# Navigating the landscape of IoT security and associated risks in critical infrastructures

Andrej Pastorek
Prague Advanced Technology and Research Innovation Center
Jugoslávských partyzánů 1580/3, 160 00 Praha 6 – Dejvice
Czech Republic
andrej.pastorek@patrik.expert

Andrea Tundis
Institute for the Protection of Terrestrial Infrastructures (PI), German Aerospace Center (DLR)
Rathausallee 12, 53757 St. Augustin, Germany
andrea.tundis@dlr.de

## ABSTRACT

The Internet of Things (IoT) presents transformative opportunities for connectivity and automation across various sectors, but it also introduces significant security risks that need to be comprehensively addressed. Indeed, the growing integration of IoT devices, including their vulnerabilities, into critical infrastructures amplifies potential risks in daily life, making these systems prime targets for cybercriminal activities, including espionage and sabotage. Cases where IoT devices have been misused, due to firmware vulnerabilities, embedded passwords, and hidden backdoors are real-world scenarios, that pose significant threats to privacy and security. That's why this paper aims to point out the urgency of addressing these issues as IoT applications continue to proliferate across healthcare, transportation, urban development and other sectors. Different types of vulnerabilities and their implications with focus on urban critical infrastructures, which can lead to severe consequences like energy blackouts, water contamination, and widespread service disruptions, especially in densely populated areas, are discussed. Moreover, the need of a multidimensional approach that encompasses technological, legal, social, and economic considerations, to deal with those broader cybersecurity and risk management implications of IoT is highlighted. As a consequence, the need for continuous evolution in security strategies to keep pace with the rapid advancements in IoT technologies is pointed out, thus arguing for a proactive approach to safeguard IoT systems against emerging threats and to ensure the safe and resilient operation of these increasingly integral parts of modern critical infrastructures.

## CCS CONCEPTS

• **Security and privacy** → **Systems security**; **Software and application security**.

## KEYWORDS

Internet of Things, Malware, Firmware, Misuse, Safety, Security, Protection of Critical Infrastructures

*ARES 2024, July 30–August 02, 2024, Vienna, Austria*
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3669979

**ACM Reference Format:**
Andrej Pastorek and Andrea Tundis. 2024. Navigating the landscape of IoT security and associated risks in critical infrastructures. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3664476.3669979

## 1 INTRODUCTION

The Internet of Things (IoT) describes physical objects or groups of physical objects with sensors, information processing capabilities, software and other technologies that connect and exchange data with other devices and systems over the Internet or another communication network. It is based on the convergence of different technologies, computing, increasingly powerful embedded systems, and machine learning [13].

IoT installations and applications continue to grow as their services make people's lives easier. However, IoT, including its communication infrastructure, could be threatened by a number of risks and its vulnerability grows with increased number of attached networked devices [11] [5]. Any malfunction in any part of IoT caused by human-made events including cybercriminal activities or natural disaster events can have significant impacts on the security of citizens and on the stability of a society accustomed to the availability of various IoT services provided 24 hours 7 days a week. Even a brief interruption in the continuity of critical infrastructures and in the provision of their services, (e.g. in healthcare, power supply or in those processes that in principle must take place continuously), can have critical impacts on people's lives.

Unfortunately, the possibility of misuse of IoT devices remains one of the most neglected areas of IoT security [10]. Indeed, developers, manufacturers and service providers themselves, could exploit them whether for their own commercial advantage or due to links to foreign powers in possible activities in the field of cyber industry and even computer espionage. Considering heterogeneous nature of the Internet of Things, vulnerabilities may also occur in the interfaces used to exchange information between network elements, even in digital signatures [7]. The primary focus is on the technological aspects, but the discussion also covers legal, social, and economic dimensions related to the security of the Internet of Things (IoT). This comprehensive analysis addresses one of the most significant threats associated with IoT usage: attacks conducted through malicious software embedded in IoT components and infrastructure. Such attacks may manifest as acts of hybrid warfare or asymmetric threats, for example, through the firmware of devices designed for IoT infrastructure.

Table 1: Emerging Aspects of IoT Misuse and Security Risks

| Emerging Aspects | Description |
|---|---|
| *Pervasive Misuse* | The increasing prevalence of IoT device misuse across various sectors and applications as digitalization expands. |
| *Vulnerabilities in Firmware* | Concerns about vulnerabilities present in the firmware of IoT devices, including common vulnerabilities in embedded Linux kernels, login passwords, and hidden backdoors. |
| *Intentional Backdoors* | Instances of intentional backdoors being exploited to gain unauthorized access to IoT devices and systems, posing serious security risks. |
| *Cross-Sector Vulnerability* | Vulnerabilities extending across various domains, including healthcare, transportation, and household appliances. |
| *Patient Safety Risks* | Risks to patient safety due to vulnerabilities in critical infrastructure devices such as infusion pumps, highlighting the potential for physical harm resulting from IoT misuse. |
| *Privacy and Security Risks* | Risks including privacy breaches and compromised security of home networks, potentially allowing malicious control over appliances, and posing safety risks to individuals. |
| *Need for Enhanced Security Measures* | The urgent need to enhance security measures and promote responsible usage of IoT devices to mitigate risks and safeguard against potential threats to individuals and infrastructure. |

The rest of the paper is structured as follows: Section 2 explains urgency of the topic by providing real cases of misuse of IoT. Impacts of threats at low level hardware/firmware on high level policies are described in Section 3. Connections with broader implications are described in Section 4; whereas particular attention on urban critical infrastructures is given in Section 5. A discussion on the limitation of the current approach is elaborated in Section 6; whereas Section 7 concludes this work.

## 2 REAL CASES ABOUT IOT MISUES AND EMERGING ASPECTS

According to our research it, the misuse of IoT devices or IoT-based systems is not new. In addition, as digitalization grows, this misuse becomes increasingly pervasive in various contexts and application domains. Here are elaborated a few examples where IoT systems have either been misused or where significant potential of this type has been revealed during testing of non-traditional devices connectable to the Internet. In particular:

- As reported in [14], extensive testing, which was focused on a total of 237 different devices usable within the IoT infrastructure, yielded the following very worrying results: 73% of the firmware files contained common vulnerabilities in their embedded Linux kernel, 22% of the firmware files contained embedded login passwords, and 6% of the firmware files contained hidden backdoors.
- The most media covered IoT incident occurred in March 2022 [8], when electric car chargers on the highway between Moscow and St. Petersburg were taken out of service. Through a backdoor allowing remote access, the chargers, manufactured by Ukrainian supplier AutoEnterprise in Kharkiv, were deactivated and programmed to display pro-Ukrainian messages.
- Cynerio tested and analyzed data from more than 10 million devices in more than 300 hospitals and healthcare facilities around the world [4]. The most common type of Internet-connected device in hospitals were infusion pumps, equipped with firmware that allowed the correct dose of medicine or other liquid to be drawn and dosed to the patient. Backdoors were discovered in infusion pumps supplied by a Chinese manufacturer.
- In 2017, the Australian Communications Consumer Action Network commissioned researchers from the University of New South Wales to test the security of 20 household appliances that can be connected and controlled via wi-fi. These included a smart TV, portable speaker, voice assistant, printer, sleep monitor, digital photo frame, bathroom scale, light bulb, switch, smoke alarm and a talking Hello Barbie doll. All devices (including Barbie) had some form of security vulnerability [3]. This could potentially mean that it is possible to break into a home's network and collect data from IoT devices. The potential for abuse is considerable, from a simple privacy violation to the possibility that someone with malicious intent could turn on the oven while turning off smoke alarms and other sensors.

Table 1 underscores the emerging aspects related to the alarming prevalence of IoT device misuse across various sectors and applications. From widespread vulnerabilities in firmware [2] to intentional backdoors facilitating unauthorized access, the implications are profound. The incidents cited highlight not only the susceptibility of IoT systems but also the potential for significant harm, ranging from privacy breaches to physical safety risks. As the IoT ecosystem continues to expand, urgent attention must be directed towards enhancing security measures and promoting responsible usage to mitigate these risks and safeguard against potential threats to individuals and infrastructure alike.

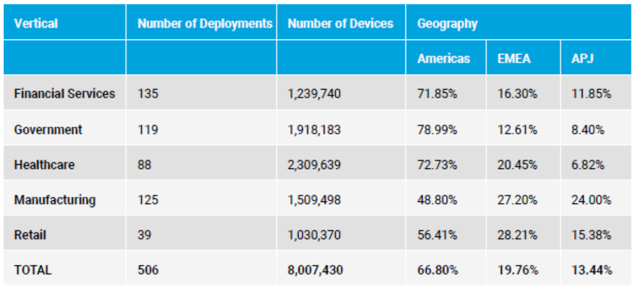
## 3 LOW-LEVEL IMPACTS AND HIGH-LEVEL POLICIES

It is important to keep in mind that nowadays hardware (H) is very often represented by a combination of hardware (H) and firmware (F), and that firmware can be updated and often updated remotely. If we take as an example a standard computer (itself an H/F combination), then almost all of its basic components (motherboard, disk drive, graphics adapter, optical drives) have the ability to update firmware, and even CPU units have microcode for updating). In the world of the Internet of Things, this remote update is becoming widespread, and only very simple sensors and actuators do not have such an option.

It is worth noting that, in the rest of the paper, the"hardware" term may also refer to an updatable H/F combination mentioned above, while the term "firmware" refers only to low-level software that is built into hardware devices. This classification follows the approach proposed in [9], that is used whenever there is need to distinguish between pure hardware and a combination of hardware and firmware.

A critical analysis of IoT failures and practical experience in the field of cyber technologies in an international context also shows that the issue of malware (M) in hardware (H) and firmware (F) is closely linked to the possibility of state sponsorship. This is related, among other things, to the peculiarities of H/F malware, which are described below. Therefore, in all cases where attacks based on the abuse of H/F are conducted, foreign forces must be considered as one of the most likely perpetrators. In the next description, this linkage is always considered, even if it is not implicitly stated.

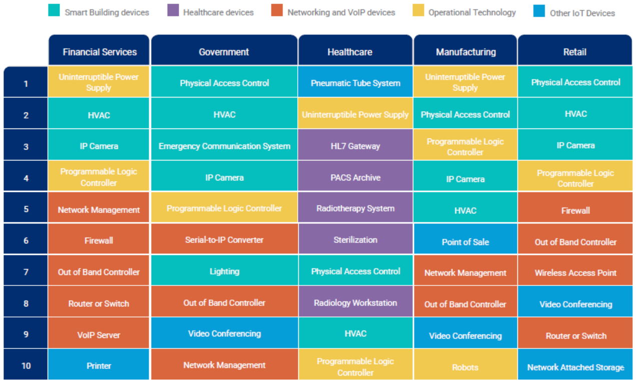
Figure 1 of the report shows that the current deployment of IoT sensors and actuators numbers in the tens of millions, providing digital data for publication or further processing, and it is reasonable to anticipate that this figure will escalate to billions in the very near future, increasing the potential incidence of cyberattacks significantly.



| Vertical | Number of Deployments | Number of Devices | Geography | | |
|---|---|---|---|---|---|
| | | | Americas | EMEA | APJ |
| Financial Services | 135 | 1,239,740 | 71.85% | 16.30% | 11.85% |
| Government | 119 | 1,918,183 | 78.99% | 12.61% | 8.40% |
| Healthcare | 88 | 2,309,639 | 72.73% | 20.45% | 6.82% |
| Manufacturing | 125 | 1,509,498 | 48.80% | 27.20% | 24.00% |
| Retail | 39 | 1,030,370 | 56.41% | 28.21% | 15.38% |
| TOTAL | 506 | 8,007,430 | 66.80% | 19.76% | 13.44% |

**Figure 1: Distribution of deployments in Vertical and Geography - ©Forescout 2024**

The first indication that IoT will not be spared from intentional malicious phenomena comes from data that illustrate alarming trends in traditional forms of IT, especially in recent years, where numbers of pre-installed or embedded forms of malware in various IT products supplied to customers, as well as various forms of exploitation of IT security vulnerabilities by state organizations or state-supported entities, is growing significantly, often without sufficient response from the affected institutions and responsible authorities.



🟩 Smart Building devices 🟪 Healthcare devices 🟧 Networking and VoIP devices 🟨 Operational Technology 🟦 Other IoT Devices

| | Financial Services | Government | Healthcare | Manufacturing | Retail |
|---|---|---|---|---|---|
| 1 | Uninterruptible Power Supply | Physical Access Control | Pneumatic Tube System | Uninterruptible Power Supply | Physical Access Control |
| 2 | HVAC | HVAC | Uninterruptible Power Supply | Physical Access Control | HVAC |
| 3 | IP Camera | Emergency Communication System | HL7 Gateway | Programmable Logic Controller | IP Camera |
| 4 | Programmable Logic Controller | IP Camera | PACS Archive | IP Camera | Programmable Logic Controller |
| 5 | Network Management | Programmable Logic Controller | Radiotherapy System | HVAC | Firewall |
| 6 | Firewall | Serial-to-IP Converter | Sterilization | Point of Sale | Out of Band Controller |
| 7 | Out of Band Controller | Lighting | Physical Access Control | Network Management | Wireless Access Point |
| 8 | Router or Switch | Out of Band Controller | Radiology Workstation | Out of Band Controller | Video Conferencing |
| 9 | VoIP Server | Video Conferencing | HVAC | Video Conferencing | Router or Switch |
| 10 | Printer | Network Management | Programmable Logic Controller | Robots | Network Attached Storage |

**Figure 2: Riskiest devices by Vertical - ©Forescout 2024**

This trend will not bypass IoT, since the massively higher number of potentially vulnerable devices, platforms, and interfaces as well as new opportunities emerging in areas that have hitherto been little affected by traditional IT technologies and that have not yet undergone the full impact of the digital evolution (e.g., Government, Healthcare, Financial Services) allow the phenomena to become widespread across all deployment areas, as shown in Figure 2.

A typical example may be the automotive industry. With the massive use of new digital technologies in modern cars, we may reasonably expect that cyberattacks will similarly increase, as hackers are already exploring new possibilities in this area. The modern car has dozens of IT components with millions of lines of code – (and it is estimated that there are up to 0,3 errors for every 1,000 lines in released code, which may represent potential doors for future hackers). With increasingly automated vehicles and their internet connectivity, the number of potential locations where a cyberattack can be carried out is growing exponentially. Successful attacks on automotive IT systems have already been proven. At the same time, there is growing concern about the possibility of using the extensive capabilities of SW in vehicles for covert purposes, which leads to administrative measures that have as their primary aim prevention in the form of bans on the use of "suspicious" devices. For example, the Chinese government has banned the entry of TESLA cars into Chinese military buildings based on such suspicions [12]. On the other hand, in the USA, the Chinese company was temporarily excluded from the tender for the supply of subway cars because of similar concerns [6].

## 4 LINKAGE TO BROADER IMPACTS

As we navigate through the landscape of the Internet of Things (IoT), it is crucial to scrutinize the intersection where expansive capabilities meet emerging threats that exploit these technologies. Specific cases of IoT misuse discussed in Section 2 have broader cybersecurity and risk management implications that are elaborated in Section 5. IoT's potential is fundamentally tethered to its capacity to seamlessly integrate diverse technologies—sensors, data analytics, automation, and real-time response capabilities. However, this integration exposes a multifaceted landscape of risk. Technological layers, from the physical hardware to the software interfaces, interlock to form a continuous chain of operation. Each component, while crucial for sophisticated IoT functionality, also introduces potential vulnerabilities that can be exploited maliciously. IoT devices amalgamate hardware with advanced software functionalities, inheriting vulnerabilities from both realms. The firmware becomes particularly susceptible to exploitation as it can serve as hidden conduits for malware, enabling attackers to disrupt device functionality or siphon data without triggering traditional cybersecurity defenses. The complexity of IoT systems compounds their vulnerability. Devices often operate within interconnected environments that are not only vast but also characterized by a lack of uniform security practices. This disparity is evident in the integration of legacy systems with modern IoT innovations, where outdated security frameworks are ill-equipped to shield against contemporary cyber threats. The implications of these vulnerabilities extend beyond general technology concerns and will have broad impact on specific key sectors, especially on urban development and critical infrastructure. Addressing these vulnerabilities requires more than traditional security measures; it necessitates adaptive strategies that are robust yet flexible enough to evolve with advancing technology. This includes enhancing the physical and network security of IoT devices and incorporating dynamic response mechanisms that can preemptively tackle new threats [1].

## 5 TYPES OF VULNERABILITIES IN URBAN CRITICAL INFRASTRUCTURES

A phenomenon of particular relevance nowadays is the so-called urbanization, i.e. the propensity of individuals to move from suburbs towards urban areas, in which classic services linked to critical infrastructures such as, energy and water provision, transportation and communication, and so on, are integrated, modernized and thus complemented through digital-based services which in turn are available via Internet and accessible through IoT devices. Although the advantages due to the continuous growth of digital-centered critical infrastructures, digitization also creates new opportunities for malicious users, who can exploit IT flaws to gain unauthorized access, to launch cyberattacks and thus affect the functioning of critical infrastructures which can have catastrophic repercussions on citizens' lives (e.g. energy blackouts, water poisoning, problems in the transport and communication system, etc.) Indeed, urban areas are complex systems that include a wide range of heterogeneous and interconnected structures and software-centric devices capable of strongly influencing each other, and whose links and dependencies are difficult to be studied through the use of linear models, due to the large number of relationships and external factors, of which many are even not controllable. These phenomena become extremely accentuated when linked to malicious and crisis situations (i.e. human-made as well as naturally occurring) that are typically not easy to be identified and handled. Some challenges that emerge from such digitization phenomenon, and which increase the vulnerability of such highly digitized systems, can be of various nature. More specifically, we can have:

*intra-domain vulnerability:* these vulnerabilities are linked to the specific component, whose introduction and use in the critical infrastructures of the urban system produces the creation or insertion of vulnerabilities in the system itself. In particular, intra-domain vulnerabilities refer to weaknesses and risks that arise within a specific domain or sector of critical infrastructure within an urban area. When digitalization is implemented within these domains, it introduces various components such as software systems, sensors, controllers, and communication networks. However, each of these components can potentially introduce vulnerabilities into the system. For instance, let's consider the energy sector within an urban area. The introduction of IoT-based technologies such as smart meters, automated control systems, and remote monitoring tools enhances efficiency and facilitates better management of energy distribution. However, each of these technologies also opens up potential avenues for exploitation by malicious actors. Smart meters, for example, can be vulnerable to hacking, leading to unauthorized access to energy consumption data or even manipulation of meter readings. Automated control systems, if not properly secured, could be targeted for sabotage or manipulation, leading to disruptions in energy supply or even damage to critical infrastructure components. The challenge with intra-domain vulnerabilities is that they are often specific to the technology and systems used within a particular domain. As urban infrastructures become more interconnected and reliant on IoT technologies, the number of potential vulnerabilities within each domain increases, amplifying the overall risk to the urban system as a whole.

*inter-domain vulnerability:* these vulnerabilities are related to the interaction between components belonging to different interrelated domains, that means, those that have interdependencies between them, whose functioning positively or negatively impact each other. Such interdependencies can create vulnerabilities that are not related to any particular component or process or belonging to any specific domain, if considered or analyzed in an isolated way, but derive from their interaction, for example related to information transmitted, logical (inter) dependency such as control, regulatory or other mechanisms. In other words, inter-domain vulnerabilities arise from the interactions and dependencies between different domains or sectors of critical infrastructure within an urban area. These vulnerabilities stem from the complex interconnections and interdependencies that exist between various systems and processes. Consider the interaction between the energy sector and the transportation sector within an urban area. Energy is needed to power transportation systems such as trains, buses, and traffic lights. At the same time, transportation systems rely on the availability of energy to operate efficiently. If there is a disruption in the energy supply due to a cyberattack or infrastructure failure, it can have cascading effects on the transportation sector, leading to delays, cancellations, or even accidents. Similarly, disruptions in transportation can impact the energy sector by affecting the distribution of fuel or the ability of workers to commute to power plants or substations. Inter-domain vulnerabilities highlight the interconnected nature of urban infrastructures and the potential for disruptions to propagate across different sectors. Identifying and mitigating these vulnerabilities requires a comprehensive understanding of the dependencies and interactions between various

| Vulnerability Type | Examples |
|---|---|
| *Intra-domain* | - Smart meters vulnerable to hacking, allowing unauthorized access to energy consumption data.<br>- Automated control systems susceptible to manipulation, leading to disruptions in energy supply.<br>- Vulnerabilities in communication networks within transportation systems, allowing remote access for malicious activities. |
| *Inter-domain* | - Energy disruption impacting transportation systems, causing delays or accidents.<br>- Transportation disruptions affecting energy distribution, leading to fuel distribution issues.<br>- Cyberattack on communication systems affecting both energy and water management, causing cascading failures in critical infrastructure. |
| *Interoperability vs. Integration* | - Compatibility issues between energy and transportation systems, leading to communication failures.<br>- Conflicts between data formats in water management and communication systems, causing data loss or corruption.<br>- Integration challenges between emergency response systems and urban monitoring platforms, hindering coordination during crisis situations. |
| *Real-data acquisition & scenario tracking* | - Unauthorized access to IoT devices used for urban monitoring, allowing manipulation of data streams.<br>- Injection of false data into scenario tracking systems, leading to incorrect assessments of crisis situations.<br>- Exploitation of vulnerabilities in sensor networks for air quality monitoring, leading to inaccurate reporting and ineffective response to pollution issues. |

**Table 2: Examples of Vulnerabilities in Urban Critical Infrastructures Related to IoT Integration**

domains, as well as proactive measures to strengthen resilience and redundancy within the urban system.

*Interoperability vs. Integration vulnerability:* Interoperability refers to connecting applications so that data from one system can be accessed by the other one. Whereas, integration involves a third party that translates the data and makes it “work” for the receiving system. Typically, existing models and analysis tools are conceived and designed to work on a single application domain. Such “isolated” fashion does not make them fit well the modelling and the analysis of an urban environment since they do not allow a holistic supportive view of the whole system. Hence there is need to integrate and introduce ad-hoc define components that enable cooperations among the different domains at different layers. However, this might introduce vulnerabilities related to interoperability and integration of existing methods, approaches, protocol of already existing and available IoT devices which were not natively conceived/created to (co-) work within such (highly-hybrid) urban context. In other words, in the context of urban infrastructure, achieving interoperability and integration is essential for enabling efficient data sharing and collaboration between different domains such as energy, transportation, water management, and communication systems. However, the process of integrating disparate systems and ensuring interoperability introduces its own set of vulnerabilities. For example, when integrating existing models and analysis tools from different domains, there is a risk of compatibility issues or conflicts between protocols, standards, or data formats. Additionally, introducing ad-hoc components to enable cooperation between domains may inadvertently create new points of vulnerability that could be exploited by malicious actors. Furthermore, the use of IoT devices within urban environments adds another layer of complexity to interoperability and integration. These devices may not have been originally designed to work together within a highly interconnected urban context, leading to potential vulnerabilities in the communication protocols or security mechanisms used by these devices. Addressing interoperability and integration vulnerabilities requires careful planning and implementation of standardized protocols, security measures, and testing procedures to ensure the seamless operation of interconnected systems while minimizing the risk of exploitation by malicious actors.

*Real-data acquisition & scenario tracking vulnerability:* The choice and use of IoT devices through which city data is acquired is another key factor to consider. Having vulnerabilities in this phase, due to untrusted devices, is extremely dangerous since it allows malicious users to access data without authorization, manipulate data, inject malicious or untruthful data that do not reflect the real state of the infrastructures and therefore the state of the city. As a consequence, this might negatively impact on the level of safety and security of citizens, especially in presence of crisis events, when it is necessarily to obtain and tracking live data, in order to monitor evolution of such crisis event and support further analysis by supporting the computation of new additional data coming from the city, thus deriving real-time useful information, which in turn can be then used to define and apply countermeasures the operation. More specifically, real-data acquisition and scenario tracking are essential components of urban monitoring and crisis management systems, allowing authorities to gather real-time data on various aspects of the urban environment and track the evolution of crisis events. However, the use of IoT devices for data acquisition introduces vulnerabilities that could be exploited by malicious actors to compromise the integrity, confidentiality, or availability of data. One key vulnerability lies in the trustworthiness of the IoT devices themselves. If these devices are not properly secured or authenticated, they may become entry points for attackers to gain unauthorized access to sensitive data or infrastructure systems. This could result in the manipulation or injection of false

| Advanced Security Measures | Short description |
|---|---|
| *Mandatory security certifications* | IoT devices must pass stringent security certifications that assess vulnerability to hacking and other cyber threats |
| *Regular security audits* | Frequent and comprehensive audits are mandated to ensure ongoing compliance with established security standards. |
| *Real-time threat detection systems* | Deployment of advanced threat detection systems that monitor and mitigate potential cybersecurity threats in real-time. |
| *Enhanced data protection measures* | Strengthened regulations around data protection specific to IoT devices to prevent unauthorized data access and ensure user privacy |

**Table 3: Advanced security measures to be implemented**

data, leading to incorrect assessments of the situation or ineffective response measures. In the context of crisis events, such as natural disasters or cyberattacks, the ability to acquire and track real-time data becomes critical for effective decision-making and response coordination. However, if the data being collected is compromised or manipulated, it can lead to delays or errors in response efforts, potentially putting lives and infrastructure at risk. To address real-data acquisition and scenario tracking vulnerabilities, it is essential to implement robust security measures for IoT devices, including encryption, authentication, and access control mechanisms. Additionally, regular monitoring and auditing of data sources and communication channels can help detect and mitigate any suspicious activities or anomalies in real-time data streams. By ensuring the integrity and reliability of data acquisition systems, urban authorities can better safeguard against malicious attacks and support effective crisis management and response efforts. Table 2 provides for each of the above-mentioned vulnerability examples in case of their potential exploitation.

## 6 DISCUSSING THE LIMITATIONS OF CURRENT APPROACHES

Existence of intentional harmful phenomena in the cyberspace associated with IoT devices is based on the information found or leaked that IoT itself is part of the cyber warfare plans of many states and the subject of intense interest of non-governmental entities (transnational hacking groups, terrorist organizations, organized crime groups, etc.). The possibilities that IoT brings in the field of cyber warfare (usually referred to as “asymmetric threats”, "hybrid warfare", "state-organized cybercrime"), are too tempting and provide countless opportunities. This fact is supported by numerous findings of intelligence services and CSIRTs across Europe. An assessment of the situation couple of years ago showed that a benevolent approach in Europe was prevailing with smartphones serving as a frightening example. Many smartphones from Far East vendors had pre-installed tracing malware [9]. Even though this information was often published and known, these phones were still sold throughout the EU without any obstacles. If we could make an analogy with other areas, such as the sale of food or toys (where EU implemented efficient pan-European warning mechanism) - it was like neglecting sales of contaminated food or dangerous toys. Since then, the evolving landscape of Internet of Things (IoT) security in Europe has witnessed significant strides toward fortifying the infrastructure against cyber threats. This transformation is in response to the prior existence of intentional harmful phenomena in cyberspace associated with IoT devices, a challenge compounded by the IoT’s integration into the cyber warfare plans of states and the intense interest from non-governmental entities like transnational hacking groups, terrorist organizations, and organized crime groups

*Revised Approach to IoT Security in Europe.* The European Union has recognized the vulnerabilities inherent in the burgeoning IoT sector—similar to the risks posed by contaminated food or unsafe toys—and has taken decisive steps to mitigate these through stringent cybersecurity measures. The analogy to consumer safety is apt; just as the EU has established mechanisms to ensure the safety of food and toys, it has begun to implement robust frameworks to safeguard IoT devices from malware, backdoors, and other cybersecurity threats.

*New Regulatory Frameworks.* Recent regulatory enhancements in the EU aim to create a more resilient digital environment. These include comprehensive directives and regulations that mandate higher security standards for IoT devices sold within the Union. For instance, the introduction of the EU’s Cybersecurity Act strengthens the overall cybersecurity of network and information systems across the bloc. Additionally, the EU has been proactive in developing a certification framework that ensures a uniform level of cybersecurity across products, processes, and services, which includes IoT devices. Based on practical experiences from the field of classical information technology, the EU’s approach now incorporates several advanced security measures that are summarized in Table 3.

*Ongoing Challenges.* Despite these significant advancements, serious challenges remain in the realm of IoT security within Europe. The heterogeneity of IoT devices and their extensive integration into various aspects of everyday life create complex security landscapes that are difficult to regulate comprehensively. Moreover, as IoT technology continues to evolve rapidly, regulatory measures must adapt at a comparable pace to remain effective. In conclusion, while the situation has markedly improved with the adoption of new EU cybersecurity measures, the inherent complexities of IoT security mean that serious challenges still loom large. The ongoing task for European regulators and technology providers is to stay ahead of threats through innovation in security technologies and robust regulatory frameworks.

- The current situation still does not ensure the security of IoT and security of users because:
- Cybersecurity measures implemented at higher levels of IT processes cannot provide a secure environment if lower-level processes contain security holes. Therefore:
- Responsible bodies must take further control over the transparency and verifiability of the hardware deployed and used in IoT, especially when they are part of critical infrastructure.

## 7 CONCLUSION

IoT is a qualitative shift not only in terms of social development, but to some extent also in terms of the traditional understanding of safety and security. New IoT technologies provide automated tools and mechanisms that (among all other potential benefits) significantly reduce unintentional human error such as negligence, incompetence or inattention, but on the other hand they significantly expand the scope for the malicious aspects and possibilities of large-scale coordinated cyberattack.

Conventional methods of malware detection are unlikely to be sufficient, mainly due to limited human resources. From a brief summary and preliminary analysis of the current situation in traditional IT industries and extrapolation of this situation to the world of IoT, it can be clearly demonstrated that the current relatively benevolent approach existing in the traditional IT field can lead to catastrophic consequences in the case of IoT.

Summarizing the current state of IoT implementation, it can be stated that: (i) currently, there is still no unified overview of millions of devices in IoT infrastructure, where virtually the only guarantee of security is the "goodwill" of vendors. The situation may worsen with rapidly increasing connection of further devices; (ii) the (state-sponsored) malware embedded and hidden in hardware is, unfortunately, an ideal tool for industrial espionage and future cyber warfare in all its forms. It can be exploited across all digital universe, ranging from ordinary households to critical infrastructure systems; and (iii) attacks performed using hidden functions in IoT components can disable IoT-based infrastructures for a long time, and in some cases permanently, thus being catastrophic especially for human lives.

## ACKNOWLEDGMENTS

This research work was conducted within the projects "urban-Model", that is funded by the German Aerospace Center (DLR). Moreover, the activity is carried out in cooperation with the LOEWE-Zentrum emergenCITY.

## REFERENCES

[1] Asimily. 2024. *IoT Device Security in 2024: The High Cost of Doing Nothing.* Retrieved May 8, 2024 from https://asimily.com/iot-device-security-in-2024-the-high-cost-of-doing-nothing/

[2] Taimur Bakhshi, Bogdan Ghita, and Ievgeniia Kuzminykh. 2024. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors* 24, 2 (2024). https://doi.org/10.3390/s24020708

[3] The Conversation. 2020. *Are your devices spying on you? Australia's very small step to make the Internet of Things safer.* Retrieved May 8, 2024 from hhttps://theconversation.com/are-your-devices-spying-on-you-australias-very-small-step-to-make-the-internet-of-things-safer-145554

[4] Cynerio. 2022. *Research Report: The State of Healthcare IoT Device Security 2022.* Retrieved May 8, 2024 from https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022

[5] Amir Djenna and Diamel Eddine Saïdouni. 2018. Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure. In *2018 2nd Cyber Security in Networking Conference (CSNet).* 1–4. https://doi.org/10.1109/CSNET.2018.8602974

[6] Justin George. 2020. *Metro's next-generation rail cars will not be made in China.* Retrieved May 8, 2024 from https://www.washingtonpost.com/local/trafficandcommuting/metros-next-generation-rail-cars-will-not-be-made-in-china/2020/01/25/1d848c7e-3e06-11ea-baca-eb7ace0a3455_story.html

[7] Francesco Buccafurri Gianluca Lax and Gianluca Caminiti. 2015. Digital Document Signing: Vulnerabilities and Solutions. *Information Security Journal: A Global Perspective* 24, 1-3 (2015), 1–14. https://doi.org/10.1080/19393555.2014.998843 arXiv:https://doi.org/10.1080/19393555.2014.998843

[8] Aaron Gordon. 2022. *Russian Electric Vehicle Chargers Hacked.* Retrieved May 8, 2024 from https://www.vice.com/en/article/akvya5/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead

[9] Václav Jirovský. 2014. Safety, Security and Privacy in Environmental Monitoring Systems. In *CTU, FD 2014, Prague.* https://doi.org/ISBN:978-80-01-05478-9

[10] B V Santhosh Krishna and T Gnanasekaran. 2017. A systematic study of security issues in Internet-of-Things (IoT). In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).* 107–111. https://doi.org/10.1109/I-SMAC.2017.8058318

[11] I. F. Mikhalevich and V. A. Trapeznikov. 2019. Critical Infrastructure Security: Alignment of Views. In *2019 Systems of Signals Generating and Processing in the Field of on Board Communications.* 1–5. https://doi.org/10.1109/SOSG.2019.8706821

[12] Reuters. 2021. *Tesla cars barred from some China government compounds - sources.* Retrieved May 8, 2024 from https://www.reuters.com/world/china/tesla-cars-barred-some-china-government-compounds-sources-2021-05-21/

[13] Arjmand Samuel and Cameron Sipes. 2019. Making Internet of Things Real. *IEEE Internet of Things Magazine* 2, 1 (2019), 10–12. https://doi.org/10.1109/IOTM.2019.1907777

[14] Wei Xie, Yikun Jiang, Yong Tang, Ning Ding, and Yuanming Gao. 2017. Vulnerability Detection in IoT Firmware: A Survey. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS).* 769–772. https://doi.org/10.1109/ICPADS.2017.00104