Elżbieta Hodyr*

Cybersecurity of nuclear weapon systems

Abstract

In my article, I would like to describe the history of cybersecurity related to nuclear safety, to answer the question of what cybersecurity is and how the development of cybersecurity was related to the development of nuclear safety and nuclear systems. Continuing, I will also describe the cyber risks associated with nuclear systems. I would also like to try to make recommendations for cybersecurity related to nuclear safety. I would also like to try to make recommendations for cybersecurity related to nuclear safety.

Key words: cybersecurity, nuclear weapon systems, cyber risks

* Elżbieta Hodyr, Ph.D. student, War Studies University in Warsaw, e-mail: ehodyr@gmail.com, ORCID: 0000-0001-5045-093X.

In the beginning, what is cybersecurity? Cybersecurity comprises three planes of study: 1) operations adress the day-to day functioning of the information security tasks. Operational issues inclued staffing, implementation of policies and procedures, incident response, business continuity, disaster recovery, systems management, tool acquisition and deployment, investigations and more; 2) governence function includes the development of organizational structure and command chain that oversees, manages and handles information and information systems. Governence include the development of policies and procedures that drive the operational aspects, the laws and policies that set the societal expectations of individual and organization activities. Categories of law include crimnal law (statutes guiding actions that are deemed to threaten harm public safety or welfare), civil law and administrative law; 3) training refers to teaching indivduals specific skills and competencies that are usually task – or project-oriented[1].

According to the US approach cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communictions systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster[2].

Continuing how cybersecurity is related to nuclear energy systems. Cyber challenge to nuclear security involves both inherent vulnerabilities in nuclear systems as well as the threat from actors seeking to gain access to these systems in order to alter, disable, disrupt or damage them. Finally, perhaps the key components of cyber are humans: it is people that design systems, write software and place their faith in computers and machines to carry out tasks as intended[3].

Nuclear weapons systems were first developed at a time when computer capabilities were in their beginning and little consideration was given to potential malicious cyber vulnerabilities. The nuclear weapons system can be infiltrated without the knowledge of the state. Why is this happening? This is

1 E. Hodyr, *Cybersecurity – new challenges in international law*, „Journal of Polish-American Science and Technology" 2016, vol. 10.

2 Ibidem.

3 B. Tertrais, *The Unexpected Risk: the Impact of Political Crises On the Security and Control of Nuclear Weapons* w: *Nuclear Weapons Security Crises: What Does History Teach?*, eds. H. Sokolski, B. Tertrais, Carlisle, PA 2013.

through the existence of security gaps and pathways, as well as through design gaps and supply chain vulnerabilities. The following cyber attack methods should also be mentioned: 1) data manipulation; 2) digital jamming; 3) cyber spoofing.

They could jeopardize the integrity of communication, leading to increased uncertainty in decision making. The making of military decisions, and in particular those related to the policy of deterrence related to nuclear weapons, was influenced by unknowns related to the cybersecurity management system, e.g. in time of peace. I mean defensive cyber activities.

Cyber attacks on nuclear weapons systems can cause escalation, and this can result in the use of weapons. Inadvertent nuclear firing can result from reliance on false information and data, and this, as mentioned earlier, affects decision making.

It is the responsibility of nuclear weapons states to incorporate cyber risk reduction measures in nuclear command, control and communication systems.

Cyber risks in nuclear weapons systems have thus far received scant attention from the nuclear weapons policy community. The potential impacts of a cyberattack on nuclear weapons systems are enormous. It should be mentioned here. Data hacks could reveal sensitive information on facilities' layouts, personnel details, and design and operational information. Cyber interference could destroy industrial control systems within delivery platforms, such as submarines, causing them to malfunction. In addition, clandestine attacks could be conducted on targeting information or operational commands, which may not be discovered until the point of launch.

Continuing, communications as well as the transfer and storage of data are key targets for cyberattackers. United Nations Institute for Disarmament Research (UNIDIR) paper, the International Security Department at Chatham House identified several areas within nuclear weapons systems that could be potentially vulnerable to cyberattacks: 1) communications between command and control centres; 2) communications from command stations to missile platforms and missiles; 3) telemetry data from missiles to ground- and space-based command and control assets; 4) analytical centres for gathering and interpreting long-term and real-time intelligence; 5) cyber technologies in transport; 6) cyber technologies in laboratories and assembly facilities; 7) pre-launch targeting information for upload; 8) real-time targeting information from space-based systems including positional; 9) navigational and timing data from global navigational systems; 10) real-time weather information from space-, air-, and ground-based sensors; 11) positioning data for launch

platforms (e.g. submarines); 12) real-time targeting information from ground stations; 13) communications between allied command centres; 14) robotic autonomous systems within the strategic infrastructure.

Cyber risk analysis should also include the assessment of actor-specific threats. The biggest of these comes from other states attempting to neutralize their opponents' nuclear weapons systems through cyberattacks. Other actors include hackers, organized crime groups, lone-actors, and terrorist organizations. Although states currently possess the necessary capabilities and knowhow to conduct attacks on advanced strategic assets and industrial control systems, the higher degree of cooperation between hackers and organized crime groups has been identified as a growing concern[4].

Electronic warfare systems, including sensors receiving information that contributes to electronic signals intelligence and those that detect, identify and locate radio frequencies operating in a theatre, have periodically had to be upgraded to counter radar spoofing and deception techniques[5].

These technologies are not new and have been used since the Cold War. However, now the spoofing of digital information has to be added into the mix of signals intelligence spoofing and thus further complicates uncertainties.

I think it should be mentioned, that the organizational cultures in military services also pose inherent risks to mitigating cyberthreats in nuclear weapons systems. Military procurement programmes tend not to pay adequate consideration to emerging cyber risks – particularly in the supply chain – regardless of the government regulations for protecting data against cyberattacks.

Cyber intrusion may occur during the maintenance of strategic assets including nuclear weapons platforms such as submarines (for example, through digital equipment used to fix or test a system, such as backup power

4 For instance, in Sicily, in October 2000, a group of people with links to mafia families worked with an insider and created a digital clone of a bank's online system. The plan was to divert around $400 million that was for the regional projects in Sicily. In another incident, a group of drug smugglers, importing heroin from South America, worked with hackers to infiltrate the containers system in the port of Antwerp. For more information, see M. Glenny, *Organized crime finally embraces cyber theft*, „Financial Times" 2017, https://www.ft.com/content/a038cd98-0041-11e7-8d8e-a5e3738f9ae4 [dostęp: 20.08.2021]. See also P. Williams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, http://www.crime-research.org/library/Cybercrime.htm [dostęp: 20.08.2021].

5 J. Keller, *Navy continues buying radar-spoofing electronic warfare (EW) equipment from Mercury Systems*, „Military & Aerospace" 2017, http://www.militaryaerospace.com/articles/2017/06/radar-spoofing-electronic-warfare-ew.html [dostęp: 20.08.2021].

generators). Well-trained military personnel are able to identify potential cyber risks, but equally, staff without adequate cybersecurity knowledge and training may become targets of attacks. As a result, insufficient cybersecurity training actually raises the risk of cyberattacks by creating targets that are easy to exploit.

Hacking nuclear systems – such as command and control, critical assets, nuclear weapons facilities – was once believed to be an impossible task. Yet, history has shown that human error, system failures and design vulnerabilities are common occurrences in nuclear weapons systems[6].

Moreover, nuclear systems that function as they are intended to under normal circumstances may respond differently when under stress. States rely on the integrity of operational information provided through information technology (IT); if the information is unreliable, the decision maker's ability to respond accurately and effectively will also be compromised[7].

The role of nuclear weapons from a command, control and communications (C3) perspective is to serve as a key military asset for decision-makers, such as presidents and prime ministers, and such weapons can only be used with authorization from a decision-maker. The authorization can only be given once a reliability assessment of data has taken place. The confirmation of data readings signalling an event that may require a nuclear response must come from at least two independent sources (for example, radar and satellite systems)[8].

For example in the US, the Integrated Threat Warning/Attack Assessment (ITW/AA) structure – which provides strategic surveillance and information about attack warnings – has a variety of sensors to detect nuclear missile launches[9].

6 P. Lewis et al., *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*, http://www.theguardian.com/world/2014/apr/29/nuclear-accident-near-misses-report [dostęp: 27.08.2021].

7 A. Borning, *Computer System Reliability and Nuclear War*, „Communications of the ACM" 1987, no. 2, p. 112–131.

8 R. Halloran, *Nuclear Missiles: Warning System and the Question of When to Fire*, „New York Times" 1983, http://www.nytimes.com/1983/05/29/us/nuclear-missiles-warning-system-and-the-question-of-when-to-fire.html [dostęp: 20.08.2021].

9 *Cheyenne Mountain Complex*, https://fas.org/nuke/guide/usa/c3i/cmc.htm [dostęp: 20.08.2021].

The ITW/AA relies on key nodes, such as ground- and space-based assets, intelligence centres, weather support centres, space control centres and the missile warning centre[10].

The integrity of the ITW/AA is critical for receiving reliable communications, upon which decisions can be made. The ground-based systems, such as large-fixed radars, rely on electronic .beams, which leaves them open to manipulation through cyber means.

However, a space-based asset is more exposed to the risk of manipulation of its communication data[11].

Many aspects of nuclear weapons development and systems management are privatized in the US and in the UK, potentially introducing a number of private-sector supply chain vulnerabilities. Presently, this is a relatively ungoverned space and these vulnerabilities could serve to undermine the overall integrity of national nuclear weapons systems[12].

Private companies themselves are often under a constant state of cyberattack[13]. In 2010, for example, General Dynamics and Northrop Grumman were breached a number of times. In 2011 Lockheed Martin was the subject of a significant cyberattack[14].

I believe it is important to mention, that cyberattacks on private sector IT systems may result in the theft of nuclear weapons design information in order to sell or pass on to interested parties, including non-state actors. Protecting nuclear weapons design information requires training personnel in nuclear weapons facilities, including laboratories, cybersecurity measures, increasing awareness and best practice[15].

When nuclear weapons systems were first designed, there was no consideration of potential cyber vulnerabilities as computer capabilities were

10 Ibidem.

11 For more information on satellites and cybersecurity, see Livingstone and Lewis (2016), Space, the Final Frontier for Cybersecurity?

12 Each nuclear weapon possessor country has different plans for supply chain integrity. In some countries, such as the US, supply chain strategies are considered in risk management. Though it is unclear how well it is implemented or what measures other countries take.

13 A. Greenberg, *For Pentagon Contractors, Cyberspying Escalates*, „Forbes" 2010, https://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html [dostęp: 20.08.2021].

14 *US defence firm Lockheed Martin hit by cyber-attack*, 30 May 2011, http://www.bbc.co-.uk/news/world-us-canada 13587785 [dostęp: 20.08.2021].

15 *Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy*, Washington 1999, https://www.energy.gov/sites/prod/files/cioprod/documents/pfiab-doe.pdf [dostęp: 20.08.2021].

very limited. Cybersecurity measures, therefore, were not included in the development of the design structures. To mitigate risks, the US Department of Defense is currently applying a framework called Program Protection Plan, which is able to identify and manage risks to mission-critical systems[16].

While defence against cyber infiltrations is important, governments continue to develop offensive cyber techniques. Through cyber offensive campaigns, states are able to examine new weaknesses and backdoors that also help them reinforce their own cyber resilience. An ongoing dilemma for governments and militaries is to decide how much to invest in cyber defence and resilience and how much to spend on offensive cyber capabilities[17].

Computers and complex systems have always been central to nuclear C2 (command and control), and the need to manage and co-ordinate increasingly sophisticated and intricate weapons, sensors and war plans, was a principal driver of early computer technology.

But the many, and often competing, requirements of nuclear C2 have also meant that these systems have always contained certain vulnerabilities, and the past is littered with accidents and near misses – a reasonable proportion of which can be linked either directly or indirectly to computers and the inherent challenges of high-tech systems. In this way cyber threats are both exacerbating and recasting the intrinsic challenges of nuclear C2, security and strategy[18].

At the heart of nuclear command and control lies the always/never dilemma. Leaders want a high assurance that the weapons will always work when directed and a similar assurance the weapons will never be used in the absence of authorized direction.

Weapons must be reliable: unlikely to fail at the moment when leaders want to use them; safe: unlikely to detonate accidentally; and secure: resistant to efforts by unauthorized people to detonate them[19].

16 *Program Protection Plan: Outline & Guidance*, *Systems Engineering Version 1.0*, Washington 2011, http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf [dostęp: 20.08.2021].

17 See C. Baylon, *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, *Research Paper*, London, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf [dostęp: 20.08.2021].

18 For an interesting overview of how this developed in the US see K. Redmond, Th.M. Smith, *From Whirlwind to MITRE: The R&D Story of the SAGE Air Defense Computer*, Cambridge, MA 2000.

19 P. Feaver, *Command and Control in Emerging Nuclear Nations*, „International Security" 1992, no. 3, p. 163.

I think it's worth mentioning that, despite the huge amounts of money invested in developing high-tech protection mechanisms, nuclear control and safety systems appear to suffer from just the same kind of design bugs, implementation blunders and careless operations as any others[20].

Returning to the history of cybersecurity of nuclear systems, it is worth remembering that during 2003 and 2004, the industry was engaged in the development of guidance documents intended to support the uniform implementation of cyber security programs at power reactors. In July 2003, cyber security assessment pilots were completed at four U.S. nuclear power reactors. These pilots were designed to inform development of NUREG/CR-6847, „Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants". The project team consisted of representatives from the Pacific Northwest National Laboratory (PNNL), the NRC, and the CSTF. NUREG/CR-6847 was released in November 2004. In November 2005, NEI released NEI 04-04, „Cyber Security".

Program for Power Reactors, Revision 1. NEI 04-04 provides guidance on establishing and maintaining a cyber security program and incorporates assessment methodology described in NUREG/CR-6847. The NEI 04-04 program provides for the cyber security protection of all systems in the plant, including those necessary for reliable electrical generation. The guidance provides a risk-informed approach, in which consequences to plant functions are considered, and provides guidance on establishing a site cyber security defensive strategy incorporating multiple defensive layers with increasing levels of security protection. NEI 04-04 also provides guidance on incorporating cyber security considerations into the procurement process. The NEI 04-04 program includes the following steps: 1) define current cyber security program; 2) identify Critical Digital Assets (CDAs); 3) validate configuration; 4) assess susceptibility; 5) assess consequences; 6) determine risk; 7) refine defensive strategy; 8) continue program management[21].

The nuclear industry established a Nuclear Strategic Issues Advisory Committee (NSIAC) that has the ability to establish initiatives binding to all nuclear power plants. The NSIAC is comprised of the Chief Nuclear Officers of each power plant site or fleet. Approved NSIAC initiatives are implemented at all U.S. nuclear power plants. In April 2006, the NSIAC established an initiative

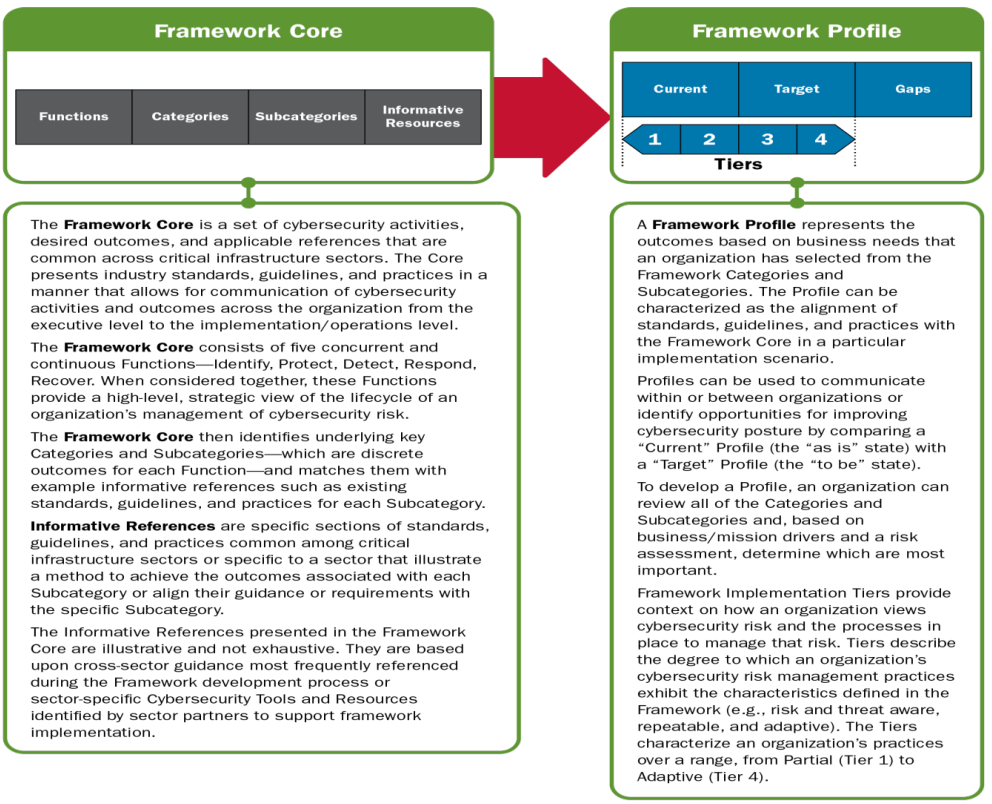
20 A. Ross, *Security Engineering: a Guide to Building Dependable Distributed Systems*, Indianapolis 2008.

21 Nuclear Sector Cybersecurity Framework Implementation Guidance US Department of Homeland Security; Cybersecurity and Infrastructure Security Agency.

requiring nuclear power plants to implement NEI 04-04 within two years. All U.S. plants implemented the initiative by May 2008.

Power plants are required by the NRC to design, implement, and evaluate their physical and cyber security programs to defend against a Design Basis Threat (DBT). In response to the increasing threat of cyber-related attacks, the NRC amended its DBT requirements in 2007 to include a cyberattack as an attribute of the adversary. The NRC describes a cyberattack as: "The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls"[22].

Below framework structure, which explain more how should cybersecurity in nuclear system works:



Picture: Nuclear Sector Cybersecurity Framework Implementation Guidance; US Department of Homeland Security; Cybersecurity and Infrastructure Security Agency.

22 Ibidem.

The Framework Core elements work together as follows. Functions organize basic cyber security activities at their highest level. They aid an organization in expressing its management of cyber security risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the effect of investments in cyber security. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services. The five Framework Core functions are: 1) identify: Develop an organizational understanding to manage the cyber security risks to systems, people, assets, data, and capabilities; 2) protect: Develop and implement appropriate safeguards to ensure delivery of critical services; 3) detect: Develop and implement appropriate activities to identify the occurrence of a cyber security event; 4) respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident; 5) recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident[23].

Closer coordination between national defence departments and the private sector will ensure that the most recent technology is used and that defence policies are in sync with cyber innovation. However, there is a contradiction in cooperating with the private sector. Although states need to limit their own cyber vulnerabilities, the existence of technical vulnerabilities could give them an advantage in future cyber offensive campaigns. In other words, national cyber agencies may prefer to be at the forefront of writing malicious codes and infiltrating industrial control systems, rather than openly sharing information about software vulnerabilities with manufacturers or users[24].

23 Ibidem.

24 B. Jopson, H. Kuchler, *US official defends NSA over Wanna Cry cyber attack*, „Financial Times" 2017, https://www.ft.com/content/74ae2600-39a3-11e7-ac89-b01cc67cfeec [dostęp: 20.08.2021]; T. Doscher, *In their own words – NORAD members recall September 11*, W. Glover, *Defence Video Imagery Distribution System (DVIDS)*, https://www.dvidshub.net/news/76668/their-own-words-norad-members-recall-september-11-william-glover [dostęp: 20.08.2021].

Bibliography

Baylon C., *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, *Research Paper*, London, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf [dostęp: 20.08.2021].

Borning A., *Computer System Reliability and Nuclear War*, „Communications of the ACM" 1987, no. 2.

Feaver P., *Command and Control in Emerging Nuclear Nations*, „International Security" 1992, no. 3.

Glenny M., *Organized crime finally embraces cyber theft*, „Financial Times" 2017, https://www.ft.com/content/a038cd98-0041-11e7-8d8e-a5e3738f9ae4 [dostęp: 20.08.2021].

Glover W., *Defence Video Imagery Distribution System (DVIDS)*, https://www.dvidshub.net/news/76668/their-own-words-norad-members-recall-september-11-william-glover [dostęp: 20.08.2021].

Greenberg A., *For Pentagon Contractors*, *Cyberspying Escalates*, „Forbes" 2010, https://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html [dostęp: 20.08.2021].

Halloran R., *Nuclear Missiles: Warning System and the Question of When to Fire*, „New York Times" 1983, http://www.nytimes.com/1983/05/29/us/nuclear-missiles-warning-system-and-the-question-of-when-to-fire.html [dostęp: 20.08.2021].

Hodyr E., *Cybersecurity – new challenges in international law*, „Journal of Polish-American Science and Technology" 2016, vol. 10.

Jopson B., Kuchler H., *US official defends NSA over Wanna Cry cyber attack*, „Financial Times" 2017, https://www.ft.com/content/74ae2600-39a3-11e7-ac89-b01cc67cfeec [dostęp: 20.08.2021].

Keller J., *Navy continues buying radar-spoofing electronic warfare (EW) equipment from Mercury Systems*, „Military & Aerospace" 2017, http://www.militaryaerospace.com/articles/2017/06/radar-spoofing-electronic-warfare-ew.html [dostęp: 20.08.2021].

Tertrais B., *The Unexpected Risk: the Impact of Political Crises On the Security and Control of Nuclear Weapons* [w:], *Nuclear Weapons Security Crises: What Does History Teach?*, eds. H. Sokolski, B. Tertrais, Carlisle, PA 2013.

Williams P., *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, http://www.crime-research.org/library/Cybercrime.htm [dostęp: 20.08.2021].

Cyberbezpieczeństwo systemów broni jądrowej

Streszczenie

Autorka artykułu analizuje historię cyberbezpieczeństwa związanego z bezpieczeństwem jądrowym. Odpowiada na pytanie, czym jest cyberbezpieczeństwo i jak jego rozwój był powiązany z rozwojem bezpieczeństwa jądrowego i systemów jądrowych. Opisała także cyberzagrożenia związane z systemami jądrowymi. W zakończeniu artykułu sformułowała rekomendacje dotyczące cyberbezpieczeństwa związanego z bezpieczeństwem jądrowym.

Słowa kluczowe: cyberbezpieczeństwo, systemy broni jądrowej, cyberzagrożenia