RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Taxonomy Of Attacks On Cyber-Physical Systems: Technological And Legal Aspects

By

Alexandra Yuryevna Bokovnya
Ph. D. in Law Faculty of Law, Department of Criminal Law Kazan Federal University Kazan, Russia (Russian Federation) e-mail: kafedra.ksu@yandex.ru ORCID: https://orcid.org/0000-0002-6395-0893

Ildar Rustamovich Begishev
Doctor of Law Senior Researcher V.G. Timiryasov Kazan Innovative University Kazan, Russia (Russian Federation) e-mail: begishev@mail.ru ORCID: https://orcid.org/0000-0001-5619-4025

Abstract

This paper considers in detail the physical and cyber attacks on and the main failures in cyber-physical systems, the basic requirements for, the issues of ensuring, and the legal aspects of the security of cyber-physical systems. Cyber-physical systems have a variety of security and privacy issues that can reduce their reliability, security, and effectiveness, and possibly hinder their widespread deployment. Thus it requires several measures to enhance their safety while maintaining the required performance. It is determined that the prospects for the development of legislation in the field of liability for harm caused by the participation of cyber-physical systems are associated with changes in digital technologies and the evolution of social norms.

Keywords: cyber-physical system, security, failures, law, responsibility, robot, robotics, cyber attack, artificial intelligence

Introduction

Modern information and telecommunication complexes, systems, and networks are the convergence of various digital technologies and communications. These foundations define the perspectives of the digital realm that enables the activities of people and machines. Currently, countering attacks on cyber-physical systems is an extremely important issue both for technological development and for determining its legal aspects.

Materials and Methods

The theoretical studies of various Russian and foreign experts in the security of cyber-physical systems served as materials for the research. The results are considered reliable based on the study of a significant and necessary array of articles, as well as the use of modern methods of cognition, including dialectical and general scientific methods (analysis, synthesis, deduction, induction).

Physical attacks on cyber-physical systems

Physical attacks have become more active in recent years, especially against industrial systems - cyber-physical systems (hereinafter referred to as CPS)[1]. There is a wide range of types of physical attacks:

1 Malicious software. The means of such an attack can be infected CDs, USB drives, devices, and drives, such as Stuxnet[2], which, after being inserted into a cyber-physical device, installs a hidden malware containing malicious software.

2 Abuse of privileges. This attack occurs when fraudsters or disappointed employees gain access to server rooms and apparatuses in the CPS domain. This allows them to use a fake USB drive to infect by installing malware, code, keystrokes, or capturing sensitive data.

3 Wire breaks, intercepts, dialing. Since the communication lines, including telephony and Wi-Fi of many Cyber-Physical Headquarters (HQ), are still physically visible, attackers can cut wires or connect to the system to intercept communications[3].

4 Fake identification. This occurs when attackers masquerade as legitimate employees with enough experience to deceive others. They mainly act as cleaners to facilitate access and improve interaction with other employees[4].

5 Stalkers: usually legal employees who show curiosity (with malicious intent), gain the confidence of administrators and engineers of the CPS to obtain their credentials to blackmail or sell them to other competing organizations.

6 Interception of CCTV cameras. This includes the interception of video recordings from CCTV cameras that ensure the security of the entrance and key points in the CPS zones. This can be done by distorting camera signals, cutting communication wires, removing footage, gaining access to a remote control and monitoring area, etc.

7 Hacking an ID card. This includes cloning ID cards stolen from employees, or creating similar genuine copies to gain full or partial access and hack into the CPS domain.

Cyber attacks on cyber-physical systems

The CPS can also be subjected to various cyber attacks as follows.

1 Eavesdropping. It includes the interception of unprotected network traffic of the CPS to obtain confidential information (passwords, usernames or any other information of the CPS). Eavesdropping can be of two main forms: passive, by eavesdropping on the transmission of a CPS network message, and active, by probing, scanning, or forging a message claiming to be a legitimate source.

---

[1] H. He, J. YanCyber-physical attacks and defences in the smart grid: a survey IET Cyber-Phys. Syst., 1 (1) (2016), pp. 13-27

[2] D. Albright, P. Brannan, C. WalrondStuxnet malware and natanz: update of isis december 22, 2010 report Inst. Sci. Int. Secur., 15 (2011), pp. 739883-739893

[3] G. Francia III, D. Thornton, T. BrookshireCyberattacks on SCADA systems Proc. 16th Colloquium Inf. Syst. Security Educ (2012), pp. 9-14

[4] J. Slay, M. MillerLessons learned from the maroochy water breach International Conference on Critical Infrastructure Protection, Springer (2007), pp. 73-82

2 Cross-site scripting. It takes place when third-party web resources are used to run malicious scripts in the web browser of the target victim (mainly the target CPS engineer, contractor, workers, etc.)
3 Password cracking. This method is the most common to gain access to the database.
4 Phishing. It can be as email phishing, vishing, spear phishing or wailing that target some or all CPS users (such as engineers, professionals, businessmen, CEOs, COOs or CFOs (CFOs)). Phishing allows an attacker to pretend to be business colleagues or service providers.
5 Use of a virus. The virus can replicate and spread to other devices through human or human intervention. Viruses spread by attaching themselves to other executable codes and programs to harm CPS devices and steal information.
6 Rootkit. It is designed to remotely and covertly access or control a computer to execute files, access or steal information, or change system configuration.
7 Polymorphic malware. It constantly and frequently changes its identity to avoid detection and become unrecognizable to any pattern matching detection methods.

Major cyber-physical failures

Considering the various threats, attacks, and vulnerabilities the CPS domain suffers from, it is important to outline the main failures of the systems. These failures can be minor (limited damage) or major (major damage). Failures can be as follows.

1 Content error: means an inaccurate content of the information provided, which may cause the functional system to fail. The content error can be either numeric or non-numeric (such as alphabets, graphics, sounds, or colors).
2 Synchronization error: means the delayed or interrupted information delivery time (transmission/reception) (received/transmitted too early or too late). This will affect the decision-making process and may cause data management issues.
3 Sensor failure: means the sensors are no longer operating properly and will seriously hamper the decision-making process due to misinformation or a sudden stop of the CPS.
4 Budget failure: occurs when the cost of implementing a cyber-physical system exceeds a set budget before ever reaching testing levels. This is mainly due to poor planning of the system implementation process.
5 Schedule failure: occurs when the schedule set for planning, testing, and evaluating a given CPS fails due to further updates, additional testing, or inconsistency with user needs.
6 Service failure: occurs when an error propagates through the interface of a service and affects decision making and/or normal performance. It can cause a partial or complete failure of the CPS, either temporarily or permanently.

Risk assessment is important to evaluate the economic impact of risk from an attack on any CPS before managing it. Such management is based on assessing and analyzing the risk before it is mitigated, and then applying the proper security measures according to the level of severity and impact of the risk.

CPS Essential Safety Requirements

1. Privacy. CPS constantly runs a huge process of data collection, which requires constant control.[5]
2. Reliability. The adaptive behavior of the CPS is achieved to improve reliability and ensure the correct quality of service through the timely implementation of fault tolerance mechanisms. Reliability is based on the ability to adapt to changing conditions to overcome and recover from any possible failures based either on cyber or physical attacks from intruders in addition to natural disasters[6].

Physical systems depend on timing and proper functionality. However, in case of any possible inconsistency, unreliability and uncertainty can cause problems and failures in the operation of the CPS services. Therefore, maintaining high reliability requires lower uncertainty.

3 Sustainability. CPS must be sustainable to overcome accidents and malicious attacks. Consequently, logical and physical CPS are subject to cyber security vulnerabilities from a security point of view.
4. Interaction and coordination. They are necessary to maintain the continuous operational security of the CPS. Interaction and coordination of CPS between cyber and physical elements of the system is a key aspect[7].
5. Operational security. Its main task is to ensure operational efficiency by denying any attacker access to public or private information; hence, the control of information and observed activities regarding a given cyber-physical system, especially in hostile environments or areas[8].
6. Identification of critical information includes identifying the information, if any, that could effectively impair CPS's operational effectiveness or compromise its potential success for the organization, and develop an initial plan to protect it.
7. Threat analysis. It includes determining the potential and capabilities of an attacker to collect, process, analyze, and use the necessary information.
8. Vulnerability analysis. Includes the study of the weak points of a given cyber-physical system and the strengths of the enemy. Thus, a possible idea is created of how a potential attacker can use this security hole to hack.
9. Risk assessment. Risks are assessed based on a combination of threat and vulnerability levels, based on how high or low those levels are. The levels of risk assessment involve assessing the costs of implementing the right security controls by striking a trade-off between an effective balance of costs and benefits.

[5] S. Belguith, N. Kaaniche, G. RusselloPu-abe: lightweight attribute-based encryption supporting access policy update for cloud assisted IoT2018 IEEE 11th International Conference on Cloud Computing (CLOUD), IEEE (2018), pp. 924-927

[6] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, K. UedaCyber-physical systems in manufacturingCIRP Ann., 65 (2) (2016), pp. 621-641

[7] F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, N.N. XiongRobust cyber–physical systems: concept, models, and implementationFuture Gener. Comput. Syst., 56 (2016), pp. 449-475

[8] K. Van Brabant, *et al.*Operational Security Management in Violent EnvironmentsOverseas Development Institute London (2000)

CPS Security

Maintaining a secure CPS is quite a task due to the ever-increasing challenges, integration issues, and limitations of existing solutions, including lack of security, privacy, and accuracy. However, this can be reduced through various means. Let's consider them in more detail

1 Reliable multi-factor authentication. Today, the concept of multi-factor authentication is being applied by combining two or more factors: (1) "you are", which includes the fingerprint of the device, the fingerprint of the user, the geometry of the hand, the iris scan, the retinal scan, etc., and (2) "you have", which includes cryptographic keys to increase its resistance to authentication attacks[9].

2 Strong password and dynamic hashing process: passwords are considered as a "you know" authentication factor.

3 Safe and secure audit. It can be done with an audit management system that collects and stores logs on a distributed system[10]. This limits any attempts by insiders against the cyber-physical system and stores digital evidence of internal and external attacks to trace them.

4 Extended non-cryptographic solutions. The anomaly detection algorithm should be chosen according to the constraints of the CPS device, which may be statistical for limited or based on a machine algorithm such as random forest for powerful CPS devices.

5 Online monitoring. This solution includes running systems in real time using specialized forensic or other tools and techniques necessary to prevent accidental or non-random failure of any cyber-physical system.

6 Security and employee check should be carried out for each employee before and during work to rule out any possible insider/whistleblower attempt to break into the system. Such security checks are especially important in critical areas such as nuclear power plants[11].

7 Periodic training of employees. It includes periodically educating ICS and PLC employees on cybersecurity best practices based on their level and knowledge, with the ability to detect any suspicious behavior or activity.

8 Periodic risk assessment. Used to examine the likelihood and impact of a certain risk on the CPS based on a qualitative or/or quantitative risk assessment and cost-benefit analysis (CBA) to classify the risk as acceptable/unacceptable and minimize it as early as possible.

9 Defense in depth. There is a need for a multi-purpose security solution that provides the best protection at each operational level (perception, transmission, and application) of the CPS.

[9] H.N. Noura, R. Melki, A. ChehabSecure and lightweight mutual multi-factor authentication for IoT communication systems2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE (2019), pp. 1-7

[10] H.N. Noura, O. Salman, A. Chehab, R. CouturierDistlog: a distributed logging scheme for IoTforensics Ad Hoc Netw., 98 (2020), p. 102061

[11] J. Hogan, R. HoganHow to measure employee reliability. J. Appl. Psychol., 74 (2) (1989), p. 273

Legal Aspects of CPS Security

Inclusion of CPS into human life entails the emergence of relations with their participation, which inevitably brings to life the need for the legal regulation of such relations[12].

From a legal standpoint, the study of cyber-physical systems is still at its initial stage. The reason is the newly emerging social relations and the still limited practice of applying the CPS[13]. The most acute among lawyers today is the problem of AI liability, both tort and contractual, its legal personality, etc.

There are prerequisites for the formation of the so-called "robo-law" or "the law of cyber-physical systems", the subject of which are relations in the research, implementation, and development of modern artificial intelligence technologies.

According to D.L. Kuteynikov, O.A. Izhaev, S.S. Zenin, V.A. Lebedev, the spread of innovative technical means capable of making human-independent decisions based on complex computer algorithms is of great importance for legal science and practice. It is the autonomy that underlies the discussion of jurists regarding the emergence of the legal personality of AI and other components of cyber-physical systems[14].

E.S. Mikhaleva, E.A. Shubina believe that the challenge for the legal regulation of social relations in the new reality is precisely the autonomy of material and intangible objects. It is in this context that the definition of such concepts as "cyber-physical system", "cyber-biological system" and "artificial cognitive system" is of particular scientific interest, as the phenomena they designate potentially have a sign of autonomy[15].

However, the legal literature state that robots and other cyber-physical systems generally fit well into the existing regulatory mechanisms of civil liability[16]; however, the authors acknowledge that a number of theoretical and practical issues are still controversial, and getting an unambiguous answer seems impossible today.

Regardless of the nature of the development of cyber-physical systems, they will still be inherent in causing harm, even if they are configured to prevent such harm in other situations. One example would be an airbag, which is designed to provide safety, but in some cases, they do serious harm to people[17-19].

---

[12] Begishev I.R. Draft federal law "On the turnover of robots, their components (modules)" // Relevant issues of economics and law. - 2021. - V. 15. - No. 2. - P. 379-391. – DOI 10.21202/1993-047X.15.2021.2.379-391.

[13] Arkhipov V.V., Bakumenko V.V., Volynets A.D., Naumov V.B., Neznamov A.V., Pobryzgaeva E.P., Sarbash S.V., Smirnova K.M., Tytyuk E.V. Regulation of robotics: an introduction to “robo-law”. Legal aspects of the development of robotics and artificial intelligence technologies / Ed. A.V. Neznamova. - Infotropic Media, 2018. P. 3.

[14] D.L. Kuteinikov, O.A. Izhaev, S.S. Zenin, V.A. Lebedev. Cyberphysical, cyberbiological, and artificial cognitive systems: essence and legal features // Russian law: education, practice, science. 2019. No. 3. P. 77

[15] E.S. Mikhaleva, E.A. Shubina. Issues and prospects of legal regulation of robotics // Relevant issues of Russian law. 2019. No. 12. P. 26-35.

[16] A.V. Neznamov, B.U. Smith. Robot is not to blame! A view from Russia and the United States on liability for robot-caused harm // Law. 2019. No. 5. P. 139.

[17] The general study of the effectiveness of airbags, see: Kent R., Viano D.C., Crandall J. The Field Performance of Frontal Air Bags: A Review of the Literature // raffic Injury Prevention. 2005 Vol. 6. N 1.

Conclusion

Cyber-physical systems have a variety of security and privacy issues that can reduce their reliability, security, effectiveness, and possibly hinder their widespread deployment. Thus it requires a number of measures to enhance their safety while maintaining the required performance.

The prospects for the development of legislation in the field of liability for harm caused with the participation of cyber-physical systems are associated with changes in digital technologies and the evolution of social norms.

Acknowledgments

This paper has been supported by the Kazan Federal University Strategic Academic Leadership Program.

References

C. Kearney, "Strategic Planning for Financing and Growing Biotechnology Companies," Journal of Commercial Biotechnology, vol. 24, no. 4, pp. 62-67, 2019. DOI: https://doi.org/10.5912/jcb917

H. He, J. YanCyber-physical attacks and defences in the smart grid: a survey IET Cyber-Phys. Syst., 1 (1) (2016), pp. 13-27

D. Albright, P. Brannan, C. WalrondStuxnet malware and natanz: update of isis december 22, 2010 report Inst. Sci. Int. Secur., 15 (2011), pp. 739883-739893

G. Francia III, D. Thornton, T. BrookshireCyberattacks on SCADA systems Proc. 16th Colloquium Inf. Syst. Security Educ (2012), pp. 9-14

J. Slay, M. MillerLessons learned from the maroochy water breach International Conference on Critical Infrastructure Protection, Springer (2007), pp. 73-82

S. Belguith, N. Kaaniche, G. RusselloPu-abe: lightweight attribute-based encryption supporting access policy update for cloud assisted IoT2018 IEEE 11th International Conference on Cloud Computing (CLOUD), IEEE (2018), pp. 924-927

L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, K. UedaCyber-physical systems in manufacturingCIRP Ann., 65 (2) (2016), pp. 621-641

F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, N.N. XiongRobust cyber–physical systems: concept, models, and implementationFuture Gener. Comput. Syst., 56 (2016), pp. 449-475

K. Van Brabant, et al.Operational Security Management in Violent EnvironmentsOverseas Development Institute London (2000)

H.N. Noura, R. Melki, A. ChehabSecure and lightweight mutual multi-factor authentication for IoT communication systems2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE (2019), pp. 1-7

H.N. Noura, O. Salman, A. Chehab, R. CouturierDistlog: a distributed logging scheme for IoTforensics Ad Hoc Netw., 98 (2020), p. 102061

J. Hogan, R. HoganHow to measure employee reliability. J. Appl. Psychol., 74 (2) (1989), p. 273

Begishev I.R. Draft federal law "On the turnover of robots, their components (modules)" // Relevant issues of economics and law. - 2021. - V. 15. - No. 2. - P. 379-391. – DOI 10.21202/1993-047X.15.2021.2.379-391.

J. Jordan, "Setting Up and Working with a Board of Directors: A Guide for Startups," Journal of Commercial Biotechnology, vol. 24, no. 4, pp. 86-90, 2019. DOI: https://doi.org/10.5912/jcb921

Arkhipov V.V., Bakumenko V.V., Volynets A.D., Naumov V.B., Neznamov A.V., Pobryzgaeva E.P., Sarbash S.V., Smirnova K.M., Tytyuk E.V. Regulation of robotics: an introduction to "robo-law". Legal aspects of the development of robotics and artificial intelligence technologies / Ed. A.V. Neznamova. - Infotropic Media, 2018. P. 3.

D.L. Kuteinikov, O.A. Izhaev, S.S. Zenin, V.A. Lebedev. Cyberphysical, cyberbiological, and artificial cognitive systems: essence and legal features // Russian law: education, practice, science. 2019. No. 3. P. 77

E.S. Mikhaleva, E.A. Shubina. Issues and prospects of legal regulation of robotics // Relevant issues of Russian law. 2019. No. 12. P. 26-35.

A.V. Neznamov, B.U. Smith. Robot is not to blame! A view from Russia and the United States on liability for robot-caused harm // Law. 2019. No. 5. P. 139.

The general study of the effectiveness of airbags, see: Kent R., Viano D.C., Crandall J. The Field Performance of Frontal Air Bags: A Review of the Literature // raffic Injury Prevention. 2005 Vol. 6. N 1.