Does the competent authority conduct regular **inspections** focusing on cyber security issues?
20.1. What is the nature and scope of the inspections?
20.2. Which methodology is used for the inspections? (E.g. performance-based, compliance-based…)?
20.3. What are the competencies of the people conducting the inspections (e.g., training, education, or certification)?
20.4. How often are they conducted? What is their duration?
20.5. Must the facilities also perform self-assessments or performance tests?

Q 21. Is the **nuclear supply chain** regulated/controlled?
21.1. If so, are the **cyber security elements** of the supply chain explicitly regulated?

Q 22. Does the competent authority conduct **vetting** or **trustworthiness checks** for individuals or third parties accessing or managing sensitive digital systems (I&C systems, computers…)?

Q 23. Is there any compulsory training on cyber security for individuals or third parties accessing or managing sensitive digital systems?
23.1. If so, please describe the mandatory requirements (i.e. training name, duration, and periodicity).

Q 24. How is the cyber security of activities **outside the nuclear sector** (but relevant to nuclear security) regulated (e.g. import/export of technology, legal activities, etc)?
24.1. In particular for **law enforcement** activities?

Q 25. Does your country have any national educational program on **nuclear security**?
If so, are these:
25.1. University degrees
25.2. Certifications
25.3. Trainings
25.4. Others

Q 26. Does your country have any national educational programs on **IT and/or Cyber security**?
If so, are these:
26.1. University degrees
26.2. Certificates
26.3. Trainings
26.4. Others

Q 27. Does your country have any national educational programs for **nuclear IT and/or Cyber security**?
If so, are these:
27.1. University degrees
27.2. Certificates
27.3. Trainings

27.4. Others

If not:

27.5. Are there **plans** to establish one?

27.6. Which area of education would be affected?

Do/would these educational programs follow relevant specifications from:

27.7. National bodies?

27.8. International bodies?

27.9. If so, which ones (i.e. Regulator, ISO, IAEA)?

11 Appendix 2 – List of Abbreviations

AHGNS	Ad Hoc Group on Nuclear Security
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	Design Basis Threat
EC	European Commission
ENSREG	European Nuclear Safety Regulators Group
EU	European Union
IAEA	International Atomic Energy Agency
IC	instrumentation and control
ICT	information and communication technology
IS	information systems
ISS	Institute for Security and Safety at the Brandenburg University of Applied Sciences
NMAC	nuclear material accounting and control
NPP	nuclear power plants
NTI	Nuclear Threat Initiative
WINS	World Institute of Nuclear Security

12 References

[1] International Atomic Energy Agency; Computer Security at Nuclear Facilities; IAEA Nuclear Security Series 17, 2011

[2] Several publications available, e.g.: World Institute of Nuclear Security; Security of IT and IC Systems at Nuclear Facilities; 2014

[3] ANSI/ISA–99.00.01–2007; Security for Industrial Automation and Control Systems; 2007

[4] Nuclear-Security – Measures to protect Against Nuclear Terrorism, Amendment to the Convention on the Physical protection of Nuclear Material (2005) GOV/INF/2005/10-GC(49)/INF/6, IAEA Board of Governors General Conference. WWW: http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf

[5] Nuclear Energy Act (1999) Act No. 46 of 1999, NEA. WWW: http://www.energy.gov.za/files/policies/act_nuclear_46_1999.pdf

National Nuclear Regulatory Act (1999) Act No.47 of 1999, NNRA. WWW: http://www.energy.gov.za/files/policies/act_nuclear_47_1999.pdf

Other regulations:

National Radioactive Waste Management Bill – Notice No. 654 of 2008

Nuclear Energy Policy (2008)

Radioactive Waste Management Policy and Strategy (2005)

Act 53 of 2008 National Radioactive Waste Disposal Institute

Promotion of Access to Information Act 2 of 2000

South Africa Government Gazette 8755 – Safety Standards R388 28 April 2010

National Key Points Act (No.102 of 1980) amended in 1985 as Act No.47

National Strategic Intelligence Act (No.39 of 1994)

Disaster Management Act, 2002, (Act 57 of 2002);

Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004)

[6] An Act to amend the Atomic Energy Act of 1946, as amended, and for other purposes (1954) The 83th United States Congress. WWW: http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf# page=23 (pages 7-228). Also known as Atomic Energy Act of 1954

National Nuclear Security Administration Act; 2010

[7] Act on the peaceful utilization of atomic energy and the protection against its hazards (Atomic Energy Act) (1959) Bundestag, AtG. WWW: http://www.gesetze-im-internet.de/bundesrecht/atg/gesamt.pdf

[8] There are two Government Decrees that establish fundamental requirements to physical protection (PP) of nuclear materials and nuclear facilities and control and accounting (MC&A) of nuclear materials. These Decrees are:

Regulation on the State System for Nuclear Material Accounting and Control. Enacted by the Government Decree #352 of May 6, 2008. Rules of the Physical Protection of Nuclear Material, Nuclear Facilities

Nuclear Material Storage Points. Enacted by the Government Decree #456 of July 19, 2007.

[9] Verordnung über die Gewährleistung von Atomsicherheit und Strahlenschutz (1984) AtStrlSV. WWW. http://www.gesetze-im-internet.de/bundesrecht/atstrlsv/gesamt.pdf

[10] Two Government Decrees that establish fundamental requirements to physical protection (PP) of nuclear materials and nuclear facilities and control and accounting (MC&A) of nuclear materials, establish general requirement to protect PP and MC&A information that can be classified as secret or official use only (OUO). This general requirement drives applicability of a set of legislation that is external to nuclear security, but applies to nuclear security as well, and covers protection of information in computer systems.

Government Decree on PP also considers information protection equipment as component of physical protection system. PP equipment that handles secret or OUO information is subject to mandatory certification.

[11] Electronic Communications and Transactions Act (2002) Act No. 25 of 2002, ECT. WWW: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/South%20Africa/ElecComm.PDF

COMSEC Act (2003)

Minimum Information Security Standards (MISS) (1996). WWW: http://www.kzneducation.gov.za/LinkClick.aspx?fileticket=aDNwzVuiANQ%3D&...

[12] Protection of secret or OUO information is governed by the:

Federal Law "On State Secret" and

Federal Law "On Information, Information Technologies and Information Protection." (2006) Duma, No. 149-FZ. WWW: http://old.svobodainfo.org/en/node/441

Draft Law "On Security of Critical Information Infrastructure of Russian Federation" that would cover protection of industrial control systems has been developed by the Federal Security Service (FSB), but has not yet submitted for consideration in Russian legislative body.

Abovementioned laws apply to multiple domains, including nuclear security, but nuclear security is not explicitly referenced in these laws.

[13] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (2009) Bundestag. WWW: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.pdf?__blob= publicationFile

[14] Information Security Doctrine of the Russian Federation (2000) Pr-1898. WWW: http://www.scrf.gov.ru/documents/6/5.html

Main Directions of the State Policy in the Area of Ensuring Security of Automated Control systems for Industrial and Technology Processes at Russian Federation Critical Infrastructure Objects (2012) Approved by the President. WWW: http://www.scrf.gov.ru/documents/6/113.html

[15] IT-Grundschutz, BSI. WWW: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Cyber-Sicherheitsstrategie für Deutschland (2011) BMI. WWW: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf;jsessionid=A894A62800C80EAFD386F0FFFD0D6976.2_cid364?__blob=publicationFile

[16] Executive Order -- Improving Critical Infrastructure Cybersecurity (2013) The White House. WWW: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Also known as Executive Order 13636

Presidential Policy Directive -- Critical Infrastructure Security and Resilience (2013) The White House. WWW: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Presidential Policy Directive 21

Framework for Improving Critical Infrastructure Cybersecurity (2014) National Institute of Standards and Technology. WWW: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. Also known as NIST Framework 2/12/14

[17] Resolutions of Maintaining Computer Network Security (2000) The National People's Congress. WWW: http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content_5131101.htm.

Criminal Law (revision 1997) mentions crimes of no-authorized access to /or sabotage computer information system. However, they all have no provisions specific to nuclear security

[18] National Cyber Security Policy Framework ([4] NCSPF, 05/2011) WWW: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/docs/100219cybersecurity.pdf

[19] Ministry of Industry and Information Technology [2011] Strengthening Industrial Control System(ICS) Information Security Management (in Chinese), WWW: http://www.miit.gov.cn/n11293472/n11293832/n12843926/n13917012/14294613.html

[20] The US has cyber security regulations specific to power grids and utility published by FERC/NERC

[21] Regulations applicable to industrial control systems:

Requirements to protection of information in automated systems of control of industrial and technology processes at critically important sites, potentially hazardous sites, as well as objects constituting increased hazard for life and health of people and for environment. Approved by FSTEC Order #31 of March 14, 2014.

Regulations applicable to industrial control systems and IT systems:

Basic Model of Information Security Threats in Key Systems of Information Infrastructure. Issued by FSTEC on May 18, 2007.

Methodology for Defining Actual Information Security Threats in Key Systems of Information Infrastructure. Issued by FSTEC on May 18, 2007.

General Requirements for Ensuring Information Security in Key Systems of Information Infrastructure. Issued by FSTEC on May 18, 2007.

Recommendations on Ensuring Information Security in Key Systems of Information Infrastructure. Issued by FSTEC on November 19, 2007.

Regulation on the Registry of Key Systems of Information Infrastructure. Issued by FSTEC Order #74 on March 4, 2009.

National Standard GOST RO 0043-002-2012 Ensuring Information Protection in Key Systems of Information Infrastructure. System of Documents.

[22] Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (2009) BMI. WWW: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Nat-Strategie-Kritis_PDF.pdf?__blob=publicationFile

[23] Regulation PRC Computer Information System Security Protection Regulations (1994), but no specific mention on "national infrastructure" and "nuclear facilities".

[24] Electronic Communications and Transactions Act (2002) Act No. 25 of 2002, Department of communications: Director-General of the Department. Specifically see Chapter VI.

Information Regulator (ICASA) See chapter V of the PPIA 4 of 2013

[25] Regulations applicable to IT systems:

Requirements to protection of non-state secret information handled in state information systems. Approved by FSTEC Order #17 of February 11, 2013.

Requirements to protection of information handled in common use information systems. Approved by FSTEC Order #489 of August 31, 2010.

Regulation on attestation of information objects for compliance with information protection requirements. Approved by the Head of State Technical Commission (FSTEC predecessor) on November 25, 1994.

GOST R ISO/IEC 15408-2002 Security of information technologies. Criteria for evaluating security of information technologies.

Protection from unauthorized access to information. Part 1. Software for information protection tools. Classification based on the level of control of absence of undeclared capabilities. Approved by the Order #114 of the Head of State Technical Commission (FSTEC predecessor) of June 4, 1999.

Computer technology equipment. Firewalls. Protection from unauthorized access to information. Indicators of protection from unauthorized access to information. Approved by the Order of the Head of State Technical Commission (FSTEC predecessor) of July 25, 1997.

Automated systems. Protection from unauthorized access to information. Automated systems categorization and requirements to information protection. Approved by the Order of the Head of State Technical Commission (FSTEC predecessor) of March 30, 1992.

Computer technology equipment. Protection from unauthorized access to information. Indicators of protection from unauthorized access to information. Approved by the Order of the Head of State Technical Commission (FSTEC predecessor) of March 30, 1992.

Protection from unauthorized access to information. Terms and definitions. Approved by the Order of the Head of State Technical Commission (FSTEC predecessor) of March 30, 1992.

Concept of protection of computer technology equipment and automated systems from unauthorized access to information. Approved by the Order of the Head of State Technical Commission (FSTEC predecessor) of March 30, 1992.

Guidelines

Information protection measures in state information systems. Approved by FSTEC on February 11, 2014 to support implementation of FSTEC Order #17.

[26] Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT), 2012, RS-H 3-99, classified information VS-NfD, 2012

[27] U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations (2009) NRC, Final Rule in 2009, specifically see: § 73.54 Protection of digital computer and communication systems and networks (10 C.F.R. 73.54). WWW: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html