Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation

Management and Engineering of Critical Infrastructures

Hurst, W.S.K.; Shone, Nathan

https://doi.org/10.1016/B978-0-323-99330-2.00010-6

CHAPTER 12

Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation

William Hurst[a] **and Nathan Shone**[b]
[a]Information Technology Group, Wageningen University & Research, Wageningen, The Netherlands
[b]School of Computing and Mathematics, Liverpool John Moores University, Liverpool, United Kingdom

1 The emerging cyber-threat

Critical infrastructures have seemingly invisible boundaries, inherently intertwined, interconnected and codependent. Initially, this was a physical overlap, where one service relied on the direct output or production of another. More recently, the boundaries have become increasingly fuzzy—cyber-based—as a result of the societal move toward smart city innovations, which replace manual (labor-intensive) tasks with automation [1] by means of sophisticated digital technologies. Their digital interconnectivity is now complex, and this technical switch has produced a new frontier for security, where threats to the health and wellbeing of critical infrastructures are no longer just weather-related (climate change [2], extreme weather [3]), physical (terrorism [4], drone [5]) or blockade-based [6] but now also cyber. Displayed in Fig. 1, a simplified network of external threat vectors is based on a compilation of research articles that focus on varied domains of critical infrastructure protection (specifically [2–7]).

For visualization purposes, Fig. 1 arranges the threat vectors into groups, Weather, Physical and Cyber. Yet each is multifarious resulting in three issues: (i) The nature of the impact of a successful attack is somewhat unpredictable. For instance, impacts have the potential to range from severe (e.g., nuclear meltdown, flooding, blackouts, economic shutdown, etc. [8]) to minor (individual loss of personal data, minor delays to service provision); (ii) The threat source is diverse, where security solutions (physical or cyber) in one domain may have no or little benefit for others; and (iii) Interdependency, while a major benefit, also has the potential to spread the damage exponentially (referred to as *cascading*) across differing critical infrastructure types.

1.1 Research trend

These challenges have created a spate in research over the last 20 years into cascading failure analysis, protection plans and simulations of interconnectivities. Yet, what we see is

Management and Engineering of Critical Infrastructures
https://doi.org/10.1016/B978-0-323-99330-2.00010-6

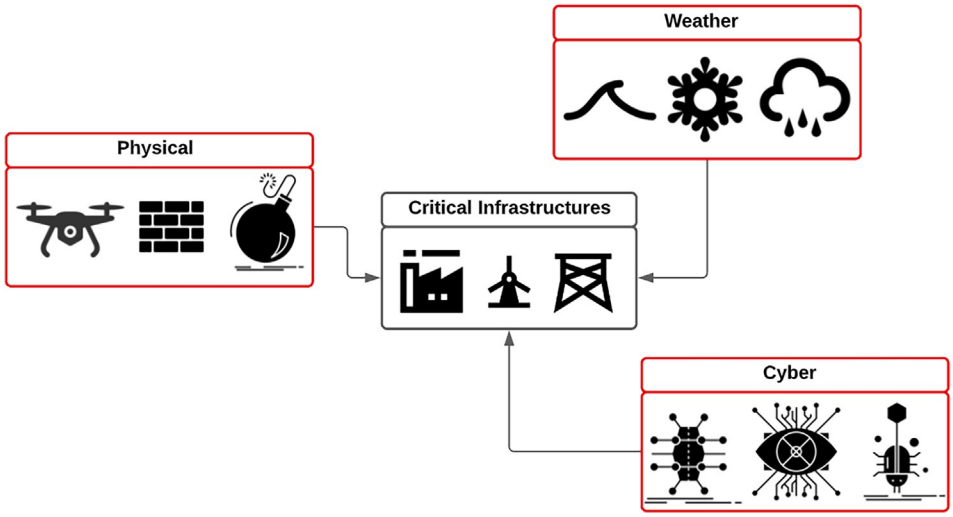

Fig. 1 External threat vectors.

also a shift toward cyber-security research, as indicated in Fig. 2 displaying the research focus trend from 1922 journal articles on the Scopus digital library over a 20-year period between January 1, 2001 and December 31, 2021.

While now a prominent topic in the research community, for most this cyber-threat is invisible and unseen, despite some staggering statistics. For instance, Kaspersky solutions blocked 1,686,025,551 cyber-attacks from online resources across the globe during the second quarter of 2021, documented in a report available in Ref. [9]. Yet, recent high-profile examples (in varied critical infrastructure domains) have found prominence in the wider media, pushing critical infrastructure security more into the mainstream. One of particular prominence being WannaCry.

1.2 WannaCry

WannaCry simultaneously established a foothold throughout multiple continents and organizations in May 2017 [10]. WannaCry is classified as a type of an attack known as *ransomware*, involving the use of malware (malicious software) to encrypt files on a target device, rendering it inoperable (Fig. 3). Perpetrators of ransomware demand payment (ransom) for the decryption of the device, thus granting access to the files. Ransomware is common for use in small (i.e., personally-directed) attacks. Kaspersky defeated 97,541 ransomware attacks for their users documented in Ref. [9]. Yet, on this scale, with a critical infrastructure target, the use of ransomware was almost unprecedented prior to WannaCry. It is now known to have spread to over 150 countries and did so within a matter of a few hours [11].

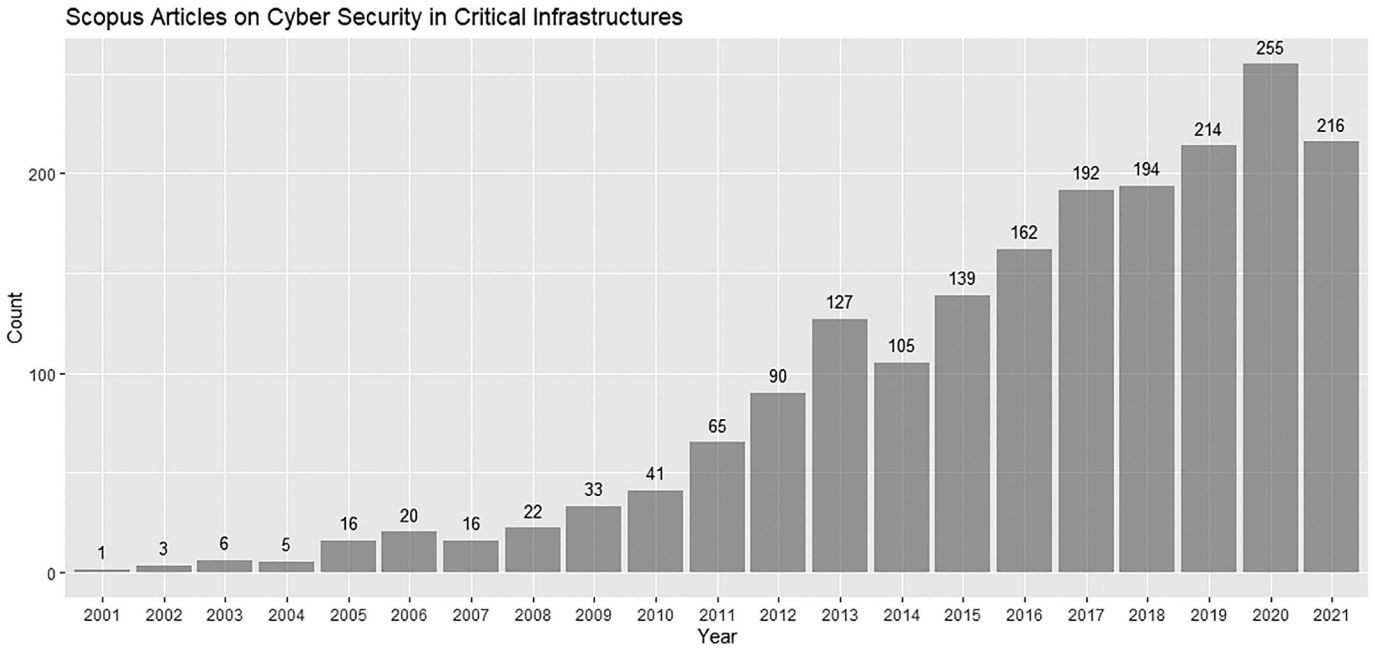

Fig. 2 Research trends 2001–21.

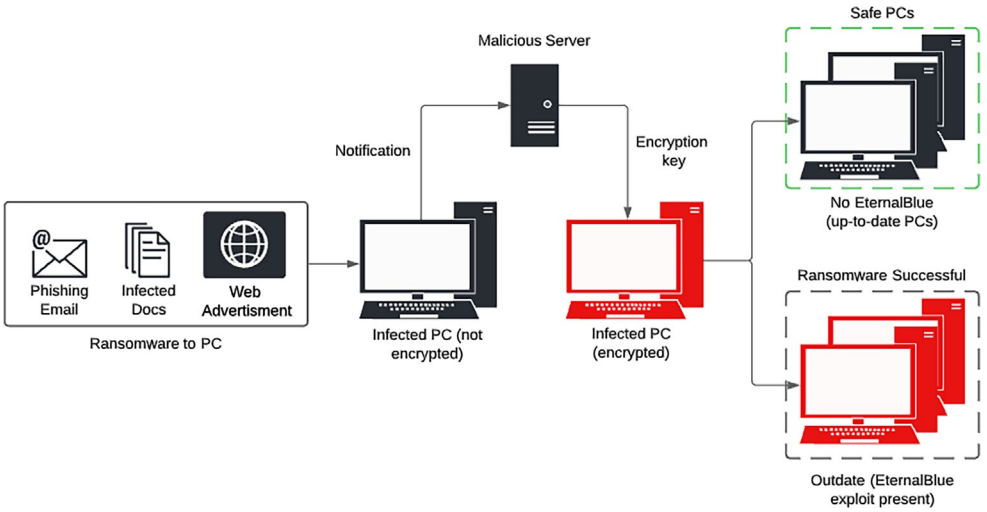

Fig. 3 High-level view of WannaCry.

Ghafur et al. document the impact of WannaCry on the United Kingdom's National Health Service (NHS), by means of a retrospective analysis in Ref. [10]. Despite WannaCry infecting around 600 organizations nationwide, the main documentation in the media was relating to the 34 infected hospital trusts. Ghafur et al. detail in their findings that, specifically, fiscal costs were the main impact of WannaCry. For instance, £4 m in lost inpatient admissions and £1.3 m from canceled outpatient appointments. However, no difference in mortality was noted [10].

WannaCry had further impact after 2017 with The Hacker News media outlet documenting that WannaCry briefly resurfaced in 2018 as a new variant, causing the Taiwan Semiconductor Manufacturing Company (a producer of microchips) to shut down several factories temporarily as a result of 10,000 machines becoming infected [12].

1.2.1 Cryptoworm

WannaCry is known as a *ransomware cryptoworm*, specifically designed to target users working with the Microsoft Windows Operating System (OS). The cryptoworm works by encrypting data and then, as with other ransomware approaches, demands payment for decryption (in this instance in cryptocurrency). The cryptoworm propagated through an exploit (a software which takes advantage of a vulnerability within another software) known as EternalBlue. EternalBlue was an exploit allegedly developed take advantage of a vulnerability in Microsoft's Server Message Block (a communication protocol created to share access to files or printers on a shared network). EternalBlue's designs were leaked by hackers. However, the deployment of WannaCry also required coupling

EternalBlue with a backdoor implant tool known as DoublePulsar, which allowed WannaCry to install and execute a copy of itself [13].

1.3 ThreatNeedle

However, Windows OS is not alone in facing high-profile threats, macOS also finds itself a target, notably within the defense industry critical infrastructure grouping. During 2020, a spate of spyware attacks from using the ThreatNeedle cluster on defense enterprises in over 12 countries were documented in a report by Kaspersky [14,15]. ThreatNeedle is an advanced cluster of malware known as NukeSped, which is a trojan designed to target macOS devices, allegedly linked to the North Korean government [16]. Cybersecurity expert Patrick Wardle provides a clear breakdown of NukeSped's functionality on his blog *Objective-See* found in Ref. [17]. The trojan works by posing as a cryptocurrency application and subsequently gains persistence on the host device. The infected device then contacts a server for the second-stage malicious payload [16].

1.4 Stuxnet

ThreatNeedle is not unique as a state-backed cyber-threat. Possibly, the most well-known state-based cyber-attack example is Stuxnet. Stuxnet was first uncovered in 2010 and immediately gained prominence within cyber-security research communities and the mainstream media for both its level of sophistication and target. Stuxnet was designed specifically to damage the Programmable Logic Controllers (PLC) at a nuclear power plant in Natanz, Iran [18]. PLCs are used to automate mechanical processes, such as gas centrifuges. Stuxnet was able to spread toward its target using a number of different mechanisms, namely: USB flash drives, Siemens SIMATIC WinCC (interface to SCADA systems), Siemens SIMATIC Step7 (industrial control projects) and network shares.

1.4.1 Zero-day

Stuxnet exploited zero-day flaws to deploy its payload which, as Bilge et al. discuss, are vulnerabilities that have not been disclosed publicly or to those who may directly be invested in knowing the vulnerabilities exist [19] (i.e., security teams). Typically, as vulnerabilities remain unknown, there is no defense against a zero-day exploit, with antivirus solutions (and traditional intrusion detection systems) unable to provide patches to attack signatures that are yet unidentified [19] and only understood after an attack has taken place. A further nature of a zero-day exploit is that the attacks are targeted. For instance, the attackers are specifically aware of a vulnerability in a particular system of their target and the attack is adjusted as such. For example, Stuxnet exploited several Microsoft zero-day flaws, two of which are labeled MS10-061 (Print Spooler Service) and MS08-067 [20] (server service allowing remote code execution in Windows XP [21]).

To date, much research has been conducted on detecting zero-day exploits, for example, in Refs. [22–24], with a comprehensive review by Abri et al. in Ref. [25]. Effective solutions tend toward proactive security models, where the detection of an attack relies upon identifying when there are instances (outliers) that vary from the norm (benign traffic). Approaches to achieve this can be grouped using subfields of artificial intelligence, for instance (i) supervised learning [26] (involving training autonomous security solutions on known benign traffic and outliers), (ii) unsupervised learning (where the AI algorithm does not require pretraining to detect outliers), (iii) a combination of both, where a hybrid approach leverages the benefits of the detection accuracy provided by supervised learning and also the flexibility and adaptability of unsupervised [27]; or, more recently, (iv) deep learning, using techniques known as autoencoders, able to detect outliers in traffic patterns with high success [28].

1.4.2 Honeypots

In addition to the use of proactive security systems with integrated AI, one possible solution to overcome zero-day attacks is to find the vulnerabilities using honeypots. Honeypots involve isolating traffic, deceiving the attacker into assuming they have breached the system and generate attack signatures [29] based on monitoring the behaviors within a controlled environment.

In short, the goal of a Honeypot is to let the attacker believe they are successfully breaching the system, but in fact are being studied in an artificial environment (e.g., a virtual machine) where no actual damage can be caused. The Honeypot concept is depicted in Fig. 4. Critical infrastructures adopt a *defense in depth* model, firstly involving an external perimeter consisting of an advanced intrusion detection system and firewall. Beneath this, different levels of access rights are provided depending on the staff role within the organization. The high-level layer, for example, would provide access to vital systems and would not be accessible to those with low security clearance. Between each layer, further intrusion detection systems and firewalls are in place. The Honeypot will mimic this structure, for instance as documented in many works over the last 20 years, for example, in Refs. [30–33].

1.4.3 Duqu

Related to Stuxnet, Duqu is a collection of malware which was discovered in 2011 and received far less publicity despite using much of the Stuxnet code. Duqu derives its name from the temporary files it creates on the infected device, which all start with ~DQ. Similar to Stuxnet, the malware also functions by exploiting Windows zero-day vulnerabilities [34]. A full report on Duqu is published by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics found at Ref. [34].

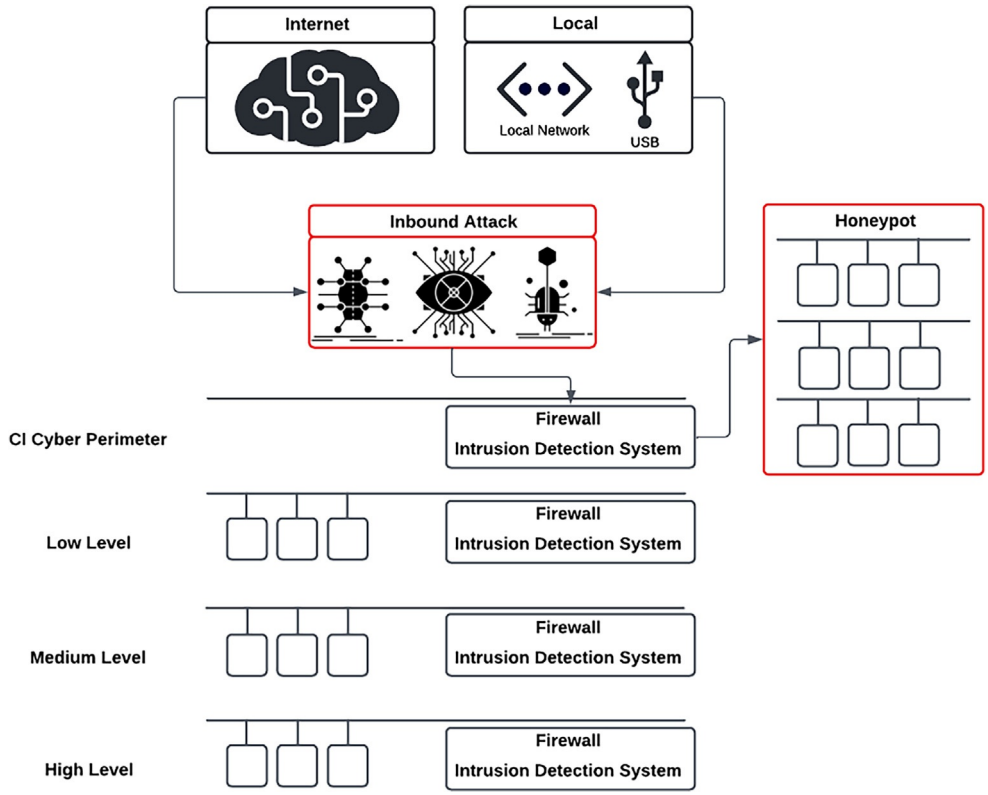

Fig. 4 Role of the Honeypot for cyber-security support.

1.5 Flame

At the time of writing this manuscript, Flame (discovered in 2012 and also recognized under the name Flamer) is documented as potentially the most complex cyber-attack ever created. Similar to Stuxnet, Flame, in the form of a trojan, has the ability to spread over a local area network (LAN) or via USB, targeting vulnerabilities within Microsoft OSs. The European Network and Information Security Agency (ENISA) document the threat of Flame in Ref. [35] and its mission as an information stealer, particularly targeted at the Middle East. Once deployed, Flame has a compilation of spying tools (documented by ENISA [35]) for listening to microphones, exfiltrating documents, tapping phones and online chats, Bluetooth scanning, taking screenshots, recording keyboard activity and intercepting Internet traffic.

Similar to Stuxnet, Flame is specifically a targeted attack, and, therefore, has infected relatively few PC devices (estimated between 100 and 1000 devices). Yet, differing from Stuxnet, Flame was designed for espionage rather than damage [36,37]. In terms of its

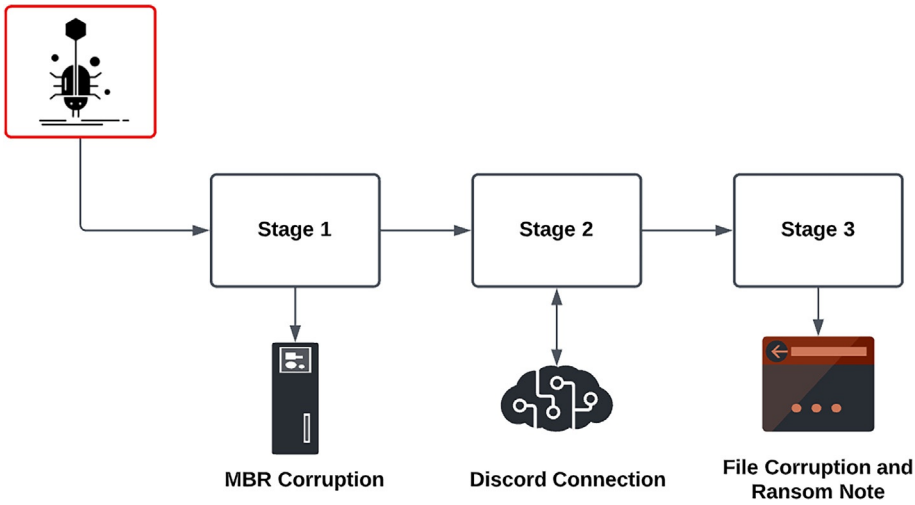

Fig. 5 High-level view of WhisperGate.

construction, Flame is uniquely larger than other viruses (approximately 20 megabytes in size) and, in result, it masquerades as a legitimate Windows update.

1.6 WhisperGate

In early 2022, a destructive malware was discovered targeting Ukrainian organizations [38]. At the time of writing this manuscript, relatively little is known about WhisperGate compared to the other aforementioned high-profile attacks given its infancy; and most information regarding the attack is found in the mainstream media and security blogs such as in Refs. [38–40] (Fig. 5).

What is known is that WhisperGate is aimed to be a destructive malware, with a technical analysis provided by the INSIKT Group at Ref. [39]. According to their article, WhisperGate is deployed in three stages (which must be executed before the PC reboots to take effect): (i) corruptions of the Master Boot Record (MBR), which in turn corrupts other drives on reboot. The MBR is then overwritten with a ransom note demanding payment and containing the details for a Bitcoin wallet; (ii) download of the malware (malicious file corrupter) needed for stage 3 which are hosted on a Discord channel; (iii) written in .NET, corruption of files on systems and network drives takes place.

1.7 Cyber-threat landscape

The emergence of the aforementioned media-documented attacks is depicted in the timeline in Fig. 6, with a summary provided in Table 1. All have specific goals and in some cases, direct targets.

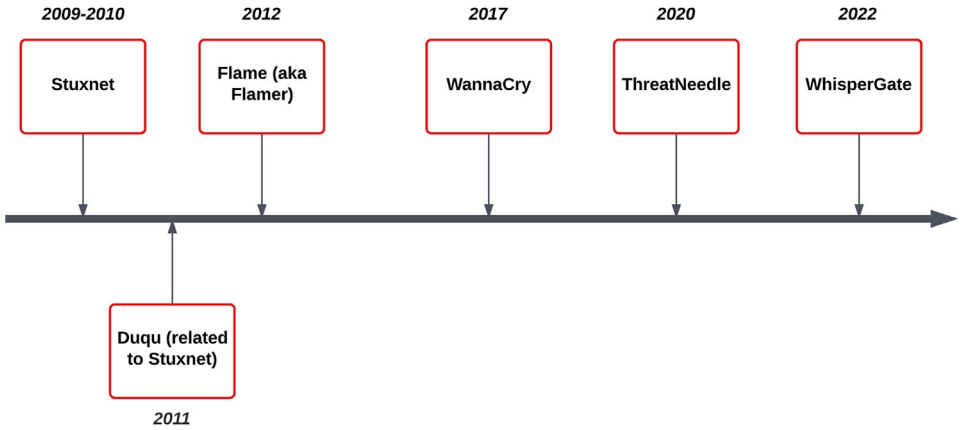

Fig. 6 Timeline of high-profile attacks.

Table 1 Comparison of high-profile attacks.

Name	Goal	Operating system
Stuxnet	Damage	Windows
Duqu	Damage	Windows
Flame	Espionage	Windows
WannaCry	Ransom	Windows
ThreatNeedle	Espionage	MAC
WhisperGate	Damage and ransom	Windows

Despite the developing landscape with varied sophistication, cyber-based security threats can still be assigned to 1 of 7 categories (Table 2), as defined in various gray literature sources, such as Refs. [42–45].

To offer a quantitative understanding of the division of these attack types within the critical infrastructure sectors, IBM Security X Force Threat Intelligence provide a detailed account of the percentages in Refs. [46,47]. Key findings from the report outline that ransomware malware accounted for 1 in 5 cyber-attacks (worldwide) in 2021 and Phishing was the top infection method, particularly in the United Kingdom against businesses where it accounted for 63% of incidents [46]. Globally, manufacturing was the most attacked infrastructure (23% of attacks), with ransomware as the main attack type. In the United Kingdom, the energy critical infrastructure sector was the main focus, with 24%, with manufacturing and finance second with 19% [46].

With this growing threat landscape, it is essential to consider how attack success continues to be possible and what methods are appropriate for securing critical infrastructures in a time of constant change. In the following section, the focus is on legacy systems, the

Table 2 Cyber-threat categories.

Cyber-threat	Description
Malware	Malware is software developed for malicious purposes, with further subcategories (spyware, ransomware, viruses and worms)
Emotet	Specifically a banking trojan, which is a type of malware but given its own unique category
Denial of Service	A process involving flooding computer networks with illegitimate requests, thus blocking legitimate access requests
Man in the Middle (MITM)	When attackers insert themselves into a two-party transaction
Phishing	Fake communication-based attack, namely using fake messages (such as emails) which seem legitimate to the user in order to request information or follow instructions which lead to the loss of information (such as a credit card number)
Structured Query Language (SQL) Injection	Involves inserting malicious code into a server that uses SQL to store data (such as customer details). In result, the server can be manipulated into releasing sensitive information
Password Attacks	Social engineering to ascertain data which can be used to trick people into providing information about their password. For instance, trending posts on social media asking for "first car," "pet names," etc. This could also include a brute-force attack, where the attack type relies on the computing power to find the correct combinations of usernames and passwords [41]

Industrial Internet of Things (IIoT), weakening segmentation and how legacy and aging systems are a considerable road block for holistic cyber-attack prevention.

2 ICS attack success

Almost all critical infrastructure sectors rely upon Industrial Control Systems (ICSs) as a core part of their operations. Unfortunately, due to the visibility and significant impact of any successful attacks, they are highly-valued targets for not only cyber-criminals but malicious state actors and politically-motivated adversaries.

Statistics published by Kaspersky highlight the severity of this issue, by showing that in the first half of 2021, 33.8% of ICS computers were attacked, which is an increase of 0.4% from the second half of 2020 [48]. This is a clear indicator that ICS-specific threats are growing. Nozomi Networks estimate that ICS shutdowns resulting from attacks cost between $225 K and $670 M [49].

There are various key themes emerging, which can help to explain why attacks against ICSs are successful, the most pertinent are summarized in this section.

2.1 Industrial internet of things

Industry 4.0 is considered to be the next industrial revolution, brought about by the integration of smart and connected systems to increase the level of automation in manufacturing and industrial processes. The integration of IIoT devices into modern critical infrastructure networks can offer various performance, cost and operational benefits. The improved connectivity facilitates increased levels of functionality, accessibility and communicability for IIoT devices. In turn, this poses significant security challenges by increasing both the security demands and breadth of the network's attack surface.

Numerous IIoT devices and their corresponding applications have been developed in existing ICS networks, which inherit or coexist with current impaired security practices and assumptions. Given the rapid evolution of such devices, it is unsurprising that for some manufacturers, security is not always a priority. This means that such devices are attractive targets for attacks and can introduce an element of uncertainty, which is not desirable in a sector renowned for its low-risk appetite. Increasingly, security concerns are being raised regarding the integrity of IIoT device supply chains and the vulnerabilities this may pose, from both software and hardware perspectives.

Many IIoT devices have limited computational power; therefore, data is commonly passed to a local or cloud-based controller for processing. Depending on the nature of the IIoT device, the sheer volume of data traversing the network or awaiting processing may introduce additional overheads. Ensuring the confidentiality and authenticity of any data transmitted is critical for avoiding common attacks (e.g., eavesdropping, replay or man-in-the-middle attacks), but the computational limitations also restrict the protocols supported for securing communications.

The use of cloud-based controllers requires the use of a IIoT gateway, which has been identified as a notable target for attacks and has garnered significant research interest [50,51]. It has been suggested that some of the security responsibilities regarding assuring device authenticity could be offloaded to a cloud-based platform. However, safety and real-time responsiveness are the most desired characteristics in an ICS. Therefore, any such security platform must be capable of real-time responses, which rules out cloud-based platforms on account of the unacceptable latency that would be introduced.

The use of cloud-based controllers for data processing and storage also raises many security questions relating to confidentiality, control and locality. This is especially important given the potential sensitivity and criticality of the data involved in ICSs.

2.2 Weakening segmentation

ICSs can be split into two distinct segments: Information Technology (IT)—hardware and software used for managing and utilizing data, and Operational Technology (OT)—hardware and software used to monitor and control industrial equipment. Historically, there has always been physical segmentation between the IT and OT segments

of an ICS, known as an *air gap*. However, the continued adoption of IIoT and the shifting of applications, data and infrastructure to cloud providers has eroded network perimeters and this separation. This has resulted in the increasing convergence of IT and OT network segments, sometimes unbeknownst to operators. The exposure of ICS protocols to the internet can provide new attack surfaces and can lead to unusual and unwanted behavior. Shodan's ICS Radar crawls the Internet and detects direct access to ICSs [52], at the time of writing, there were over 55,000 systems accessible. The most common core ICS protocols supported by these accessible systems were ModBus, Siemens S7 and DNP3.

Some ICSs are embracing the convergence by blending technologies between the segments, e.g., using IT-side database technologies for OT. Unfortunately, many ICSs security practices have not been modernized to accommodate this. There is an over-reliance on proprietary protocols as a form of protection, this is an example of security-through-obscurity, which is not an effective security strategy.

Many ICSs are not prepared for defense against malware, and they rely on the OT practices of old and do not embrace modern cyber-security approaches. Vulnerable to many attacks such as eavesdropping, interception, replay and DoS. An increasingly common attack pattern is for the initial attack vector to reside within the IT segment and the attacker to pivot into the OT segment [53], notable examples include EKANS and Havex. The significance of this convergence is emphasized by the initial stage of the ICS Cyber Kill Chain, which is focused on intelligence gathering [54]. The top 3 initial attack vectors for ICSs are external remote services, exploiting public-facing applications and internet accessible devices [55].

The convergence has exposed ICS protocols designed for use in air gapped systems, being introduced to the wider internet. Air gaps have previously been depended upon as a defensive strategy but even in traditional networks, there were still situations where the gap was bridged. Examples of this include the transfer of config files and software patches from IT to OT (whether physically or digitally).

2.3 ICS protocol weakness

Many of the protocols utilized in ICSs are proprietary and were originally designed based upon the security assumptions of older serial-based and/or air gapped systems. Therefore, the majority of original protocols were focused on functionality and efficiency, whereas security was not factored into their designs [56]. The inherent and fundamental security issues associated with such protocols [57], especially when combined with poor documentation and maintenance practices, significantly increases the risk faced by ICSs. With many of these protocols still in use [58], it emphasizes the concern over the IT/OT convergence. This is further evidenced by Bratus et al.'s LZFuzz security fuzzing tool, which proved most successful when applied to proprietary and poorly documented protocols.

The most common core ICS protocols currently in use are Modbus, EtherNet/IP and S7comm [53]. Therefore, these three have been focused upon to examine their security attributes.

2.3.1 Modbus

The Modicon Communication Bus (Modbus) protocol is one of the oldest and widely used protocols. It was originally designed in 1979 for RS-232 or RS-485 serial networks between computationally limited microcontrollers [59]. In recent times, the protocol has migrated to being ethernet-based (Modbus TCP). Both versions of this protocol are based on the assumption that there would be limited physical access to the network, therefore negating security requirements. The resulting simplicity and efficiency of the protocol has made it popular.

However, as networking has evolved, there are increasing requirements for communications to be made from within LANs or WANs. This poses a significant problem, as Modbus was never designed for this type of use and appropriate security mechanisms are not provided. Furthermore, due to required backwards compatibility, this is not something that can or will be easily changed (although the Modbus Security Protocol has been introduced as an alternative solution). Some of the security concerns with the TCP-based variant are summarized in Table 3.

2.3.2 EtherNet/IP

EtherNet/IP (here IP stands for Industrial Protocol, not Internet Protocol) is an adaptation of Rockwell's Common Industrial Protocol (CIP), providing networking through the use of standard Ethernet frames. There are two types of communication in EtherNet/IP, implicit and explicit [60]. Implicit communication is used for I/O data transfer, and it is performed over UDP to leverage the speed and latency benefits, allowing the use of producer-consumer model. Explicit communication is used for nontime critical data and is performed over TCP.

CIP uses three object classes to define characteristics of a device: Required Objects (defines attributes e.g., identifiers, manufacturer and serial number), Application Objects (defines input and output for devices) and Vendor-specific objects (defines proprietary attributes). Its functionality can be considered similar in some respects to SNMP. To increase interoperability and cross-vendor support, objects (except Vendor-specific Objects) are standardized by device type and/or function. Some of the security concerns relating to the base protocol (i.e., not using CIP Security) are clarified in Table 4.

The existing CIP standards have not been updated to accommodate increased security requirements, in order to maintain compatibility. Instead, CIP security has been introduced as an alternative protocol that addresses most of the security limitations of the original protocol.

Table 3 Modbus TCP security concerns.

Concern	Description
Confidentiality	Modbus communications are all transmitted in clear text, offering no protection against eavesdropping, command injection or MiTM attacks
Integrity	Modbus does not support any integrity checks of the transmitted data, such as message checksums
Authentication	Modbus operates using a master/slave model, requiring only a valid address to communicate, there is no authentication used in the protocol. Therefore, there is no mechanism to verify the authenticity of devices, which facilitates various attacks such as identification of slave devices, DoS and spoofing attacks. Similarly, there is no session management used within Modbus, making replay attacks possible
Authorization	Modbus does not perform any authorization checks to ensure that privileged actions can only be performed by specific entities. Master and slave components will action valid commands received, without any security checks. Therefore, unauthorized/malicious commands can be executed by attackers
Accountability	As Modbus does not support authentication, there is no facility to maintain an audit trail
Simplicity	Although seen as a positive attribute for ease of implementation, the simplicity of the protocol and its structure makes reconnaissance activities by attackers much easier
Purpose	Part of the protocol's purpose is the programming of controllers; therefore, the repercussions of ineffective security can be severe

Table 4 EtherNet/IP security concerns.

Concern	Description
Confidentiality	Communications are transmitted in clear text, offering no protection against eavesdropping attacks or MITM attacks
Integrity	No network-based checks are performed to validate integrity, thus allowing data tampering to occur
Authentication	The lack of verification of users/devices allows for disruptive changes (e.g., change device's IP) to be made by untrusted parties [61] or the launching of replay attacks. Furthermore, the protocol is based on UDP, which is stateless and offers no transmission control mechanism to help in preventing spoofing
Availability	Various implementation weaknesses have been exposed by researchers, which facilitate DoS attacks. For example, weak session ID generation and improper TCP timeout [62]
Multicast traffic	Multicast traffic is utilized within the protocol to reduce network traffic load. However, this also lacks transmission control mechanisms and is unable to prevent transmission path manipulation using injected IGMP packets
Standardization	Unfortunately, standardizing Required and Application Objects has made common devices much easier to identify and exploit during attacks

Table 5 S7Comm security concerns.

Concern	Description
Confidentiality	The protocol provides no encryption functionality, so it is unable to prevent eavesdropping or MITM
Integrity	The protocol doesn't offer any integrity mechanisms, meaning it cannot prevent data/command modification or replay attacks [63]
Authentication	Some PLCs can be configured to utilize basic password protection for certain operations. However, this offers limited protection as password lengths are constrained. Passwords are supplied for authentication as hashes but are sent in clear text. When this is combined with the lack of confidentiality and integrity, it enables passwords to be replayed and rainbow table attacks
Authorization	Passwords can be used to prevent unauthorized actions, but various attacks are possible to bypass any protection afforded [64]
Documentation	There is limited documentation available for the protocol [65], suggesting security through obscurity is utilized as a form of protection, which is widely considered poor practice

2.3.3 Siemens S7Comm

S7 Communication (S7Comm) is a proprietary protocol from Siemens first introduced in 1994 for data transfer and programming of its S7 family of PLCs. There are three versions of the protocol: S7Comm, S7CommPlus v1 and S7CommPlus v2.

Similar to the previous protocols, S7Comm was deployed with inadequate security protection, which was infamously exploited by the Stuxnet worm. Some of the main concerns of this protocol are summarized in Table 5.

In response to the vulnerabilities exploited by Stuxnet, S7CommPlus v1 was released, which utilizes session IDs to prevent replay attacks. However, researchers identified that the mechanism used to generate the IDs was too simplistic and could be exploited and sessions stolen [64].

S7CommPlus v2 improves upon the vulnerabilities of the previous versions by utilizing encryption as well as improved antireplay mechanisms and an integrity check mechanism. However, researchers have demonstrated that these improvements can be broken too [66].

2.3.4 Weakness trends

As evidenced throughout this subsection, the flawed and outdated assumptions of physical isolation that underpin many ICS protocols are the primary cause of most security issues. Compatibility is commonly cited as the reason behind not improving existing protocol standards to meet basic security goals. Although the three protocols discussed all have security enhanced versions of the original protocols to overcome these issues, many live implementations have not, or are unable to, adopt these enhanced versions. Unfortunately, this seems to be a representative picture across the sector, and the evolution of

ICSs will continue to expose the security weaknesses and vulnerabilities of these protocols.

2.4 Legacy/aging systems

ICS systems are intended to have significantly longer operational lifespans (typically 20–25 years), than commodity systems [67], so components will inevitably be considered as legacy at some point. Therefore, the standards, principles, security assumptions and anticipated threats originally used to devise architectural designs could be significantly outdated. Similarly, cutting-edge protocols and software used for implementation at the time will rapidly become outdated given the pace of technological evolution. For instance, there are numerous examples of End-Of-Life (EOL) operating systems such as Windows XP still being used [68].

Future-proofing systems decades in advance cannot be accurately accomplished. So it is unsurprising that such systems are inadequately equipped and secured for modern requirements. Furthermore, given the critical nature of these systems and their required stability, continuous development (as seen with commodity systems) is not a desirable characteristic.

One crucial example of this is the inherent security limitations of ICSs, original designs accommodated the differing priorities and needs of the IT and OT segments. As OT systems were typically air gapped, availability was prioritized over confidentiality and integrity [69] (e.g., availability of critical sensor readings is far more important than their confidentiality).

Facilitating the modern connectivity requirements of ICSs often requires legacy systems to be used or configured in ways that they were not originally designed for, or the retrofitting of additional components. Such alterations deviate from the original design and can result in unexpected behavior, as well as the introduction of new weaknesses and vulnerabilities. The continued blurring of boundaries that used to exist between IT and OT is increasing the visibility of basic security shortcomings in the OT segments, e.g., lack of encryption, poor/no authentication, weak/default passwords [70]. A common example of this is the migration from serial-based to IP-based communications, the level of internet exposure and attack surface expansion are often not fully considered.

2.5 ICS summary

As the modern connectivity requirements of ICSs continue to shift toward greater internet accessibility, the exposed surface of these systems will become increasingly scrutinized for credible attack vectors. Throughout this section, only a few of the reasons behind successful ICS attacks have been covered, there are many more contributory factors. However, it is clear that the probability of security problems occurring and the severity of associated impacts are only going to increase. There is therefore a need to focus upon

factoring security into the design of an ICS (for both new and existing systems), rather than the continued approach of retrofitting. Similarly, ICS security needs to orient toward a holistic approach, which encompasses both IT and OT segments, rather than adopting a siloed approach with separate expertise.

3 Conclusion

Future cyber-security focus is orienting toward IIoT security, smart home appliances and data storage devices, where the pervasiveness of personal information stored across multiple devices (laptops, PCs, smart phones, etc.) has increased the entry point of hackers [42]. Further, IBM details that in 2021 the global shift in work habits as a result of the Covid-19 pandemic forcing many to work from home, created opportunities for threat activators to infiltrate organizations [47].

Ensuring the security of critical infrastructure systems poses an ongoing challenge, with failings having potentially catastrophic consequences. A significant hurdle is the ever-increasing number of critical infrastructure components that are now directly or indirectly exposed to the internet, causing potential attack surfaces and associated risks to grow. Similarly, the heterogeneity of such devices also contributes to increasing the attack surface and adds additional complexity when coordinating defensive efforts.

There are three emerging attack patterns of significance, which need to be adequately considered to ensure the future security of critical infrastructures. These are:

1. **Supply chain attacks**—Attacks are no longer directly launched directly against the intended organization or system. Instead, weaker elements of the supply chain are targeted offer greater opportunity to inflict widespread damage. A notable global example of this was the Solar Winds attack in 2020. Usually, targets for this type of attack will be third-party vendors or suppliers, with poor cyber-security. Some of the example techniques used include software weaknesses, firmware backdoors, preinstalled malware installation and certificate theft.
2. **Top-down infrastructure attacks**—Traditionally, attacks have followed a bottom-up approach due to the perimeter security model adopted by many. Here, the exposed elements of a system (usually lower value assets) are exploited, and attackers work to elevate their access to the higher value targets afforded greater protection. However, with the shift to cloud-based services, assets that were typically well-protected from internet exposure (e.g., Active Directory servers) are now increasingly accessible online. Hence, attackers can now directly target these high-value cloud-based administrative/management systems, instead of having to work to elevate themselves to this point.
3. **Ransomware**—Unfortunately, this type of attack is common throughout many types of networks. However, a recent Claroty report estimated that around 80% of critical infrastructures had been subject to ransomware and around 60% had paid

the ransom [71]. The very nature of critical infrastructure means that any impairment of functionality can have devastating consequences; hence, targets are far more likely to pay. Given the likelihood of success, and the increased attack surface created by IT and OT mergence, it is inevitable that attackers will be prioritizing attacks against these systems.

Thus, *could one solution be for better use of AI*? For instance, IBM details that organizations who have a fully deployed security-based AI and automation had lower costs associated with breaches ($2.9million vs $6.71 million) compared to organizations without AI [72]. Further, as indicated in current scientific literatures, the level of preparedness is dependent on two factors: (i) the use of more effective intrusion detection processes; (ii) the types of security techniques. Panagiotis et al. provide a comprehensive list in their review article in Ref. [41], discussing some of the most well-known algorithms and models integrated into security systems for better overall resilience, focusing primarily on machine learning and deep learning. Within this domain, AI-based approaches (specifically machine learning techniques) such as K-means, Naive Bayes, support vector machines, decision trees and density-based spatial clustering of applications with noise have all been used with effect in research-based approaches [73–75]. Building on this, deep learning models are becoming increasingly employed, namely the use of autoencoders, long short-term memory networks (LSTMs), recurrent neural networks (RNNs) and convolutional neural networks (CNNs) [76–78]. Research demonstrates that AI-driven approaches are the way forward to a holistic security system. The challenge remains—translating research findings into real-world implemented systems to counter the level of sophistication discussed in Section 1.

References

[1] I. Ghafir, J. Saleem, M. Hammoudeh, et al., Security threats to critical infrastructure: the human factor, J. Supercomput. 74 (2018) 4986–5002.
[2] G.M. Karagiannis, Z.I. Turksezer, L. Alfier, L. Feyen, E. Krausmann, Climate Change and Critical Infrastructure—Floods, European Commission, Science for Policy Report, Brussels, 2019.
[3] K.V. Ruiten, T. Bles, J. Kiel, EU-INTACT-case studies: impact of extreme weather on critical infrastructure, in: European Conference on Flood Risk Management (FLOODrisk 2016), Lyon, 2016.
[4] B. Bennett, Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructures, Wiley, 2018.
[5] Z. Xindi, C. Krishna, Critical infrastructure security against drone attacks using visual analytics, in: Computer Vision Systems, Lecture Notes in Computer Science, vol. 11754, 2019.
[6] B. Kai, C. Charmaine, The counter sovereignty of critical infrastructure security: settler-state anxiety versus the pipeline blockade, Antipode (2021) 1–23.
[7] M. Rong, C. Han, L. Liu, Critical infrastructure failure interdependencies in the 2008 Chinese Winter Storms, in: International Conference on Management and Service Science, Wuhan, 2010.
[8] P. Wagner, Critical Infrastructure Security, 2021, Available at SSRN: https://ssrn.com/abstract=3762693.
[9] ICS Cert, IT threat evolution in Q2 2021. PC statistics, Kaspersky (2021). 12 August. Available from: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/. (Accessed 20 January 2022).

[10] S. Ghafur, S. Kristensen, K. Honeyford, A retrospective impact analysis of the WannaCry cyberattack on the NHS, NPJ Digit. Med. 98 (2) (2019).
[11] Z. Whittaker, Two years after WannaCry, a million computers remain at risk, TechCrunch (2019). 12 May. Available from: https://techcrunch.com/2019/05/12/wannacry-two-years-on/. (Accessed 20 January 2022).
[12] M. Kumar, TSMC chip maker blames WannaCry malware for production halt, The Hacker News Media (2018). 7 August. Available from: https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html. (Accessed 14 February 2022).
[13] D. Goodin, >10,000 Windows computers may be infected by advanced NSA backdoor, ars Technica (2017). 21 April. Available from: https://arstechnica.com/information-technology/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/. (Accessed 8 March 2022).
[14] ICS CERT, PseudoManuscrypt: a mass-scale spyware attack campaign, Kaspersky (2021). 16 December. Available from: https://securelist.com/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/105286/. (Accessed 19 January 2022).
[15] ICS CERT, Lazarus targets defense industry with ThreatNeedle, Kaspersky (2021). 25 February. Available from: https://securelist.com/lazarus-threatneedle/100803/. (Accessed 20 January 2022).
[16] New Jersey Cybersecurity & Communications Integration Cell, NukeSped, NJCCIC Threat Profile (2019). 10 December. Available from: https://www.cyber.nj.gov/threat-center/threat-profiles/macos-malware-variants/nukesped. (Accessed 20 January 2022).
[17] P. Wardle, Lazarus Group Goes 'Fileless', Objective-See, 2019. 3 December. Available from: https://objective-see.com/blog/blog_0x51.html. (Accessed 20 January 2022).
[18] D. Kushner, The real story of stuxnet, IEEE Spectr. 50 (3) (2013) 48–53.
[19] L. Bilge, T. Dumitras, Before we knew it: an empirical study of zero-day attacks in the real world, in: ACM Conference on Computer and Communications Security, Raleigh North Carolina, 101, 2012.
[20] P. Mueller, B. Yadegari, The stuxnet worm, in: Political Science, University of Arizona, Arizona, USA, 2012, pp. 1–12.
[21] Microsoft, Microsoft security bulletin MS08-067—critical, Microsoft (2019). 12 March. Available from: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067. (Accessed 22 February 2022).
[22] X. Sun, J. Dai, P. Liu, A. Singhal, Using Bayesian networks for probabilistic identification of zero-day attack paths, IEEE Trans. Inf. Forensics Secur. 13 (10) (2018) 2506–2521.
[23] N. Sameera, M. Shashi, Deep transductive transfer learning framework for zero-day attack detection, ICT Express 6 (4) (2020) 361–367.
[24] V. Sharma, J. Kim, S. Kwon, I. You, K. Lee, K. Yim, A framework for mitigating zero-day attacks in IoT, in: CISC-S'17, Sinchang-Asan, 2017.
[25] F. Abri, S. Siami-Namini, M.A. Khanghah, F.M. Soltani, A.S. Namin, The performance of machine and deep learning classifiers in detecting zero-day vulnerabilities, in: IEEE BigData, 2019. arXiv:1911.09586v1.
[26] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, Zero-day malware detection based on supervised learning algorithms of API call signatures, in: Australasian Data Mining Conference, Ballarat, 2011.
[27] P.M. Comar, L. Liu, S. Saha, P.-N. Tan, A. Nucci, Combining supervised and unsupervised learning for zero-day malware detection, in: Proceedings of IEEE INFOCOM, Turin, 2013.
[28] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, X. Bellekens, Utilising deep learning techniques for effective zero-day attack detection, Electronics 9 (2020) 1684.
[29] C. Musca, E. Mirica, R. Deaconescu, Detecting and analyzing zero-day attacks using honeypots, in: International Conference on Control Systems and Computer Science, Bucharest, 2013.
[30] Y.M.P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, IoTPOT: a novel honeypot for revealing current IoT threats, J. Inf. Process. 24 (3) (2016) 522–533.
[31] M.L. Bringer, C.A. Chelmecki, H. Fujinoki, A survey: recent advances and future trends in honeypot research, Int. J. Comput. Netw. Inf. Secur. 10 (2012) 63–75.
[32] M. Nawrocki, M. Wählisch, T.C. Schmidt, C. Keil, J. Schönfelder, A survey on honeypot software and data analysis, arXiv:1608.06249, ACM, 2016.
[33] N. Provos, A virtual honeypot framework, in: Usenix Security Symposium, San Diego, 2004.

[34] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi, Duqu: A Stuxnet-Like Malware Found in the Wild, Laboratory of Cryptography and System Security (CrySyS), 2011. 14 October.
[35] ENISA, The Threat From Flamer, European Network and Information Security Agency, Brussels, 2012.
[36] R. Cohen, New massive cyber-attack an 'industrial vacuum cleaner for sensitive information', Forbes (2012). 28 May. Available from: https://www.forbes.com/sites/reuvencohen/2012/05/28/new-massive-cyber-attack-an-industrial-vacuum-cleaner-for-sensitive-information/. (Accessed 24 February 2022).
[37] D. Lee, Flame: massive cyber-attack discovered, researchers say, BBC News (2012). 28 May. Available from: https://www.bbc.com/news/technology-18238326. (Accessed 24 February 2022).
[38] Microsoft, Destructive Malware Targeting Ukrainian Organizations, Microsoft Security, 2022. 15 January. Available from: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/. (Accessed 24 February 2022).
[39] INSIKT Group, WhisperGate malware corrupts computers in Ukraine, 2022, 28 January. Available from: https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/. (Accessed 24 February 2022).
[40] CrowdStrike, Technical Analysis of the WhisperGate Malicious Bootloader, CrowdStrike Intelligence Team, 2022. 19 January. Available from: https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/. (Accessed 24 February 2022).
[41] F. Panagiotis, K. Taxiarxchis, K. Georgios, L. Maglaras, M. Ferrag, Intrusion detection in critical infrastructures: a literature review, Smart Cities 4 (2021) 1146–1157.
[42] University of North Dakota, 7 Types of Cyber Security Threats, University of North Dakota, 2022. Available from: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/. (Accessed 8 March 2022).
[43] Guru Schools, 7 Types of Cyber Security Threats, Guru Schools, 2019. 5 November. Available from: https://guruschools.com/7-types-of-cyber-security-threats/. (Accessed 8 March 2022).
[44] C. Evans, 7 Types of Cyber Security Attacks With Real-Life Examples, E-Tech, 2021. 16 September. Available from: https://www.etechcomputing.com/7-types-of-cyber-security-attacks-with-real-life-examples/. (Accessed 8 March 2022).
[45] Jaro Education, 7 Types of Cyber Security Threats, Jaro Education, 2022. Available from: https://www.jaroeducation.com/blog/7-types-of-cyber-security-threats/. (Accessed 8 March 2022).
[46] G. Hastings, IBM security report: energy sector becomes UK's top target for cyberattacks as adversaries take aim at nation's critical industries, 2022, 23 February. Available from: https://uk.newsroom.ibm.com/2022-02-23-IBM-Security-Report-Energy-Sector-Becomes-UKs-Top-Target-for-Cyberattacks-as-Adversaries-Take-Aim-at-Nations-Critical-Industries?utm_medium=OSocial&utm_source=Twitter&utm_content=CAAWW&utm_id=Twitter-XforceUKI-2022-0. (Accessed 24 February 2022).
[47] IBM Security X-Force, Manufacturing Becomes the World's Most Attacked Industry, 2022, Available from: https://www.ibm.com/security/data-breach/threat-intelligence/. (Accessed 8 March 2022).
[48] ICS CERT, Threat landscape for industrial automation systems. Statistics for H1 2021, Kaspersky (2021). 9 September. Available from: https://ics-cert.kaspersky.com/publications/reports/2021/09/09/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2021/. (Accessed 14 February 2022).
[49] Nozomi Networks, The Cost of OT Cybersecurity Incidents and How to Reduce Risk, Nzomi Networks, 2020.
[50] C.H. Chen, M.Y. Lin, C.C. Liu, Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers, IEEE Netw. 32 (1) (2018) 24–32.
[51] T. Gong, S. Zheng, M. Nixon, E. Rotvold, S. Han, Demo abstract: industrial IoT field gateway design for heterogeneous process monitoring and control, in: IEEE Real-Time and Embedded Technology, Porto, 2018.
[52] Shodan ICS Radar, Shodan, Available from: https://ics-radar.shodan.io/, 2022 (Accessed 11 February 2022).

[53] D. Masson, Darktrace, 2020, 6 August. Available from: https://www.darktrace.com/en/blog/darktrace-ot-threat-finds-defending-the-widening-attack-surface/. (Accessed 11 February 2022).
[54] M.J. Assante, R.M. Lee, The industrial control system cyber kill chain, Sans Institute White Paper, 2015, pp. 1–23.
[55] M. Bristow, A SANS 2021 survey: OT/ICS cybersecurity, in: Nozomi Networks, SANS Institute, 2021, pp. 1–23.
[56] M. Conti, D. Donadel, F. Turrin, A survey on industrial control system testbeds and datasets for security research, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2248–2294.
[57] G.P.H. Sandaruwan, P.S. Ranaweera, V.A. Oleshchuk, PLC security and critical infrastructure protection, in: IEEE 8th International Conference on Industrial and Information Systems, Peradeniya, 2013.
[58] G. Barbieri, M. Conti, N.O. Tippenhauer, F. Turrin, Assessing the Use of Insecure ICS Protocols via IXP Network Traffic Analysis, arXiv:2007.01114, 2020.
[59] Modbus.org, MODBUS Over Serial Line: Specification & Implementation Guide V1.0, 2002. 2-12-2002 (Accessed March 2022).
[60] I. Open DeviceNet Vendor Association, Ethernet/IP quick start for vendors hand, ODVA, Ann Arbor, MI, 2008. Tech. Rep.
[61] B. Batke, J. Wilberg, D. Dube, CIP security phase 1 secure transport for EtherNet/IP, in: Industry Conference and Annual Meeting, Frisco, Texas, 2015.
[62] R. Grandgenett, R. Gandhi, W. Mahone, Exploitation of Allen Bradley's implementation of EtherNet/IP for denial of service against industrial control systems, in: 9th International Conference on Cyber Warfare and Security, West Lafayette, Indiana, 2014.
[63] A. Ghaleb, S. Zhioua, A. Almulhem, On PLC network security, Int. J. Crit. Infrastruct. Prot. 22 (2018) 62–69.
[64] H. Hui, K. McLaughlin, S. Sezer, Vulnerability analysis of S7 PLCs: manipulating the security mechanism, Int. J. Crit. Infrastruct. Prot. 35 (2021) 100470.
[65] L. Martín-Liras, M.A. Prada, J.J. Fuertes, A. Morán, S. Alonso, M. Domínguez, Comparative analysis of the security of configuration protocols for industrial control devices, Int. J. Crit. Infrastruct. Prot. 19 (2017) 4–15.
[66] C. Lei, L. Donghong, M. Liang, The Spear to Break the Security Wall of S7CommPlus, Blackhat, 2016. Available from: https://www.blackhat.com/docs/eu-17/materials/eu-17-Lei-The-Spear-To-Break%20-The-Security-Wall-Of-S7CommPlus-wp.pdf. (Accessed 14 February 2022).
[67] S.P. McGurk, Industrial Control Systems Security, Homeland Security, 2008. December. Available from: https://csrc.nist.gov/CSRC/media/Events/ISPAB-DECEMBER-2008-MEETING/documents/ICSsecurity_ISPAB-dec2008_SPMcGurk.pdf. (Accessed 14 February 2022).
[68] CyberX, 2019 Global ICS and IIoT Risk Report, CyberX-Labs, 2019 (Accessed 11 February 2022).
[69] S. Abe, M. Fujimoto, S. Horata, Y. Uchida, T. Mitsunaga, Security threats of internet-reachable ICS, in: Annual Conference of the Society of Instrument and Control Engineers of Japan, Tsukuba, 2016.
[70] Mandiant, What About the Plant Floor? 2022, Available from: https://www.mandiant.com/resources/six-subversive-security-concerns-for-industrial-environments. (Accessed 11 February 2022).
[71] Claroty, Claroty Biannual ICS Risk & Vulnerability Report: 2H 2021, Team82, 2021. Available from: https://claroty.com/2h21-biannual-report/. (Accessed 14 February 2022).
[72] IBM Corporation, Cost of a Data Breach Report, IBM Security, Armonk, NY, 2021.
[73] J.-H. Li, Cyber security meets artificial intelligence: a survey, Front. Inform. Technol. Electron. Eng. 19 (2018) 1462–1474.
[74] H.M. Farooq, N.M. Otaibi, Optimal machine learning algorithms for cyber threat detection, in: UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim), Cambridge, UK, 2018.
[75] Y. Fan, K. Tian, X. Wang, Z. Lv, J. Wang, Detecting intrusions in railway signal safety data Networks with DBSCAN-ARIMA, Front. Cyber Secur. 1286 (2020) 254–270.
[76] M. Banton, N. Shone, W. Hurst, Q. Shi, Intrusion detection using extremely limited data based on SDN, in: IEEE 10th International Conference on Intelligent Systems (IS), Varna, Bulgaria, 2020.

[77] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, Machine learning and deep learning methods for cybersecurity, IEEE Access 6 (2018) 35365–35381.
[78] S.A. Salloum, M. Alshurideh, A. Elnagar, K. Shaalan, Machine learning and deep learning techniques for cybersecurity: a review, in: Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020), Cairo, Egypt, 2020.