INTERWEAVING BETWEEN THE CYBER AND PHYSICAL DOMAINS IN THE THREAT ANALYSIS FOR NUCLEAR SITES

Tudor RĂDULESCU, PhD candidate*

Abstract: *In this paper we overview the threat analysis process in the fields of physical and cyber security, as part of the requirements preparation for the implementation of security measures in nuclear sites. We highlight the essential characteristics of capability, motivation and intent, used as criteria in qualifying the threats. We analyse the interweaving between the two domains and the dynamic aspects of the threat.*

Keywords: *threats; physical security; cyber security; nuclear; design basis threat.*

Introduction

The concepts of physical and cyber security had, until a few years ago, separate paths. The idea of correlation between the two domains appeared only after the events that showed, on one hand, the credibility of the cybernetic risk and, on the other hand, an interdependence between the two domains, created by the infusion of digital technology in the area of industrial processes of physical nature.

In time, the concept of cyber-physical systems emerged, representing "integrations of computation and physical processes"[1]. These build on the flexibility of digital systems to create, measure, and control functions of physical systems in ways that did not seem possible through the analogue technology.

Along with the systems' evolution, the introduction of the cyber component created new vulnerabilities, exploitable by malevolent actors. Thus, a new range of threats appeared on the table of security specialists.

This paper does not approach the natural factors and the systems' intrinsic technological factors, as components of the general threat towards the system. In the nuclear field, these are included in the systems safety domain.

[1] Edward A. Lee, *Cyber Physical Systems: Design Challenges*, in 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4519604, accessed 30.05.2015, p. 3.

"Carol I" National Defence University
t.radulescu@gmail.com

Physical threats analysis

Physical security, also known in the nuclear field as physical protection, is the field that addresses the measures required for lowering, to an acceptable level, the risks of physical action, based on a malevolent intent, with potential unacceptable consequences, as uncontrolled radioactivity release in the environment.

To be able to dimension and design technical systems and organizational measures that will ensure the physical security, it is necessary to obtain information about the maximum credible attack which the nuclear site's defence system must withstand. In order to meet this requirement, the United States Nuclear Regulatory Commission (NRC) introduced, in 1979, the concept of Design Basis Threat (DBT).

The Design Basis Threat is a document that describes the types of attack the site must be protected against, with data on the capabilities of the attack force, its tools, the level of competence in various fields, as well as the intended purpose (sabotage, nuclear material theft).

The DBT model was adopted by other states, with the support of professionals at the IAEA (International Atomic Energy Agency in Vienna). Thus, both in the best practices courses organized by the IAEA and during the IPPAS (International Physical Protection Advisory Service) support missions, the experts recommend that the implementation of security measures be based on the DBT document.

The Design Basis Threat can be developed with applicability for one nuclear facility or for an

entire category of sites in a country. The analysis is done at the state level, since the structures involved both in drafting the document and in the response to a security event are at the national level; most of them part of the national defence system). This is stipulated in the Amendment to the Convention on the Physical Protection of Nuclear Material[2], among the fundamental principles.

In 2009, the IAEA published a guide for the development and maintenance of DBT, entitled "Development, Use and Maintenance of the Design Basis Threat"[3]. This guide specifies the state's role by suggesting the existence of, and the need to establish, a clear demarcation of responsibility for the response, depending on the characteristics of the threat:

For the development of the DBT, one of the essential steps is the threat assessment. According to the guidance, the assessment process includes gathering input data, their analysis and drafting the document.

The input data for the analysis are provided through a joint effort of all state structures with responsibilities in intelligence and incident response. The structures involved in this process can include: state's internal and external intelligence services, structures of the Ministry of Interior and Ministry of Defence, Ministry of Transport, Ministry of Environment, organizations specialized in emergency response, structures that ensure government communications and their security.

The intelligence process is based on all the types of information sources and aims to determine:

- security events that occurred on the state's territory and in other states with similar characteristics (e.g. attacks on nuclear targets, on critical infrastructure elements, theft of weapons or explosives, breaches of airport security, border crossing attempts by members of the extremist groups);
- proven or credible attack capabilities exhibited by various factors (e.g. based on information on procurement of technology or on recruitment of members with specific skills);
- elements that could facilitate an attack (e.g. the existence, in the vicinity of the protected sites, of explosives warehouses or chemical plants);

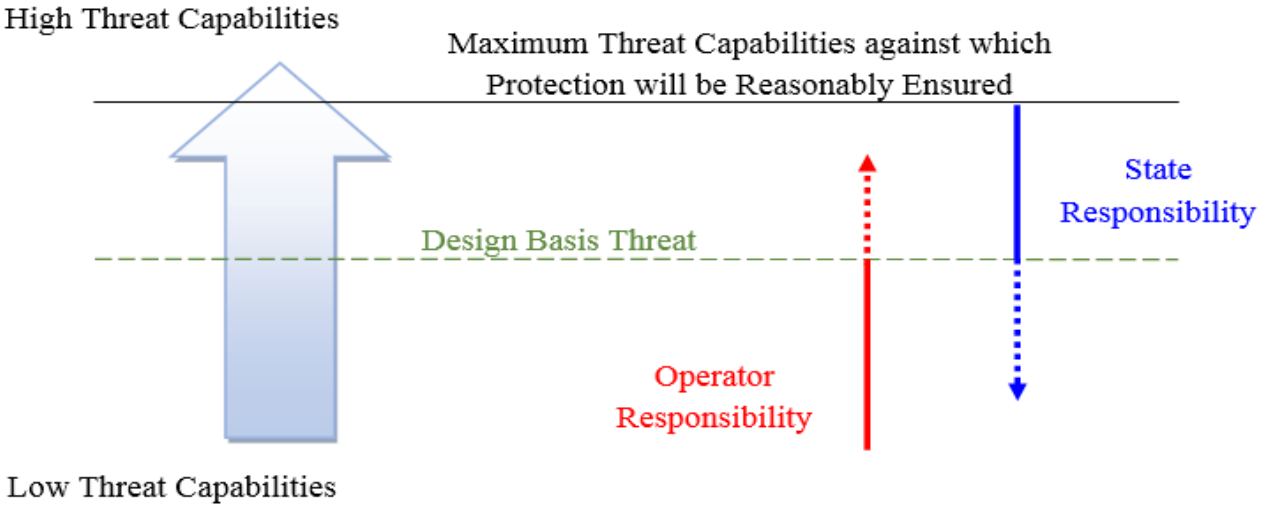

Figure no. 1 - Roles and responsibilities for protecting against threats

- insider threat elements.

After the data collection is completed, the next process is the analysis to "identify and document the credible motives, intentions and capabilities of the potential threats."[4] The guide specifies[5] a number of features of the physical threats that must be documented and taken into account for the assessment:

- motivation;
- willingness to put one's own life at risk;
- intentions;
- group size;
- available weapons;

[2] IAEA, *Amendment to the Convention on the Physical Protection of Nuclear Material*, IAEA, 2005, http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf, accessed 30.05.2015.

[3] IAEA, *Development, Use and Maintenance of the Design Basis Threat*, 2009, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, accessed 30.05.2015.

[4] IAEA, *Development, Use and Maintenance of the Design Basis Threat*, 2009, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, accessed 30.05.2015, p. 15.

[5] *Ibidem*, p. 16.

- types and quantity of explosives;
- tools and equipment;
- means of transportation;
- technical skills;
- cyber skills;
- level of knowledge and information on the site;
- financial support;
- possible insider support;
- support from other organizations;
- attack tactics.

During the assessment, threats, for which there are no credible capabilities or for which either intention or motivation are missing, are discarded.

The list of remaining candidate threats is transformed, after the analysis, into a synthetic description of the maximum credible attack, which will be the basis in dimensioning technical systems, organizational measures and the response force.

In situations where the operator and the relevant national regulator agree on this, the operator can use a graded approach to apply security measures proportionally with the attractiveness and specific vulnerabilities of the target. For example, a low-level radioactive waste repository is much less attractive, because of the relatively low consequences of the theft of materials, compared with enriched nuclear fuel storage.

Since the information supporting the analysis is valid at the time of collection and threats evolve over time, best practices require a cyclical process of reassessment of DBT with a period of 1 year or whenever an event that brings major changes in threat perception (capabilities, motivations, intentions) occurs.

Considering that the sources of information used in drafting the DBT may be classified, and the fact that disclosure of the information, which formed the basis to the response structures design, in the public space can create prerequisites for preparing a successful attack, DBT documents are protected by classification.

Analysis of cyber threats

Cybersecurity focuses on measures needed to ensure an acceptable level of confidentiality, integrity and availability of protected system's elements. Most events analyzed in detail in literature and in the media consist of breaches of confidentiality and availability. The report, presented to the United States Senate Armed Services Committee in February 2015, stated that it is expected to "see more cyber operations that will change or manipulate electronic information in order to compromise its integrity"[6].

As a general approach, the concept of threat does not exist in the absence of concepts of vulnerability and potential consequence. Therefore, in many cases, threat analysis is limited, in practice, to the analysis of system vulnerabilities, addressing the premise that there is capability, intention and motivation for a possible attack.

In the nuclear field, we found no structured, industry-specific, approach regarding threat analysis.

The ISO 27000 family of standards, which is used by many operators for information security management processes, specify the responsibility of the organization to identify "the threats to resources"[7].

Given the importance of nuclear facilities in the light of the potential consequences of a security incident, operators receive support from regulators and governmental structures. In Romania, the Norm regarding the Protection of Nuclear Installations against Cyber Threats, issued in 2014, states that "cyber threats to be taken into account by the licensee shall be established by CNCAN in cooperation with the national authority for cyber security"[8], which is defined as the CyberInt National Centre.

Other potential sources of information for cyber threats analysis are the CERT structures, government or private. Analysing the Report on Cyber Security Alerts issued by CERT RO[9], we see that there is no structured information to characterize the threat, but rather a mix of vulnerabilities and incidents without specific data analysis to identify the origin or intention, motivation and capabilities. There are, though, private companies offering

[6] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf, accessed 30.05.2015, p. 3.

[7] SR ISO/CEI 27001 - *Tehnologia informatiei, Tehnici de securitate, Sisteme de management al securitatii informatiei - Cerinte*, 2006, p. 12.

[8] CNCAN, *Norma privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice*, p. 2.

[9] CERT RO, *RAPORT cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2014*, 2015, http://www.cert-ro.eu/files/doc/915_20150325000331012990800_X.pdf, accessed 30.05.2015.

"threat intelligence"[10],[11] services.

We see thus that the analysis of cyber threats is addressed as a niche problem, the team participating in defining the threats being more limited than in the case of physical threats. It is possible that the delegation of this process to a specialized centre is a result of specialists shortages in other structures, this being one of the symptoms of the outstanding dynamics of the information technology.

The cyber security domain is characterized by a much wider dynamic of vulnerabilities compared to the physical security domain. First, information systems development cycle is very short. Updates to the operating systems and applications are released sometimes on a weekly basis, and new major versions of applications are launched every year. These things involve a potential of creating new vulnerabilities with every version, while patching previous vulnerabilities. Secondly, Moore's Law[12] suggests a doubling of the processing power of information in digital systems every two years. This means a great dynamic of the capabilities that characterize the threat.

In recent years, there have been more and more discussions on the Advanced Persistent Threat (APT). This refers to sophisticated offensive campaigns prepared by groups with high levels of resources and skills, with the potential involvement of state actors. Hutchins[13] proposes an analogy to characterize a cyber attack cycle, based on the mechanisms of combat "kill chain" with the following steps:

- reconnaissance;
- weaponization;
- delivery;
- exploitation;
- installation;
- command and control;
- actions on objectives.

APT type campaigns take place over several months, even years. The cited article emphasizes the importance of real-time attacks tracking and correlation of information, to enable early detection. The author shows that "defender's objective is less to positively attribute the identity of the intruders than to evaluate their capabilities, doctrine, objectives and limitations"[14].

Correlation and differences between the physical and cyber domains

Looking at the physical threat analysis approach, we note that there is a reduced dynamic of mechanisms employed by the potential attackers, changes in the Design Basis Threat being rather dictated by the motivations and intention areas. The evolution of the threat is dictated more by political and social issues.

In the area of cyber threats there is a significant technological dynamic. The definition of the threat has a predictable component, with a definition similar to the Design Basis Threat, updated annually. On the other hand, there is an unpredictable component, characterized by threats for which there are currently no available means of detection.

For both areas the interest remains in the basic elements of the threat: motivation, intention and capability.

If in the case of physical security the analysis is based on the classic intelligence component, using a real-time monitoring mechanism for detecting APT can provide information about threat elements between DBT reviews.

If we consider the context of the widespread use of digital technologies in physical protection systems, interdependencies between physical and cyber domains manifest by creating vulnerabilities that can be exploited through blended attacks. Such attacks could be targeted at computer systems used in the operation of the physical protection systems.

There are also recent elements of technology, at the boundary between the physical and cyber domains, suggesting the need for unification in threat analysis. Digital technologies, recently appeared on the market, as software defined radio systems, create attack capabilities considered unrealistic 10 years ago, allowing, for example, hacking or blocking the communication systems of response forces.

[10] *Dell SecureWorks Counter Threat Unit*, http://www.secureworks.com/cyber-threat-intelligence/, accessed 30.05.2015

[11] *iSightPartners ThreatScape*, http://www.isightpartners.com/products/threatscape/, accessed 30.05.2015.

[12] G E Moore, *Cramming more components onto integrated circuits* (Reprinted from Electronics, pp. 114-117, April 19, 1965), Proceedings Of The IEEE 86, 1 (1998).

[13] Eric M. Hutchins et al., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, 6th Annual International Conference on Information Warfare and Security July 2005 (2011), http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, accessed 30.05.2015, pp. 4-5.

[14] G E Moore, *Cramming more components onto integrated circuits* (Reprinted from Electronics, pp. 114-117, April 19, 1965), Proceedings Of The IEEE 86, 1 (1998), p. 7.

Another disruptive technology is the 3D scanning and printing. In addition to the potential use for creating weapons, the technology can be used to create biometric models ("fingerprint phantoms"[15]).

Conclusions

As the interweaving between the physical and cyber domains creates interdependencies and correlations regarding threats and vulnerabilities, we consider that threat analysis should be conducted in a correlated manner.

Although the dynamic of the threat evolution is high, the long implementation cycle of the technical measures and the service life of implemented systems dictate the need, in the drafting of the Design Basis Threat, to use a conservative approach and a strategic analysis, for the capabilities prediction to cover a minimum of 5 years.

In this paper we did not consider the insider threat, given its special, unstructured nature. The literature mentions, in analyses, the insider threat as an additional factor and facilitator for an attack initiated from the outside[16]. The insider threat, coming from people with legitimate access to the systems, is a threat with potential major impact. Insider threat is at the same time, "difficult to measure"[17], with no modelling tools at the same level as the ones for the outside attacks. We will approach the insider threat analysis in future works.

[15] Sunpreet S. Arora et al., *3D Fingerprint Phantoms*, 2013, http://www.cse.msu.edu/rgroups/biometrics/Publications/Fingerprint/Aroraetal_MSUTechReportMSU-CSE-13-12.pdf, accessed 30.05.2015, p. 1.

[16] IAEA, *Development, Use and Maintenance of the Design Basis Threat*, 2009, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, accessed 30.05.2015.

[17] R. Chinchani et al., *Towards a theory of insider threat assessment*, 2005 International Conference on Dependable Systems and Networks (DSN'05) (2005), p. 1.

ACKNOWLEDGEMENTS

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number **POSDRU/159/1.5/S/138822** with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers – "SmartSPODAS"."***

BIBLIOGRAPHY

1. Arora, Sunpreet S.ș Cao, Kaiș Jain, Anil K., *3D Fingerprint Phantoms*, 2013, http://www.cse.msu.edu/rgroups/biometrics/Publications/Fingerprint/Aroraetal_MSUTechReportMSU-CSE-13-12.pdf, accessed 30.05.2015.
2. CERT RO, *RAPORT cu privire la alertele de securitate cibernetica procesate de CERT-RO in anul 2014*, 2015, http://www.cert-ro.eu/files/doc/915_20150325000331012990800_X.pdf, accessed 30.05.2015.
3. Chinchani, R.; Iyer, A.; Ngo, H.Q.; Upadhyaya, S., *Towards a theory of insider threat assessment*, 2005 International Conference on Dependable Systems and Networks (DSN'05) (2005).
4. Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community*, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf, accessed 30.05.2015.
5. CNCAN, *Norma privind protecția instalațiilor nucleare împotriva amenințărilor cibernetice*
6. Hutchins, Eric M., Cloppert, Michael J., Amin, Rohan M. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, 6th Annual International Conference on Information Warfare and Security July 2005 (2011), pp. 1-14, http://www.lockheedmartin.com/

content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, accessed 30.05.2015.

7. IAEA, *Amendment to the Convention on the Physical Protection of Nuclear Material*, IAEA, 2005, http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf, accessed 30.05.2015.
8. IAEA, *Development, Use and Maintenance of the Design Basis Threat*, 2009, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf, accessed 30.05.2015.
9. Lee, Edward A., *Cyber Physical Systems: Design Challenges*, in 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008, pp. 363-369, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4519604, accessed 30.05.2015.
10. Moore, G E, *Cramming more components onto integrated circuits* (Reprinted from Electronics, pg 114-117, April 19, 1965), Proceedings of the IEEE 86, 1 (1998), pp. 82-85.
11. *SR ISO/CEI 27001 - Tehnologia informației, Tehnici de securitate, Sisteme de management al securității informației - Cerințe*, 2006.
12. *Dell SecureWorks Counter Threat Unit*, http://www.secureworks.com/cyber-threat-intelligence/, accessed 30.05.2015.
13. *iSightPartners ThreatScape*, http://www.isightpartners.com/products/threatscape/, accessed 30.05.2015.