

### Analysis of Cyber Assaults Targeting Essential Information Structure Utilizing Iot Technologies

**Bobur Abidov**

Independent academic researcher

#### Article Information

**Received:** July 03, 2023

**Accepted:** Aug 04, 2023

**Published:** Sep 05, 2023

**Keywords:** Digital intrusion, smart power grid, Internet of Things (IoT), critical infrastructure, and cybersecurity.

#### ABSTRACT

*There are varying methods of protection from cyber-attacks in vital information structures in every country. In this research paper, we take a close look on difficulties related with invasive cyber-attacks on significant information infrastructures in recent years. Various methods for enhancing information security and minimizing or deterring cyber assaults are indicated. The paper makes use of such concepts as Internet of Things, IoT solutions, and network. It is by no means unimportant to reveal all possible types of cyber assaults, take necessary measures to prevent them, and invent means of protection.*

#### 1. Introduction

Most of the highly developed countries in the world have information systems, information and telecommunication networks, automated control systems for critical information infrastructure entities that provide important services such as electronic communications, energy, banking and finance, public services, transport and water management, which should be securely protected from various external threats. Due to the widespread use of IoT applications that allow you to control almost everything via the Internet, security vulnerabilities are simultaneously emerging. The Internet of Things is a significant innovation of our time, but it also poses a serious cybersecurity threat to critical information systems objects. Security vulnerability compromises the security of the entire system and provides an opportunity for attackers to attack. When IoT applications are used in critical infrastructure, some serious cybersecurity issues arise on their own. If an intruder's cyber-attack is directed at a critical information infrastructure, the result of such an attack can be catastrophic. Power outages in hospitals, temperature changes in the cooling systems of nuclear reactors, deliberate misuse of features in smart cars are just a few of the many devastating scenarios. Cases of deliberate hacking of the critical information infrastructure of different countries for the purpose of theft, espionage, intimidation, destruction, cyber terrorism, etc., have become more frequent, which serves as a pretext for the escalation of the conflict, and the likelihood of armed confrontation. Obviously, the problem of cybersecurity is one of the most relevant and important today. Cyber-attacks can destroy the physical systems

of an organization or government, transfer control of those systems to a third party, renders them inoperable, or compromise people's privacy

[1]. The purpose of this study is to analyze cyber-attacks on critical information infrastructure for the period from 2017 to 2022. Objectives: to consider possible losses and losses caused by common types of cyber-attacks; classify cyberattacks under study based on common features and characteristics; propose measures that can be taken to prevent cyber-attacks or minimize their consequences.

### **1.1. Cyber-attacks on critical information infrastructure**

The Internet of Things (IoT) is an evolution in machine-to-machine communication, a unique connection that allows computing devices to transmit data across the entire network without the participation of even one person. An alarming situation is the growing interconnection of critical information infrastructure objects using the technologies of the Internet of Things and the accompanying increase in the number of organized cyber-attacks around the world. It was found that many Clone Security cyber-attacks committed in recent years were directed at the official websites of the mayor's office of the Surkhandarya region, cities and districts of the region, belonging to various subjects of critical information infrastructure. It is clear that malware that targets water and gas stations, power plants and transport systems is the work of professionals and was specifically designed to perform such actions. Many devices operating on the basis of the Internet of Things are integrated into the subjects of a critical information infrastructure to achieve the most effective interaction and communication. According to forecasts, by 2025 the number of devices connected to the Internet will reach 75 billion, which can significantly worsen the situation and lead to an increase in the growth of cyber-attacks aimed at critical information infrastructure [1], which are developed using solutions based on the Internet of Things and, accordingly, may be subject to cyber-attacks.

Let's review cyberattacks for the period 2017-2022. We can say that devices connected to the Internet are within the concept of the Internet of Things, thanks to the existing infrastructure of the Internet. Thus, all devices using the technology of the Internet of Things can be subject to almost any cyber-attack. Vulnerabilities in the Internet security system can also disrupt the operation of programs based on the Internet of Things. It can be concluded that this innovative technology, in addition to positive prospects, also poses new threats to cybersecurity. Let's consider the most significant examples of cyberattacks based on the Internet of Things, as well as their danger to critical information infrastructure.

**Power Grid Hacking:** Attackers managed to seize control of Uzbekistan's power grid by hacking into the SCADA system. This led to a massive power outage that left about 700,000 people without power for several hours. It is believed that this attack, based on the IoT system, is a test for attackers of a new, probably the most sophisticated malware to sabotage subjects of critical information infrastructure [2].

**DDoS attack on Dyn:** This DDoS attack used a system known as the Mirai botnet. The Mirai botnet targets IoT devices by scanning the Internet in parallel to find poorly secured IoT devices that typically have a default username and password. Moreover, this botnet is involved in large-scale DDoS attacks on the servers of the American Internet provider Dyn. This cyberattack can be called "successful" as many users left the logins and passwords of their devices "by default", which made them an easy target for this botnet. Many websites such as Twitter, Netflix, Reddit and Spotify were unavailable throughout the day [3].

**Attack on light rail network:** The tram network in the city of San Francisco has been attacked by ransomware hackers. During which not a single firewall was hacked, but one of the employees let the hackers into the network by clicking on the phishing mail [4].

**Water Company Hack:** Attackers infiltrated a water utility's SCADA system, taking control of

the system and altering the amount of chemicals used. With the help of this attack, they intervened in the process of water purification and production [5].

**Attack on the smart building:** smart homes and buildings are common Internet of Things technologies. These technologies are developed using IoT devices, and their connection to the Internet remains uninterrupted. The DDoS attack was carried out in winter, heating and hot water supply systems were turned off in two buildings. A DDoS attack overwhelmed the system for managing fake Internet traffic. Due to the overload, the system rebooted uncontrollably every few minutes and, along the way, denied administrators remote access [6].

**Cyberattack on the electricity grid:** In the UK, on Election Day, the electricity grid was attacked. The purpose of a cyberattack is to disable the power supply network by penetrating the SCADA system. The attack was carried out using fake emails addressed to high-ranking employees that used social engineering techniques to get the employee to click on a fake link, provoking malware. This attack was a more polished, polished version of a common phishing attack called spear phishing [7].

**Cyber Attack on Oil Refinery:** An unsuccessful attempt was made to attack an oil refinery. The purpose of the attack is to sabotage the operation of the enterprise and cause an explosion that could lead to the death of people. As a result, an error in the code of the attacker's program led to the failure of the attack and the explosion was not carried out, the source code of this program was not found earlier in other cyberattacks. All hacker IoT tools were created for this particular enterprise [8].

**Cyber-attack on the transport network:** A cyber-attack hit the transport network, causing train delays and disrupting travel services, customers could not book a ticket or receive information about train delays [9].

**Cyberattack on a healthcare company:** the attackers seized registration information from a supplier that provided electronic equipment for the hospital, attacked the server using remote launch methods, activating the SamSam ransomware virus, eventually encrypting the hospital's most important data files [10].

Critical information infrastructure entities are gaining more efficient performance and connectivity through IoT-based applications. But this can lead to security vulnerabilities and an increase in the number of cyberattacks on them.

## **2. Common types of cyber attacks**

Cyberattacks can be targeted at IoT applications and industrial enterprise control systems interacting with them. This type of attack can pose a threat to human life, property and the environment. Most often, such cyber-attacks are very complex and well-thought-out, which significantly distinguishes them from ordinary cyber-attacks. they combine several different methods and technologies. Consider the most common methods.

The introduction of malware is a deliberate entry of virus software into the cyberspace of the control system in order to damage or disable the entire system [11]. Adware, keyloggers, worms, spyware, rootkits, ransomware, trojans or viruses are the most commonly known malware. WannaCry ransomware is one of the most famous examples of malware. This software is used to deprive people of access to their files and important network services until a certain amount of money is paid to regain access.

Phishing is a request to obtain sensitive user data for an untrusted network resource. An attacker, the owner of such a resource, is trying to convince users of the security and reliability of his, say, site. The victim of such a deception performs certain actions pre-selected by the attacker, for example, following a link to a malicious site or entering his confidential data. In this case, the victim transfers his personal data to the attacker with his own hand.

Spear phishing is a more common phishing attack, especially among various critical information infrastructure actors. Data attached to an email is used to force a potential victim to click on a link, thereby activating malware.

Hacking (Hacking) is the process of gaining unauthorized access to a system. The most important step in this process is obtaining a password to access the system. Hacking is usually done through various methods such as brute force.

Denial of Service (DoS) attacks are aimed at flooding the system network with excessive traffic and spam data. The communication system becomes overloaded with too many unnecessary connection requests. Such an overload greatly slows down the system or puts it in a non-working state. DDoS attacks can potentially be carried out from any device connected to the Internet.

SQL injection is a cyberattack that aims to steal, modify, or delete the contents of a database. A similar method is used to attack systems that are directly controlled by the data they have. Attackers activate SQL query statements to access the database server [12].

Man-in-the-middle is a type of attack, the purpose of which is to listen to the communication channel between devices. Since data transmission is carried out through an attacker's device, network transmissions can be stolen and altered by an attacker. When data transmission does not have a strong encryption algorithm, an attack can be easily achieved in IoT applications.

Targeted cyberattack (developed persistent threat) is a cyberattack in which attackers gain access to the system network and remain unnoticed for some time. The purpose of this attack is usually to steal data. A targeted cyberattack is a complex process that requires modern knowledge and tools to implement; such attacks are usually the work of large organizations or countries. In addition, the process of targeted cyber-attack requires a high level of stealth throughout all stages of implementation.

Thanks to the services and capabilities of ISPs, the number of mobile and IoT devices will grow, along with this, the number of cybersecurity vulnerabilities in IoT-based systems will also grow. Thus, security systems for critical information infrastructure facilities will be constantly tested by attackers to the limit. In addition, personal and corporate data can be stolen by cybercriminals for ransom, which is facilitated by the increase in the number of devices connected to the Internet.

### **3. Cyber-attack mitigation**

New cyberattacks occur daily and it is almost impossible to prevent each of them. However, initial protection methods are of great importance in terms of mitigating the effects of current and future attacks. Cyberattack mitigation includes both intrusion detection techniques and intrusion prevention techniques. Let's consider some of the methods for mitigating the consequences of cyber-attacks on critical information infrastructures based on the Internet of things.

Access control: It is very important to determine in advance which resources, data files, and components can be accessed by users and devices. In addition, you need to define areas that unauthorized users or undefined devices should not have access to. The use of predefined access rules reduces the possibility of unauthorized access to the network. Access controls such as discretionary, mandatory, and role-based access controls can increase the security of a system against potential threats. Access control methods such as selective access control, mandatory access control, and role-based access control can greatly improve the effectiveness of an information security system. In remotely controlled cyber-physical systems such as smart grids, access control is very important to limit the access of users and devices on the network.

Encryption: often, the purpose of an attack is to steal data from the system or intercept internal network packets, but the use of strong encryption methods greatly reduces the chances of a

successful attack. Therefore, when IoT applications are used in critical infrastructures, the communication channel between IoT devices and the control system must be securely encrypted. The use of weak encryption methods can create information security problems. Thus, encryption is very important for protecting data integrity and confidentiality in communication networks.

Device authentication is the main step in the process of secure data transfer. This stage is responsible for identifying devices and agreeing on the tasks that devices must perform on the network. Authentication ensures that smart devices do not execute unauthorized commands. Authorization and identification are an integral part of authentication.

**Regular Remote Security Updates:** IoT devices should be easy to update remotely. Therefore, device security updates should also be performed easily and remotely. If the device is not configured to receive regular updates, then it is not possible to constantly update the security system. Unfortunately, most manufacturers currently design IoT devices without firmware and security updates in mind. At the same time, due to the rapid development of technology, it is very important to provide regular updates to solve problems that operating systems and programs may encounter due to security vulnerabilities. In addition, for the smart grid based on the Internet of Things, regularly updating the firmware is a smarter solution than mass replacement of obsolete grid elements. Moreover, remote and accessible firmware update is one of the important security requirements to mitigate potential threats in IoT-based systems.

**Physical security:** It is very important to ensure the physical security of the devices in the system. Tamper protection mechanisms should be integrated into system elements to protect them from physical unauthorized access. Physical access by unauthorized persons to devices can lead to compromise of data stored in them. Stored data may be associated with identification, account or authentication. Therefore, devices should have security measures such as data wipe or data lock to protect them in the event that the device is taken over by intruders. Also, it is crucial to note that the physical security of control rooms and servers is more important because a physical security vulnerability on any device poses a threat to the entire network. Therefore, precautions must be taken at the stage of creating an information security system.

The security of environments based on the Internet of Things, such as subjects of critical information infrastructure, is a serious and urgent problem. The networks of the Internet of Things are one of the main structures of the critical information infrastructure. Thus, any security vulnerability of Internet of Things networks can directly affect the entire environment in which they are used. The development of reliable, convenient, integrated and high-performance hybrid IDS is an effective solution for detecting various types of cyber-attacks.

#### **4. Conclusion**

The security of a critical information infrastructure is the state of security of a critical information infrastructure that ensures its stable operation when carried out against its computer attacks [13]. The subjects of critical information infrastructure are subject to cyberattacks for various reasons, mainly because of their importance. It is also clear that physical or cyber-attacks will never stop. Therefore, each country must apply the most affordable and reliable information security measures for these infrastructures everywhere. Cyber-attacks on critical infrastructures can cause serious damage. The number of cyberattacks on nuclear facilities, power systems, dams and other critical facilities is growing every day. The increased number of smart devices connected to the Internet creates serious security vulnerabilities for networks. Thus, if very important steps are not taken to solve security problems, it is obvious that the damage caused by cyber-attacks on the subjects of critical information infrastructure will lead to catastrophic consequences for states and organizations.

Applications of the Internet of Things are the most important structures in terms of improving the efficiency of work and interaction between subjects of critical information infrastructure.



However, all attacks that can occur on the Internet can also be carried out on the Internet of Things. In the article, we presented an analysis of cyberattacks in recent times and the most common methods used in cyberattacks on subjects of critical information infrastructure. Discussed various modern ways to mitigate the effects of cyber-attacks from a cyber-security perspective. A particularly important aspect of cybersecurity is the use of appropriate identification methods, as it helps to take countermeasures in advance, and also allows the development of a predictive and proactive cybersecurity strategy for critical information infrastructure entities with Internet of Things technologies.

## References

1. Richard Haeussler, Sammy Lin, Jens-Peter Kaps, and Kris Gaj. Side-channel resistant implementations of three finalists of the NIST lightweight cryptography standardization process: Elephant, tinyjambu, and xoodoo. 2022.
2. Christopher Hadnagy. *Social Engineering: The Science of Human Hacking*.
3. Yigael Berger, Avishai Wool, and Arie Yeredor. Dictionary attacks using keyboard acoustic emanations. In Proceedings of the 13th ACM conference on Computer and communications security, pages 245–254, 2006.
4. Michael Sikorski, Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*
5. Adam Shostack. *Threat Modeling: Designing for Security*
6. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Annual international cryptology conference*, pages 388–397. Springer, 1999.
7. Dawn Cappelli. Big picture of the insider threat problem over time, complex interactions and unintended consequences of existing policies. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering)*