Looking Back to Look Forward: Lessons Learnt from Cyber-Attacks on Industrial Control Systems

Thomas Miller

Lancaster University, LA1 4WA, United Kingdom

Alexander Staves

Lancaster University, LA1 4WA, United Kingdom

Sam Maesschalck

Lancaster University, LA1 4WA, United Kingdom

Miriam Sturdee

Lancaster University, LA1 4WA, United Kingdom

Benjamin Green

Lancaster University, LA1 4WA, United Kingdom

Abstract

Since the 1980s, we have observed a range of cyberattacks targeting Industrial Control Systems (ICS), some of which have impacted elements of critical national infrastructure (CNI). While there are access limitations on information surrounding ICS focused cyberattacks, particularly within a CNI context, this paper provides an extensive summary of those publicly reported. By identifying and analysing previous ICS focused cyberattacks, we document their evolution, affording cyber-security practitioners with a greater understanding of attack vectors, threat actors, impact, and targeted sectors and locations, critical to the continued development of holistic risk management strategies.

Keywords: Industrial Control Systems, ICS, Cyber-Physical Systems, Cyber Attacks, Threat
Disclaimer: The definitive version is published at the International Journal of Critical Infrastructure Protection under this DOI: `https://doi.org/10.1016/j.ijcip.2021.100464`

1. Introduction

Industrial Control Systems (ICS) comprise a unique set of hardware and software used in the operation of complex industrial processes, some of which underpin Critical National Infrastructure (CNI). Throughout the years, there has been a clear development of ICSs across three generations: – Monolithic, Distributed, and Networked. Although all ICSs are unique in their own way, they share standard components and logical frameworks. For example, the Purdue Model [1] for control hierarchy, which dissects ICSs into zones and levels, as shown in Figure 1. These zones are defined as: The *Safety Zone* which comprises of components that are used to ensure safe operations; the *Manufacturing Zone* consisting of components that are used for monitoring, control, and automation of physical processes; the *Demilitarized Zone* which provides a bridge to share data between the Manufacturing Zone and the Enterprise Zone; and finally the *Enterprise Zone* which contains traditional IT devices and systems, utilising data fed from the Manufacturing Zone via the Demilitarized Zone. The increased interconnectivity of ICSs intro-

Email addresses: `t.miller@lancaster.ac.uk` (Thomas Miller), `a.staves@lancaster.ac.uk` (Alexander Staves), `s.maesschalck@lancaster.ac.uk` (Sam Maesschalck), `m.sturdee@lancaster.ac.uk` (Miriam Sturdee), `b.green2@lancaster.ac.uk` (Benjamin Green)

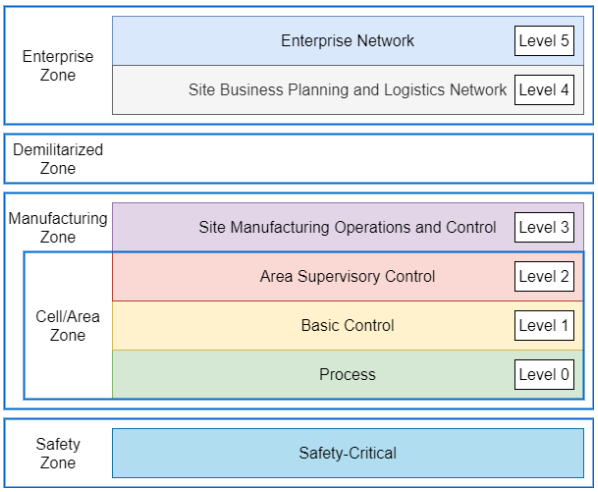

Figure 1: The Purdue Model for Control Hierarchy [1]

duces new cybersecurity challenges. If identified and exploited by adversaries, attacks could result in operational process shutdown, financial loss, damaged equipment, and even the loss of human life [2]. Since the 1980s we have observed a range of cyberattacks targeting ICSs, including elements of CNI. In tracking historical attacks, a wealth of information can be obtained, useful in the security, maintenance, and development of ICSs.

In this paper, we explore a large set of publicly disclosed cyberattacks targeting ICSs. These attacks have been selected based on the quality of the publicly available information. Through an associated analysis using the STIX and MITRE ICS ATT&CK frameworks as a foundational structure, we provide information on targeted infrastructures, targeted geographic locations, threat actor characteristics, initial access techniques, and observed impact trends. This analysis also leads to the creation of a graphical ICS cyberattack timeline. In identifying, analysing, and comprehending historic cyberattacks, risk can be more comprehensively understood, and deficiencies in current best-practice can be addressed.

The core contributions of this paper are as follows:

1. A comprehensive list of ICS historical attacks;
2. a methodology for the analysis of ICS attacks;
3. an analysis of ICS attacks, including attack trends;
4. and, lessons learnt with suggested actions to improve security capabilities.

The remainder of this paper is structured as follows: Section 2 covers related work. Section 3 provides a description of forty-three ICS cyber attacks. Section 4 discusses three key ICS attacks, namely Stuxnet, Triton and BlackEnergy, in more depth. Section 5 provides an analysis of the summarised cyberattacks from Section 3, focusing on lessons learnt. Section 6 concludes the paper and discusses future work.

2. Related Work

Existing academic work has already been undertaken on the collation of cyber-attacks against ICSs [3, 4, 5]; however, attack coverage and their associated detail are limited. In Derbyshire et al. [3], twenty attacks are used to support a discussion on attack taxonomies. As these attacks are used in a supporting capacity, they are introduced at a high-level with no focused analysis. Within Hemsley & Fisher [5], a discussion is provided on twenty-three attacks. Unlike Derbyshire et al. [3], this paper is primarily focused on the attacks themselves, and is, therefore, more comprehensive. However, it excludes many noteworthy attacks and does not provide a single centralised resource summarising key findings. In Miller & Rowe [4], fifteen ICS incidents in CNI are identified and analysed. However, it too excludes a significant number of noteworthy attacks and uses vague sector categorisation.

In addition to the aforementioned academic work, cybersecurity-focused companies have provided extensive white papers focusing on a subset of ICS attacks [6, 7, 8, 9, 10]. In [7], Dragos provide an evaluation of historical and future attacks on industrial environments. The evaluation of the attacks detailed is in-depth. However, a considerable number of attacks are excluded – similar to academic works [4, 5]. Panda Security [6] provide a list of fourteen attacks to exhibit an increasing magnitude of attacks against ICSs. FireEye [8] provide a top twenty list of cyber-attacks on ICSs which focuses on attack-types. Although this report's core focus is not historical attacks, it still uses them to justify their ranked lists. This may be valuable to cybersecurity specialists, giving them a more prominent understanding of attack vectors. PandaSec [6] and FireEye [8] provide a partial collation of historical attacks on ICSs. However, these attacks are used in a supporting capacity with no analysis. Since 2016, Kaspersky [10] have provided a biannual report on the threat landscape for industrial automation systems using statistical data obtained from their Kaspersky Security Network (KSN). This provides an analysis of trends for each half of the year, and a comparison with previous years. Although a comprehensive analysis is provided, it only focuses on the past four years and ICSs connected to the KSN. Therefore, we argue that it provides

an incomplete list of attacks. SANS [9] state that cyber-attacks on ICSs differ in impact due to a variety of factors, e.g. (intent and capabilities). Therefore, they propose an ICS Cyber Kill Chain (CKC) to help defenders comprehend the adversaries attack campaign. Within the publication, case studies are examined with the ICS CKC to provide validation and insight. Although this provides a detailed insight into attacks, a small sample of case studies is provided.

Most importantly, the main focus of commercial reports is to advertise a product. Therefore, the information within them is used to promote focused offerings which leaves the potential to omit attacks or data that are out of scope. In addition to this, not all companies provide a single centralised resource to examine a comprehensive list of attacks. This comprehensive list, and analysis, can afford cybersecurity practitioners with a greater understanding of ICS attacks which is critical to the continued development, maintenance, and security of ICSs.

Across the literature in this section, we have identified that existing works do not provide a comprehensive list of ICS historical attacks and comparative analysis. Therefore, the following section will provide a comprehensive list of ICS attacks, including a method for their identification.

3. Historical Attacks on ICS

To identify additional attacks, and due to these attacks' nature, we searched ICS related news sources, white papers, and case studies to provide a comprehensive list of attacks to discuss and analyse. To provide a comprehensive list, we must first define an ICS incident; an ICS incident is an attack that must impact the ICS of an ICS-reliant organisation or directly impact an ICS within an organisation. We define an ICS as Level 0 - Level 3 of the Purdue Model for Control Hierarchy (see Figure 1) [1]. For the purposes of this paper, we will be focusing on ICS incidents that impact Critical Infrastructure Providers (CIPs) within the thirteen CNI sectors identified by the NCSC [11].CIP can consist of both Information Technology (IT) and Operational Technology (OT). We will be excluding attacks that target the IT component of CIPs unless it affects an ICSs operations. An example of exclusions would be ransomware attacks on public services not containing ICS.

This was commenced by examining the attacks provided in [12] and the aforementioned relate work – (See Section 2). The following sub-sections detail forty-three historic ICS attacks.

3.1. PLC Password Change (1988)

The actions of a disgruntled employee from the Pulp & Paper company are identified to be one of the first reported cases of ICS "hacking". The disgruntled employee changed the password on an Allen-Bradley DH+ PLC to "something obscene" [12]. This blocked all maintenance changes/access to the PLC. To nullify the change, the PLC was rebooted to clear the memory and reload the program.

3.2. Ignalina Nuclear Plant (1992)

Oleg Savchuk, a technician at the Ignalina Nuclear Power Plant, was arrested on the charge of premeditated sabotage [13, 12]. He intentionally introduced a virus into the power plants ICSs. Although the viruses impact is unclear, there was a station shut down at the time.

3.3. Chevron Refinery Alarm System (1992)

An ex-employee of Chevron Refinery was able to access the companies emergency alert network, by first obtaining access to computers in New York and San Jose [14]. Once inside the network, the ex-employee reconfigured devices causing them to crash. The organisation was not aware of the disrupted alarm system until an emergency arose, and a noxious substance was released. Thousands of lives were put at risk as the Chevron refinery was unable to notify the local community.

3.4. Salt River Project (1994)

Lane Jarret Davis accessed a computer connected to the Salt River Project through a dial-up modem connected to an internal backup computer. Davis was able to access customer and personnel records, and deleted files holding data used to monitor water and power delivered to consumers [12].

3.5. Omega Engineering (1996)

A worker at Omega Engineering logged on to an internal system, and unintentionally released a 'software time bomb' that removed critical software running the organisations manufacturing operations [12]. Tim Lloyd, a network manager for Omega Engineering and adversary of the sabotage, moved all critical software onto a centralised NetWare file server and took backup tapes off the premises to reformat them. Lloyd was found guilty of computer sabotage and sentenced to 41 months in federal prison, with a $2 million indemnity. The organisation suffered a $12 million loss, and eighty workers lost their jobs.

3.6. Worcester, MA Airport (1997)

An adversary disabled the Next Generation Digital Loop Carrier (NGDLC) system of Worcester Airport [12]. NGDLC systems are used as programmable remote controllers which integrate voice and data communication. The adversary identified the telephone numbers of modems connected to the NGDLC and disabled the phone systems for the airport's control tower, security, fire department, weather service, and couriers for approximately six hours. In addition to this, the attack also disabled the phone services of the nearby town of Rutland.

3.7. Gazprom (1999)

With the help of an insider, adversaries placed a trojan inside the network of Gazprom. This trojan allowed the adversary to take over the SCADA (Supervisory Control And Data Acquisition) system that controlled gas flow. No serious impact was realised, and the services were restored after a short period of time [12, 3].

3.8. Bradwell Nuclear Power Plant (1999)

A security guard set off a high-level alarm at Bradwell Nuclear Power Plant. The guard reportedly hacked into one of the computers to alter and delete sensitive information. This "caused a shutdown of the station's access control system" [15] which automatically locked the facilities electronic doors. To combat this, security tests were reviewed and adjusted, allowing them to identify insider threats at an earlier stage [15].

3.9. Maroochy Water System (2000)

Vitek Boden worked as an engineer for Hunter Watertech and oversaw the installation of SCADA systems for two years before resigning in December 1999. Within the following year's early months, Boden approached the Maroochy Shire government to pursue employment but was quickly rejected. During this time, pumps were reported to be malfunctioning, sewage overflowed and escaped into the surrounding environment (canal and buildings), and multiple pump alarms were disabled. A PDS Compact 500 computer was found in Boden's car, which was the property of Hunter Watertech, and used to communicate with the pumps installed throughout the Maroochy Water System [12, 3].

3.10. Cal-ISO System (2001)

Adversaries identified and exploited "two Solaris servers that were part of a development network at Cal-ISO" [12]. The servers were not firewalled, and configured with default settings, presenting a multitude of vulnerabilities. Security specialists at Cal-ISO were unable to identify what adversaries were doing due to a lack of logging. Rootkits were found on both servers. A source familiar with the attack and Cal-ISO stated that the attack "was very close to being a catastrophic breach" [16].

3.11. Virus on Manufacturing System (2001)

A large manufacturing company within the US implement an up-to-date anti-virus program to their IT enterprise [12], the process control environment was out of scope for this work. An engineer logged into the process control server, unaware that his personal machine was infected with the Nimda virus. The virus spread across the organisations manufacturing system infecting and slowing down the devices within it. The organisations IT staff enabled the facility to continue running; however, the recovery time & effort had a large financial impact.

3.12. Houston Port (2001)

Aaron Caffrey performed a DDoS attack on the Port of Houston [12]. The attack crashed multiple devices that provided critical data to incoming and outgoing ships. The devices recorded data such as; tides, water depths, and weather. This made it extremely risky for shipping companies to navigate the port (the eighth busiest maritime facility in the world) [17]. Although no accidents occurred, it was considered a form of "electronic sabotage" [17].

3.13. Gas Processing Plant (2001)

A gas processing plant run by a US petroleum company had three of their systems hacked simultaneously. This caused outages to homes and businesses within Western Europe and resulted in environmental fines, and contract violations [12]. A 6-month investigation identified that a supplier was hacking the company. Allegedly, the supplier attempted to disguise a mistake they had made on one of the processing plants computers [6].

3.14. PDVSA (2002)

PDVSA, a Venezuelan oil company, suffered multiple attacks against their terminals, refiners, and computer systems. This caused the organisation to reduce production from 3 million barrels of oil a day to approximately 370,000 [12, 6]. PLCs were remotely accessed and erased to impact the site further and reduce its production. The attacks occurred while staff were on strike.

3.15. Flight Planning Computer (2003)

The Blaster Virus [18] was introduced into the flight planning system used by Air Canada Jazz. It increased network traffic and continuously locked/restarted the infected system due to errors within the code. The infected system provided the airline with essential data, including weather conditions, fueling, and predetermined flight paths for approximately 700 flights [12]. Without this critical information, planes were unable to take off, and it was estimated that 200 flights had been impacted [12].

3.16. CSX Train Signalling System (2003)

The Train Signalling system throughout the US's east coast was brought to a halt during peak hours. The Sobig virus was identified as the cause, although no information is available on how it infected the system. Sobig disrupted the telecommunications network which is relied upon for identifying the state of signals and when trains dispatch from stations [12]. This caused all trains to halt unexpectedly due to the lack of critical information.

3.17. Contractor Infects SCADA Network (2004)

A contracting company employee connected an infected laptop into a SCADA system being used on a pilot plant. Pilot plants are small-scale implementations of existing infrastructure used to test/identify processes' behaviour before being applied to large scale environments. The pilot plant stopped operating, and it was discovered that the SCADA network was infected with a large number of viruses. The plant was shut down, and its components reset [12].

3.18. Daimler Chrysler Plants (2005)

Systems at thirteen manufacturing plants were infected with the Zotob worm [3]. This worm spreads through the exploitation of a Windows PnP (Plug and Play) vulnerability. The worm caused systems to slow down, crash, and reboot.

3.19. Tehama-Colusa Canal (2007)

Unauthorised software was installed on the Tehama-Colusa canal SCADA System. It was identified that a former employee intentionally accessed and damaged the system on the same day he was fired. The effects of this attack cost the Tehama-Colusa Canal Authority more that $5,000 in damages [12].

3.20. Lodz Tram System Hacked (2008)

A fourteen-year-old from Poland modified a TV remote control to change track points on the local tram system [19]. The manipulation of the track points caused four trams to de-rail with one of those trams colliding with a passing tram. It was later identified that the teenager had been conducting reconnaissance for months to determine which track point change locations could cause the most damage [20].

3.21. US Power Grid (2009)

An unnamed US official claimed that Spies from Russia and China were attempting to map US CNI with network mapping tools [21]. This was made possible through the US electrical power grid's penetration and was identified via potentially unruly software left behind.

3.22. Hospital HVAC (2009)

A hospital in Texas experienced problems with their Heating, Ventilation, and Air Conditioning (HVAC) system, as no alarms were being activated as expected. The online alias 'GhostExodus' was used to post screenshots of the Human Machine Interfaces (HMI) that gave control to most of the HVAC utilities throughout the hospital [12]. In addition, these screenshots showed that the alarm system was switched to "inactive". It was later identified that a hospital security guard was the user 'GhostExodus', and had been downloading malicious code onto the hospital's HVAC system causing the disruption.

3.23. Night Dragon (2009)

Five (and potentially another seven [22]) global petrochemical organisation have been identified as victims of Night Dragon attacks. These attacks consist of social engineering, spear-phishing, Windows-based exploits, Trojans, Active Directory, and Remote Administration Tools (RATs), used to extract sensitive competitive data, including operational blueprints [22, 3, 21]. These attacks originated from several locations within China that have used "Command and Control servers on purchased hosted services in the United States, and compromised servers in the Netherlands" [22].

3.24. Sality Virus Infects DCS Servers (2009)

Two Open Platform Communications (OPC) Servers used to communicate with PLCs had their services stopped after a software upgrade was enforced [12]. Clients could revert to an older build; however, the OPC servers were unable to reboot. Sality Virus was later

identified as the cause. Sality has the ability to delete files with a certain extension, terminate security-related processes, and communicate with a remote server to download malicious software/files [23]. Operators ran the plant for over 8 hours without any communication to the OPC servers while they were rebuilt [12].

3.25. Natanz - Stuxnet (2010)

Anti-virus experts identified the Stuxnet worm in 2010 [24]. They found that it consisted of four zero-day exploits that enabled the worm to access Siemens Simatic WinCC or PCS 7 software running on Windows systems[4, 12]. Using default passwords that are hardcoded into the software, the worm accesses Control System Databases [12]. It is estimated that 14,000 machines were infected with Stuxnet in Iran alone and that the majority of infected machines are located in the US, Iran, Iraq, and Indonesia [24, 12]. Stuxnet was reported to fluctuate centrifuge speeds within the uranium enrichment facility at Natanz, causing them to fail, resulting in an operational shutdown. It is believed that initial access was gained through a USB stick [24, 25].

3.26. Shionogi (2011)

Shionogi, a pharmaceutical company, lost 88 virtual servers across 15 hosts. The hosts contained the majority of Shionogi's American infrastructure, and their loss stopped the organisations activities for several days, creating an estimated $800,000 deficit [12]. It was later identified that a former IT employee gained access to the computer network using a known account. From here, he utilised malicious software covertly installed to deleted the contents of all 15 hosts.

3.27. Niagra AX (2012)

Tridium state that in 2012 they had more than 300,000 instances of the Niagra AX Framework used worldwide [26]. A backdoor vulnerability for the Niagra AX ICS was posted online, allowing a user to connect to the system through an IP address with no authentication [12]. Using this method, adversaries gained access to the ICS used by an air conditioning company to control the organisations' heating and air conditioning.

3.28. Espionage on Iranian Critical Infrastructure (2012)

Flame is considered once of the most complex malware examples ever developed and was initially discovered on computers belonging to the Iranian National Oil Co. and the Iranian Oil Ministry [4, 27]. It has remained undiscovered in Iran's classified networks (including nuclear enrichment) for several years with the ability to "map networks, activate and microphones, transmit large amounts of state-secret information back to a central source" [28]. Flame is modular-based, consisting of different activation and propagation vectors, complex code injection techniques, encryption algorithms, registry modification, compression of logs and databases, C&C communication, attack dictionaries, attack scripts, and evasion techniques [27]. In addition to this, communication with the C&C enables the adversaries to adjust and import additional modules into the toolkit.

3.29. Turbine Control System (2012)

A contractor used a USB drive infected with an adapted version of the Mariposa virus on a US Electric Utility Turbine Control System [12]. Mariposa is a botnet that connects to a C&C server through anonymous VPN services, and has impacted computers in more than 190 countries [29]. The malware caused over 3 weeks of downtime due to the plant not being able to restart [12].

3.30. Rye Brook Dam (2013)

A small dam near New York was attacked by Iranian hackers using unsophisticated methods [5]. The Bowman Dam was controlled by a SCADA system connected to the internet through a cellular modem. Iranians used this cellular modem to access the SCADA system. The cyber-attack commenced during maintenance, and technicians could not control the SCADA system, only monitor it [5].

3.31. European Public Utility Services Attacked (2014)

Public utility services within Spain, US, France, Italy, and Germany were attacked after malicious actors gained access through phishing, compromised websites, and "trojanised" updates from ICS vendor websites [30]. It was later identified that the ICS focused malware, Havex, was distributed throughout the utility network after being breached [30]. Havex is a Remote Access Trojan (RAT) that has the ability to connect with a C&C (Command and Control) server. The payloads sent across the utility network were used to identify server names, OPC versions, vendor information, running states, and bandwidth [30]. ICS-CERT tested the malware and identified that it could cause multiple OPC platforms to crash [30].

3.32. German Steel Mill (2014)

Spear phishing was used to gain access to a German Steel Mill's enterprise network. It is suspected that the email contained a PDF file that executed malicious code once opened [31]. From here, adversaries pivoted to the ICS network [12, 31]. This access allowed adversaries to alter the code of a blast furnace, preventing its shutdown. This caused damage to the furnace and surrounding systems [31].

3.33. Ukrainian Energy (2015)

Three electricity distribution companies in Ukraine were attacked, causing power outages for more than 80,000 residents [32]. The adversaries disconnected breakers across 30 substations, while simultaneously launching a telephone denial of service attack against customer support centres, preventing customers from reporting outages [32]. It was identified that BlackEnergy3 malware was used to pivot between the business and control system network, and was delivered via spear-phishing emails [32]. In addition, the malware performed KillDisk wipes on operators machine rendering them inoperable [32].

3.34. Ukrainian Energy (2016)

The Crash Override malware was targeted at a single electrical transmission level substation in Ukraine, causing power outages for one hour [33]. Similar to Havex, Crash Override exploited OPC to map the substation's network and identify potential targets. It is also modular, consisting of an initial backdoor, a loader module, and has the ability to add additional payload modules [33]. It is assumed that the malware gained initial access to the network through spear-phishing emails, and adversaries are thought to have hidden within the network for approximately six months [3].

3.35. Wolf Creek (2017)

Wolf Creek Nuclear Operating Corp. has been identified as a target of numerous cyberattacks against utility sectors within the US. Adversaries constructed targeted emails containing fake résumés for available control engineering jobs. These fake résumés contained malicious code that once opened executed automatically. The FBI and Department of Homeland Security produced a report on the attack, confirming that no operational process disruption was caused. It was also identified that the adversaries attempted to map out Wold Creek's network, possibly for future attacks.[34]

3.36. Cadbury Factory Attack (2017)

Production at Cadbury's Claremont facility was halted on the 27th June 2017 at 9:30pm after systems shut down in the factory [35]. The downtime of the factory cause $140 million in net revenue and $7.1 million in expenses to resolve the attack [36]. It was quickly discovered that the NotPetya ransomware was the cause. The spread of NotPetya began in Ukraine, disrupting multiple systems. It impacted at least four hospitals, six power companies, two airports, more than twenty-two banks, and the majority of the federal government [37]. Within a short period of time, NotPetya spread out of Ukraine and effected companies including TNT Express, FedEx, Cadbury, Reckitt Benckiser, and Maersk [37]. The NotPetya ransomware used Mimikatz and EternalBlue for maximum reach, with a purely destructive goal to irreversibly encrypt master boot records [37].

3.37. Triton/Petro Rabigh (2017)

Adversaries were able to access a Safety Instrumented System (SIS) and used the Triton attack framework to reprogram SIS controllers [38]. It was identified that the adversaries had been inside the petrochemicals corporate network since 2014. From there, they pivoted to the operational network and deployed Triton [39]. Triton can manipulate SIS controllers into a failed safe state which can automatically shut down industrial processes [38]. Perhaps what is most worrying, is that Triconex safety controllers are the last line of defence against disasters [39]. Julian Gutmanis was requested at a petrochemical plant in Saudi Arabia and identified that the malicious code on their system could have led to the release of poisonous toxins or caused explosions [39].

3.38. Norsk Hydro (2019)

Norsk Hydro is an aluminium and renewable energy company based in Norway. Norsk Hydro was targeted by a modified version of the LockerGoga ransomware, with 22,000 computers hit in over 170 of their sites [40, 41]. Molten metal lines reverted to manual operations or were halted. This cost the organisation over £45 million to recover.

3.39. Triton/Undisclosed (2019)

As previously mentioned within this paper, Triton has been developed to target SIS controllers within ICSs. Security researchers identified that adversaries are probing ICSs within the US [42]. Adversaries were thought to be lurking in the target network for approximately a

year before gaining access to SIS engineering workstations [42]. Although no service disruptions have been reported, adversaries could have been using their access as a 'playground' to test out custom versions of Triton [38].

3.40. Hackers Target Oil Producers (2020)

Spear-phishing campaigns have targeted the Petroleum and Processing industry [43]. This has been done through carefully crafted emails appearing to bid for equipment and materials. Files attached to these emails contained the Agent Tesla spyware Trojan [43]. This RAT (Remote Access Trojan) contains a keylogger which adversaries can use to obtain usernames and passwords [44]. Most of the attacks were targeted against Malaysia, Iran, and US organisations [43].

3.41. Israeli Water Facilities Attacked (2020)

Israel's National Cyber Directorate alerted the water sector to change passwords on internet-accessible devices, reduce internet exposure, and update the software of ICSs following an attack on wastewater treatment plants [45, 46]. Adversaries targeted Programmable Logic Controllers (PLCs) and were identified due to the resulting suspicious behaviour displayed across these devices. It is unclear if the adversaries were attempting to cause damage or test their reach [46].

3.42. Cyber-Attack on Shahid Rajaei Port (2020)

Hackers carried out a "highly accurate" series of cyber-attacks on the Iranian port. It is assumed as an act of retaliation from Israel in response to the aforementioned attack on the Israeli Water Facilities [47]. The attack was able to infiltrate and damage multiple private systems at the port, causing miles-long traffic jams on highways and at sea for days [47, 48].

3.43. Honda Factories Cyber Attack (2020)

Honda was forced to freeze global production after reports that the Ekans ransomware had infected an internal server [49, 50]. The tool used within the attack was identified as a new variety of ransomware designed to disrupt ICSs. Malwarebytes identified the Remote Desktop Protocol as a possible attack vector, as some of Honda's machines were publicly exposed [51]. These machines are thought to be publicly facing due to the remote working policies put in place at the start of the coronavirus pandemic.

3.44. Summary

This section has provided an overview of forty-three attacks on ICSs between 1988 & 2020. Although the majority of ICSs were not connected to the internet in the 1980s and early 1990s, we found the extrapolated data from these attacks important for the analysis section of this paper. This additional data enables us to identify a more accurate transition over time of the attack vectors, sectors, and impact, which, in turn, provides a more accurate analysis. Due to how long ago these attacks were recorded, this data must be interpreted with caution due to the potential inaccuracy of public information. These attacks were cross-referenced, where possible, with multiple sources (RISI [12], ICS related news sources, white papers, and case studies) to provide as much accuracy as possible. An example of exclusion from this process is the Siberian Pipeline Explosion (1982) [52] as there is uncertainty around the existence of this attack. Six of the eight attacks before the year 2000 highlight insiders as the cause. Although there is a shift away from this attack type, at least in regard to publicly available information, there are still documents being published identifying it as an undefeated problem within the domain of ICS [8, 53]. Therefore, we would argue that there is still valid information available to afford cyber-security practitioners with a greater understanding of the development of attack vectors, threat actors, impact, and targeted sectors & locations.

Regarding the completeness of our attack list, we are confident that we have accumulated the majority of publicly well documented attacks between 1988-2020. This section provides a larger list of ICS attacks than we were able to find from other sources. Although this is the case, we are aware that some attacks have been unnoticed due to our data collection techniques. We discuss a solution to this problem within the Future Work component of Section 6.

The identification and collation of the aforementioned attacks will allow us to identify trends and patterns over the years. The purpose of this is to understand the development of threats against ICSs further and, therefore, afford ICS defenders with a deeper understanding of attack vectors, threat actors, impact, and targeted sectors/locations. The next section of this paper will provide a detailed insight into three key, and well documented, attacks against ICSs. The three key attacks are identified as significant historical events regarding approaches to attacking ICSs. Therefore, an insight into them will allow us to take into consideration their effects on trends. A summary for each of these attacks can be found in Table 1.

Attack	Date	Initial Access	Threat Actor	Sector	Impact
PLC Password Change	1988	Workstation Compromise	Insider	Manufacturing	Denial of Control
Ignalina Nuclear Power Plant	1992	Workstation Compromise	Insider	Civil Nuclear	Loss of Productivity and Revenue
Chevron Refinery Emergency Alarm System	1992	Workstation Compromise	Individual	Chemical	Loss of Productivity and Revenue
Salt River Project	1994	Internet Accessible Device	Individual	Energy and Water	Loss of Productivity and Revenue, Disk Wipe
Omega Engineering	1996	Workstation Compromise	Individual	Manufacturing	Disk Wipe
Worcester, MA Airport	1997	Internet Accessible Device	Individual	Transport	Loss of Productivity, Revenue, Availability, and Safety
Gazprom	1999	Unknown	Organised Group + Employee	Chemical and Energy	Loss of Productivity and Revenue
Bradwell Nuclear Power Plant	1999	Workstation Compromise	Insider	Civil Nuclear	Disk Wipe
Maroochy Water System	2000	Wireless Compromise	Insider	Water	Damage to Property
Cal-ISO System	2001	Unknown	Nation State	Energy	None Disclosed
Virus on Manufacturing System	2001	Spearphishing	Nation State	Manufacturing	Loss of Productivity and Revenue
Houston Port	2001	Internet Accessible Device	Individual	Transport	Loss of Productivity and Revenue
Gas Processing Plant	2001	Trusted Relationship	Supplier	Chemical	Loss of Productivity and Revenue
PDVSA	2002	Internet Accessible Device	Organised Group	Chemical	Loss of Productivity and Revenue, Disk Wipe
Flight Planning Computer	2003	Unknown	Individual	Transport	Loss of Productivity and Revenue
CSX Train Signalling System	2003	Spearphishing	Unknown	Transport	Loss of Productivity and Revenue
Contractor Infects SCADA Network	2004	Replication Through Removable Media	Unknown	Food	Loss of Productivity and Revenue
Daimler Chrysler Plants	2005	External Remote Service	Individual	Manufacturing	Loss of Productivity and Revenue
Tehama-Colusa Canal	2007	Workstation Compromise	Individual	Water	Damage to Property
Lodz Tram System Hacked	2008	External Remote Service	Individual	Transport	Loss of Safety
US Power Grid	2009	Internet Accessible Device	Nation State	Energy	None Disclosed
Hospital HVAC	2009	Workstation Compromise	Insider	Health	Loss of Safety
Night Dragon	2009	Exploit Public-Facing Application	Organised Group	Energy	Theft of Operational Data
Sality Virus Infects DVS Servers	2009	Unknown	Unknown	Chemical	Loss of View
Stuxnet	2010	Replication Through Removable Media	Nation State	Civil Nuclear	Damage to Property, Manipulation of View and Control
Shionogi	2011	Workstation Compromise	Individual	Health	Disk Wipe
Niagra AX	2012	Internet Accessible Device	Unknown	Manufacturing	Manipulation of Control
Espionage on Iranian CI	2012	Replication Through Removable Media	Nation State	Chemical	Theft of Operational Data, Unintentional Disk Wipe
Turbine Control System	2012	Replication Through Removable Media	Organised Group	Energy	Loss of Productivity and Revenue, Theft of Operational Data
Rye Brook Dam	2013	Internet Accessible Device	Organised Group	Water and Energy	None Disclosed
European Public Utility Services Attacked	2014	Spearphishing	Organised Group	Various	Denial of Service, Theft of Operational Data
German Steel Mill	2014	Spearphishing	Unknown	Manufacturing	Damage to Property
Ukrainian Energy	2015	Spearphishing	Organised Group	Energy	Loss of Productivity and Revenue
Ukrainian Energy	2016	Spearphishing	Organised Group	Energy	Disk Wipe, Loss of Productivity and Revenue, Loss of Safety
Wolf Creek	2017	Spearphishing	Organised Group	Civil Nuclear	None Disclosed
Cadbury Factory Attack	2017	External Remote Service	Organised Group	Food	Loss of Productivity and Revenue
Triton/Petro Rabigh	2017	Workstation Compromise	Nation State	Chemical	Denial of Control, Loss of Safety
Norsk Hydro	2019	Spearphishing	Unknown	Manufacturing and Energy	Loss of View
Triton/Undisclosed	2019	Workstation Compromise	Nation State	Undisclosed	Denial of Control, Damage to Property, Loss of Safety
Hackers Target Oil Producers	2020	Spearphishing	Unknown	Chemical	Theft of Operational Data
Israeli Water Facilities Attacked	2020	Internet Accessible Device	Organised Group	Water	None Disclosed
Cyber-Attack on Shahid Rajaie Port	2020	Unknown	Nation State	Transport	Loss of Productivity and Revenue
Honda Factories Cyber Attack	2020	Spearphishing	Unknown	Manufacturing	Denial of Control

Table 1: Summary of Attacks

CVE-2008-4250	Allows the execution of code via a crafted RPC request
CVE-2010-2568	Allows the execution of code via a crafted .LNK or .PIF shortcut files
CVE-2010-2729	Allows the creation of files in a system directory through a crafted RPC print request
CVE-2010-2743	Allows privilege escalation via a crafted application

Table 2: Exploits used in Stuxnet [54, 55]

4. Overview of Three Key ICS Attacks

In the previous section, we introduced over forty publicly disclosed attacks targeting ICS environments. This section will provide a more in-depth overview of three ICS attacks, namely Stuxnet, Triton and the attack on the Ukrainian Energy Systems. We have chosen these attacks because they are well known and extensively covered.

4.1. Stuxnet

Stuxnet is potentially one of the best known ICS attacks and, according to some, the beginning of a new era within cybersecurity [25]. It has been covered extensively in multiple subjects areas as well, such as law and political science. At the time, Stuxnet was one of the most complex cybersecurity attacks ever seen. The attack aimed to disrupt and damage Iran's nuclear program, which it did by targeting Windows machines connected to PLCs. It achieved this by exploiting several vulnerabilities and automatically propagating through the network. This announced the start of the "fire and forget" generation of malware. However, these systems were not connected to the Internet, so the initial attack occurred locally, through physical access, through a USB drive.

Stuxnet was discovered in 2010 by Sergey Ulasen [56]. It exploited several zero-day vulnerabilities (Table 2). From these, we can see Stuxnet did not target ICS vulnerabilities, but rather vulnerabilities within traditional IT systems. After gaining access to the Windows machines, Stuxnet was able to infect PLCs and disrupt their operations. There have been various reports about the impact the attack had on the Iranian nuclear program, which ranged from a setback of 18 months to more than 5 years and even claims it was not very effective at all [57]. Stuxnet was much more sophisticated than other malware of its era because it aimed to damage physical processes. It is widely suspected that the attack was carried out jointly by the United States and Israel [58]; however, it is difficult to confirm this with a high degree of certainty [59].

4.2. Triton

Triton, or TRISIS, is another well-known piece of malware targeting Safety Instrumented Systems (SIS) discovered in 2017 within a Middle Eastern oil and gas facility [60, 61]. The systems targeted by Triton are designed to prevent failures and incidents; any disruption in their operations could result in catastrophic effects and a danger to life. These dangers further show the impact a successful attack can have in the areas around the targeted facilities, especially when facilities such as nuclear power plants are attacked. The attack resulted in the shutdown of the industrial systems and disruption to operations. Whilst it did not result in considerable safety risks, it is considered another milestone within ICS attacks as it interfered with the critical safety systems and exposed the possible outcomes of an attack against these systems. Triton's availability as a blueprint for other, potentially more dangerous attacks is a clear example of the need to learn lessons from attacks.

There are two main modules to Triton, trilog.exe and library.zip, where the first former leverages the library that contains the necessary tools to communicate with the Triconex controllers [38]. Using these two modules, it can reprogram the controllers by providing custom payloads when the system is running in "PROGRAM" mode [62]. Deployment of the malware occurred though the compromise of an SIS engineering workstation. Therefore, there are many possible ways the malware can get onto the system. Some potential attack vectors include phishing, physical access, and/or trusted relationships. Conforming to the general trend of attribution in cyberspace [63], investigators were unable to identify the adversaries.

4.3. Ukrainian Energy Systems

In 2015 there has been a major attack on the Ukrainian Energy systems, relying on BlackEnergy malware as the core of the attack. BlackEnergy has evolved considerably from the first version discovered in 2007 until the third version used during the attack on the Ukraine energy systems [64]. This is a perfect example of how a threat can evolve over the years, and evade

new and more sophisticated security systems. The attack on Ukraine has been seen as a wake-up call for network operators due to its sophistication and impact, as it coupled with different modes of attacks [65]. There was a six-hour power outage during the attack, which shows the impact an attack on ICSs might have over a large geographical area. It is claimed to be the fist cyber incident that is acknowledged to have resulted in a power outage and affected around 225,000 customers [66]. The attackers used several techniques, aside from BlackEnergy, such as spear phishing, credential theft, KillDisk and a VPN to enter the ICS network.

Looking at the features of BlackEnergy, which is one of the most intriguing parts of this attack, (Table 3), we can see an incremental improvement between version one and two, and more significant improvements in version 3 and BE Lite; especially version three, which can reside in memory only, and can both detect a virtual environment and security measures. When malware resides in memory, it becomes increasingly harder to investigate, as shutting down the system removes any trace of it, a live forensic analysis is needed for this. However, this type of analysis risks changing the memory, which might negatively affect the results. Part of the attack on the Ukrainian energy systems was designed to wipe the systems of any traces using a KillDisk trojan, which would impact forensic analysis results. Initial compromise happened through Microsoft Word files sent to employees which contained malicious macros [67]. According to ESET researchers, the adversaries might have leveraged the CVE-2014-4114 vulnerability to spread the malware [68].

Feature	**v1**	**v2**	**Lite**	**v3**
Plugins		X	X	X
Denial of Service	X	X	X	X
C2C Controller	X	X	X	X
Anti Virus Obfuscation	X	X	X	X
Kernel Rootkit			X	X
Bypass Driver Signing				X
Reside in Memory				X
Detect Virtual Environment				X
Detect Countermeasures				X

Table 3: Key improvements between BlackEnergy versions [64]

4.4. Discussion

From these attacks, we can identify some changes over the years. Since the discovery of Stuxnet to the evolution of BlackEnergy over the years, ending with Triton as one of the first attacks on industrial safety systems. Organisations need to adapt and learn from these attacks to keep up with continually evolving adversaries.

As the first highly sophisticated ICS attack, Stuxnet shocked the community and showed what nations could do in terms of attacking these systems. BlackEnergy is a prime example of how adversaries adapt to security measures and that these security systems need to adapt to them. It shows how one piece of Malware can be used within several attacks and how it can still be relevant years after it was discovered. Finally, we gave an overview of Triton, the first attack that actively targeted industrial safety systems. A successful attack on these systems can have considerable impacts. Looking at these three attacks, aside from the security of these systems, we can see a need for changes within legislation and further discussion within political spheres.

Worldwide, we see that governments have put more emphasis on the security of their critical infrastructure. The European Union aims to do this with Directive 2016/1148 of the European Parliament and the Council, known as the NIS Directive. In the USA, President Obama stated [69]: "From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage." Further, in social sciences, cyberspace is sometimes seen as a 'great equaliser' as it requires less investment than traditional military domains [70]. This also enables non-State actors to enter the conflicts that used to be fought between States. Non-State actors have become a real threat with the potential to cause damage and disruption on an equal level as nation-states. The latter already employs these groups to carry out attacks in their stead [71].

This observed trend from governments and organisations to take threats more seriously must continue to keep up with the continuous evolution of the threat actors they face. When Stuxnet was used to target the Iranian nuclear program, ICSs were not connected to the Internet. Nowadays, there is a trend to connect these systems to the Internet and manage them remotely [72]. This opens them up for attacks like BlackEnergy and Triton, which can be launched from the Internet and target anyone in the organisation. The next section of this paper discusses the ICS attacks' changes over the past decades based on these three attacks and the other ones we introduced in the previous section. It also identifies clear trends and what lessons can be learnt.

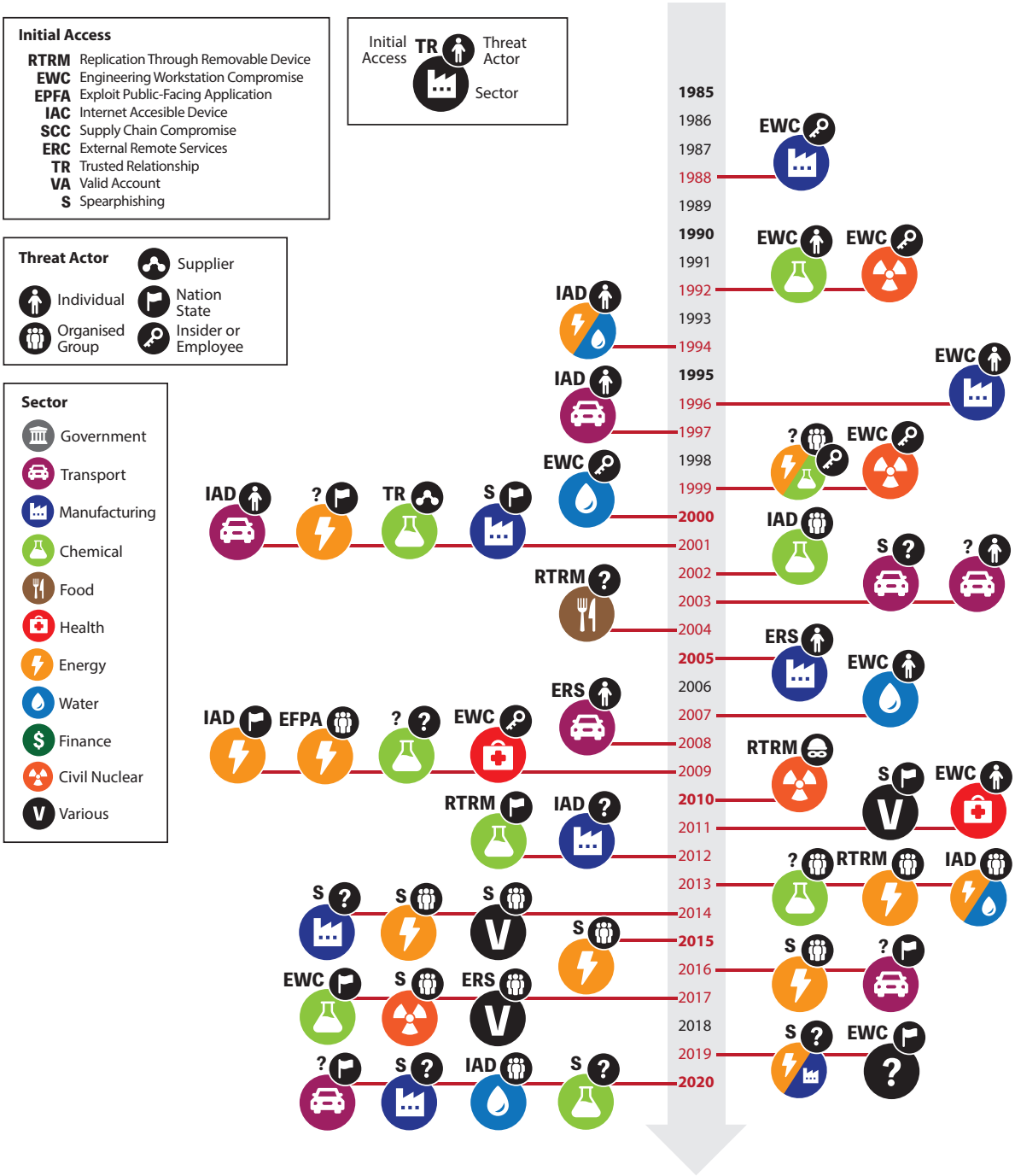

Figure 2: Timeline of Attacks against ICSs

5. Analysis of Attacks on Industrial Control Systems

Section 3 provided us with a summary of 43 attacks targeting ICSs. Using STIX (Structured Threat Information eXpression) Objects [73] and the ATT&CK ICS Framework Tactics [74, 75], we have presented the extracted information within Figure 2. This figure shows all ICS attacks from the first (1988) to the most recent (2021 at the time of publication). The sector the attack was made on (e.g. chemical, food, transport), and the agent (if known) are shown via icons and initials, e.g. in 1996, there was an Engineering Workstation Compromise (EWC) by an individual, in the manufacturing sector. Only years which had attacks are connected using red lines. Colour is used in addition to icons to more easily allow the reader to differentiate between sectors, but has no additional properties. The order of icon clusters within a year does not have meaning. This diagram is designed to give a full overview of ICS attacks to date on a single page, and allow the reader to make comparisons and see patterns, (or lack of therein), ie. Increase in frequency, sectors being targeted and so forth.

STIX serves as a standardised language that aims at providing comprehensive Threat Intelligence data in a structured way [73]. The following STIX Objects have used in the data extraction: Campaign, Course of Action, Identity, Indicator, Infrastructure, Intrusion Set, Location, Malware, Observed Data, Threat Actor, Tool, and Vulnerability. We have also leveraged additional technical information from the MITRE ATT&CK framework for ICSs [75] covering Initial Access and Impact. This framework is described as "a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. The knowledge base can be used to better characterise and describe post-compromise adversary behaviour." [76].

Four key categories were identified during our extraction of attack information: Threat Actors, Initial Access Techniques, Impact, and Targeted Infrastructures & Locations. These categories serve as the basis for our analysis. Each of these categories is supported by using existing frameworks and/or taxonomies; justifying their use in our analysis.

When analysing the data corresponding to Threat Actor information, the following STIX objects were used: Identity, Intrusion Set, and Threat Actor. Additionally, a simplified version of the Threat Actor Taxonomy provided by the Center for Internet Security (CIS) [77] was also chosen to categorise different threat actor groups. Although many taxonomies exist for classifying threat actors such as the one provided by the Cybersecurity and Infrastructure Security Agency (CISA) [78], the CIS taxonomy was selected as it provides a clear distinction between Threat Actors based on their knowledge, skills, abilities, motivations, and resources. The selected taxonomy is as follows:

- Nation State or Nation State Sponsored are groups that may be part of a nation state government branch or are provided resources and funding from a nation state. They often have immense resources and funding for carrying out their mission, and their motivations are often political, military, or to conduct espionage.

- Organised Groups include groups of cybercriminals or cyberterrorists with average to considerable resources for carrying out attacks. Their motivations are ideological, financial, or social.

- External Individuals concern individual actors with no prior access to the systems they wish to exploit. They often have little resources, and their motivations are financial or personal.

- Insiders are trusted individuals within an organisation that already have some access to the systems they intend on exploiting (often in part to being an employee within the organisation).

For our analysis of Initial Access techniques, identified techniques were mapped to the tactics and techniques from both the MITRE ATT&CK Framework [74] and the MITRE ATT&CK for ICS Framework [75]. These frameworks have been selected as some techniques found in the IT-specific framework, such as the use of Valid Accounts, were also applicable within an industrial context. Similarly to this, each attack's impact was also categorised following both these frameworks.

Identified infrastructures were categorised based on the Centre for the Protection of National Infrastructure's (CPNI) taxonomy of National Infrastructure Sectors [11]. Although not a national infrastructure, the manufacturing sector has also been considered within our analysis as this sector often involves the use of ICS networks and is the target of several of our examined attacks.

The following subsections expand on figure 2 to identify associated trends that have emerged throughout the history of ICS attacks, and what lessons can be learnt to prepare for potential future attacks. While an extensive set of resources has been used when extracting data

on the ICS cyberattacks, some attacks do not have sufficient access to resources to confidently identify the information required for a comprehensive analysis. This is most often due to information on specific attacks being classified or unavailable.

5.1. Threat Actor

One of the most critical components in today's threat intelligence is understanding threat actors, their behaviour, motivations, and capabilities. For this section of the analysis, the Identity, Intrusion Set, and Threat Actor STIX Objects were used alongside a slightly modified version of the CIS Threat Actor Taxonomy.

Prior to 2009, most attacks (13 out of 20) are confirmed to have been conducted by individuals, both external and internal. From 2009, a clear transition to larger and more organised groups can be observed. 15 of 23 attacks are either confirmed or allegedly from nation state-sponsored groups or organised groups. When analysing trends from threat actors, it is also important to note the motivation behind these attacks. Many individuals carried out attacks due to personal reasons for either financial gain or as methods of retribution. This can be seen in attacks such as the Bradwell Nuclear Power Plant attack of 1999 (see Section 3.8) or the Houston Port attack of 2001 (see Section 3.12). However, Organised Groups' motivations were mostly political with the aim of conducting espionage or disruption as observed in the Stuxnet attack of 2010 (see Sections 3.25 and 4.1).

Two clear trends concerning threat actors have been identified in the observed attacks over the past 32 years. While an increase in complexity of systems and an increase in security awareness suggests that it is more difficult for single individuals to carry out attacks due to limited skill and resources, there is also a noticeable increase in organised threat capability, often provided with extensive resources through nation-state funding. Although basic security strategies are commonly being implemented, resulting in fewer incidents from simple attack vectors such as poor access control or common vulnerabilities, the introduction of methods for increasing interconnectivity and the complexity of modern systems has increased the possible attack surface for groups with considerable resources to discover and exploit.

To mitigate security risks from individuals, practitioners must ensure the implementation of fundamental security strategies within their organisation. This includes but is not limited to the following: resilient access control such as revoking credential access from terminated employees or ensuring that only authorised members have access to critical systems, and thorough vetting of personnel. A plethora of existing standards and guidelines such as the NIST SP 800 series [79] or the IEC 62443 series [80] can be consulted for practitioners to assess their current security strategies and reevaluate them if necessary. Despite acting as individuals, insiders present additional security risks to organisations due to their already possible access to critical assets and their knowledge of the intricacies of the organisation they are employed by. For this reason, many governmental and standard bodies provide specialised guidance for these threats such as the resources provided by CISA which include methodologies for appropriately identifying and responding to insider threats [81]. Such recommendations include implementing rigorous vetting when hiring new employees, detecting changes in emotional behaviour due to psychological factors, and more. Similarly, academic articles can also provide information on mitigating risks caused by insider threats such as the survey conducted by Homoliak et al. on insider threat taxonomies, analysis, modeling, and countermeasures. Outputs from this survey include mitigation and prevention recommendations such as decoy-based, opportunity-based or anomaly-based detection methods [82].

To this day, organised groups constitute the most considerable risk to critical infrastructures. To combat this growing threat, countries across the globe have adopted the use of national cybersecurity organisations such as the National Cyber Security Centre in the United Kingdom [83] or The Cybersecurity and Infrastructure Security Agency in the United States [84]. These serve as central points of information and guidance for organisations from private and public sectors alike. Practitioners are highly recommended to ensure that they make regular use of the guidance and threat intelligence provided by these to improve their cybersecurity and incident response capabilities. A push has also been observed for organisations to share Threat Intelligence through less centralised methods such as open-source Threat Intelligence feeds like Proofpoint's Emerging Threats Intelligence software [85] or the FBI's InfraGard, which is specifically tailored towards Critical Infrastructures [86].

5.2. Initial Access

The Initial Access techniques from the MITRE ATT&CK and ATT&CK ICS Frameworks [74, 75] were selected when categorising the techniques identified from each attack within section 3.

Abuse and utilisation of a valid account through the compromise of an engineering workstation (ATT&CK ID T1078 and T0818) have been identified as the most

commonly used techniques to gain a foothold into target systems throughout the first half of our investigated time period. This trend suggests that early attacks on ICSs relied heavily on the abuse of an existing level of trust and access. This is most likely because ICS networks were traditionally disconnected from any other networks and used proprietary protocols. Therefore, either physical security needed to be bypassed or an already existing level of access is required (e.g. an employee). An example of bypassing physical security can be observed in the Lodz Tram System attack of 2008 (see Section 3.20).

Unlike the first half of our investigated time period, a wider variety of Initial Access techniques are used in the second half. These techniques include exploitation of External Remote Services (ATT&CK ID T0822), access through Internet Accessible Device (ATT&CK ID T0883), Replication Through Removable Media (ATT&CK ID T0847), and use of Spearphishing Attachment (ATT&CK ID T0865). From 2013, there is a noticeable shift from using technical Initial Access techniques towards the use of social engineering methods such as spear-phishing. Examples of these can be observed in the German Steel Mill attack of 2014 (see Section 3.32), the Norsk Hydro attack of 2019 (see Section 3.38), and the Honda factory attack of 2020 (see Section 3.43).

These identified trends suggest an evolution of the importance allocated towards ICS cybersecurity over the years. Historically, ICSs were mostly protected at the network level through the use of air-gapping and proprietary protocols, making it extremely difficult for external actors to gain access to these systems [87]. However, with the advances in modern technology and the integration of standardised protocols within industrial networks such as TCP/IP, the attack surface has increased. As technical security strategies have improved over the years, most recent attacks have turned to rely on some form of social engineering or human error to gain an initial foothold into targeted systems. This highlights the importance of both providing cybersecurity training to all employees within an organisation and ensuring that organisations correctly implement a robust security culture within work environments. Practitioners are advised to consult their national cybersecurity organisations' guidance regarding minimising attack surface and social engineering awareness. To highlight the importance of social engineering awareness, the NCSC in the UK has currently published a total of 58 guidance resources on phishing exclusively [88]. While training is important, providing this alone does not provide adequate protection against social engineering attacks. Organisations should also ensure that a resilient security culture is implemented within work environments. This includes preventing risky behaviour by establishing stress free environments to minimise mistakes (e.g. accidentally opening an email attachment due to lack of attention or holding the door to a restricted area open to someone without first checking access privileges). Guidance on establishing a robust security culture can be found through various sources such as the open source security culture framework [89].

Although initial access into the target system is commonly carried out through social engineering, follow up tactics such as Lateral Movement, Data Collection, or Command & Control are still often executed using either zero-day exploits or known vulnerabilities. Therefore it is also recommended for practitioners to keep abreast of recent Common Vulnerability and Exposures (CVEs) through sources such as MITRE's CVE Database [55] or the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) [90]. Keeping up-to-date with these vulnerabilities alone is, however, not sufficient enough to confidently prepare for cyber-attacks. Making use of Assurance Techniques such as Document Reviewing or Testing also provides benefits towards an organisation's cybersecurity capabilities and should, therefore, also be considered [91].

5.3. Impact

Similarly to Initial Access Techniques, each attack's impact was also categorised following the MITRE ATT&CK ICS Framework [75].

Unlike the trends identified for initial access techniques, there is no distinct shift in observed impact on systems. This is most likely due to the impact of attacks being closely linked to each attack's motivation rather than an evolution in adversary capabilities. Therefore, identified impacts have been associated with the three following attack motivations: Financial Gain, Espionage/Information Gathering and Disruption/Sabotage.

Only 2 of the 43 attacks were conducted due to financial motivation. The impact from these attacks includes the loss of view or control of systems (ATT&CK ID T0829 and T0813) which often also resulted in a Loss of Productivity and Revenue (ATT&CK ID T0828). This occurs mostly due to the type of malware used in these attacks: ransomware; resulting in the encryption or removal of essential files required for operation. The low frequency of these attack types suggests that financially motivated attacks target primarily IT systems. This is partly due to the ratio of IT to industrial systems (more systems to attack results in a higher possible monetary

gain). At least 15 ransomware attacks have targeted non-industrial organisations such as Universities or law firms in the first half of 2020 alone [92]. Although financially motivated attacks target IT systems more than industrial systems, poor network architecture management can result in the spread of malware from IT systems to industrial systems. This was observed in the Air Canada attack of 2003, where the Blaster Worm, a malware targeting Microsoft Windows initially, spread into the air company's flight planning network (see Section 3.15). This demonstrates the importance of correctly segregating IT networks from ICS networks to prevent IT incidents from affecting ICSs as proposed with the extended Purdue Enterprise Reference Architecture and the use of a Demilitarized Zone to separate IT and industrial networks from each other, for example [1].

8 of the 43 attacks were conducted in order to steal information. In most cases, this resulted in the successful theft of operational data (ATT&CK ID T0882) such as building blueprints, network topologies, confidential documents, or user credentials. Additionally, some of these attacks caused system disruption with disk wipes (ATT&CK ID T1561) or system crashes resulting in a Loss of Productivity and Revenue (ATT&CK ID T0828). This can be observed with the Flame malware deployment, used to conduct espionage in Middle Eastern countries and cause disk wipes (see Section 3.28). On many occasions, these attacks exist as precursors to activities with the intent to cause disruption; often cyber-related, but not always. If system operators manage to detect an attack that has resulted in the theft of confidential or valuable information, they should be prepared for a follow-up attack with a potentially more disruptive goal.

The majority of the attacks described in this paper were conducted to cause sabotage or disruption whether it be by a disgruntled ex-employee targeting a specific organisation as part of a vengeance ploy, or by a nation-state targeting systems that could damage another country's economy or operations. This often resulted in a Denial, Manipulation or Loss of Control and/or View (ATT&CK ID T0813, T0831, T0827, T0815, T0832, and T0829). Consequently, a Loss of Productivity and Revenue (ATT&CK ID T0828) was also observed with Loss of Safety and/or Damage to Property (ATT&CK ID T0880 and T0879) in some cases as seen in the attack on the German Steel Mill in 2014 which caused damage to a furnace due to it being unable to shutdown (see Section 3.32). This highlights the importance of effectively securing ICSs and responding effectively to cyber-incidents if prevention techniques fail. Compared to traditional IT systems, attacks on industrial systems also can cause a loss of safety and therefore, a danger to life. Therefore, practitioners should ensure that their organisation's response plans are thorough and make good use of existing guidance and standards available [93].

5.4. Infrastructure and Location

To conclude our analysis, each attack's targeted infrastructure and location were explored using the associated STIX Objects. This was done to determine if any specific infrastructures were more commonly targeted and if there were any changes in targeted infrastructures over the years. Identified infrastructures were categorised based on the CPNI's taxonomy of National Infrastructure Sectors [11].

Prior to 2009, a variety of targeted infrastructure and locations can be observed. This is partly due to the threat actors involved behind these attacks: as individuals from specific organisations were behind most of the incidents, no infrastructure or location-specific trends were identified. This can be seen, for example, in the Texas Hospital HVAC attack in 2009 (see Section 3.22) where a security guard working at the hospital was responsible for the attack. The corresponding infrastructure was targeted not because it was a hospital but because the attacker was employed there.

From 2010 onward, a clear shift towards targeting the chemical and energy sector can be observed. This is because of the two following reasons: the associated impact caused by targeting these sectors and the motivation behind these attacks. The destructive impact associated with the disruption of the energy sector could cause detrimental consequences to a broader array of infrastructures that require electricity to function. In contrast, an attack on infrastructure, such as oil refinery plants within the chemical sector, could have a severe economic impact on the associated nation. This is especially true for Middle Eastern countries such as Saudi Arabia where the petroleum sector accounts for 42% of the country's GDP [94]. Therefore attacks such as the one targeting Petro Rabigh in 2017 (see section 3.37) not only had the potential to cause a danger to life but could also have had severe consequences on the country's economy. Attacks such as the 2015 attack on the Ukrainian Energy Sector which caused power outages for over 80,000 residents (see Section 3.33) have the potential to affect other infrastructures, taking systems such as assembly lines, life-saving hospital apparatus, or chemical processing machines offline. It can be inferred that these sectors have been targeted because of the impact these attacks can have on other, energy-dependent, sectors.

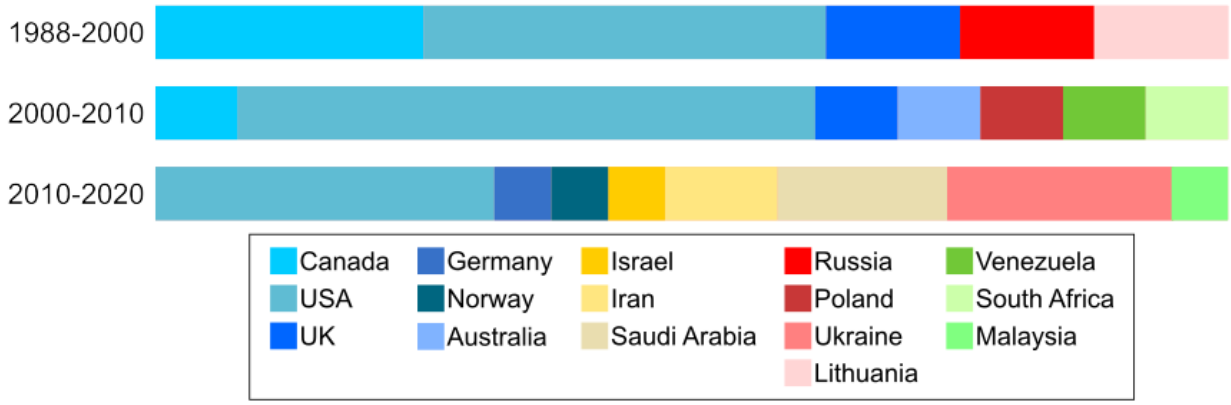

Figure 3: Evolution of Cyber Attack Locations

The location of these attacks could suggest an evolution of both post-Soviet and Middle Eastern conflicts towards a more digital environment. Many western countries are allegedly behind attacks targeting post-Soviet or Middle Eastern countries and vice versa. This cyberwarfare can be observed through the back and forth attacks between Iran and Israel as discussed in Sections 3.41 and 3.42. This evolution is illustrated in Figure 3. The risk-reward aspect of conducting cyberwarfare over the use of a physical medium must also be considered. The little risk and high reward of disrupting a nation-state through a cyber-attack lead to the logical increase in these methods' use over more traditional ones such as physical interventions or economic sanctions.

5.5. Summary

As discussed in the previous sections, multiple trends surrounding past attacks on ICSs were identified. These include Threat Actors behind the attacks, Initial Access techniques to gain a foothold into the target systems, The impact and motivation of each attack, and the attacks' target infrastructure and location. In parallel to these observed trends, baseline recommendations are also detailed; providing stakeholders with a foundation for improving their defensive and response capabilities against the associated threat(s). A summary of these trends and recommendations can be found listed in Table 4.

Prior to 2009, the Threat Actors responsible for the examined attacks were mostly individuals, whether external or internal, targeting infrastructures where these were employed. Initial Access techniques, therefore, involved the use of an already existing level of access. The motivation behind each attack was mostly personal, targeting organisations as retribution, and accordingly, the impact of these attacks was mostly disruptive in nature. During this time period, there was not a large emphasis on ICS Security as these systems mainly were protected through physical means such as segregated networks or the use of propriety technology. Weak cybersecurity policies such as Access Control enabled employees such as security guards to access systems on an industrial network without much difficulty. Although organisations have accorded much greater importance towards cybersecurity in recent years, it is still essential that stakeholders ensure their security policies are implemented thoroughly throughout the organisation, and make good use of existing guidance and guidelines.

From 2009 onward, we observed a shift towards attacks conducted by more organised groups such as cybercriminal or nation state-funded groups. Therefore, the motivation behind these attacks also shifted towards more political reasons such as espionage or sabotage and targeted more critical infrastructure such as the energy sector. Nation-states with a long history of tension have adopted cyberspace as an additional battleground against each other. As security awareness has increased considerably in the past decade, threat actors have also become more reliant on exploiting human vulnerabilities with social engineering when gaining an initial foothold into target systems. Due to this ever-expanding threat landscape that we now face, organisations must work together to understand and prepare against such threats effectively. Keeping in regular contact with national cybersecurity organisations and sharing threat intelligence between organisations have become essential.

There is a clear separation between the identified trends before and after 2009. This shift in trend coincides with the public exposure of the Stuxnet attack of

Threat	Recommendation
Insider Threats	Ensure that fundamental security measures (e.g. access control) are implemented
Organised Groups	Exchange Threat Intelligence regularly with national cybersecurity organisations
Social Engineering	Provide adequate training to all employees and establish a robust security culture
Post-Access Techniques	Regularly monitor vulnerability databases (e.g. NVD) and make use of assurance techniques (e.g. Penetration Testing)
IT-Attacks Pivoting to OT	Segregate critical networks (e.g. Purdue Model)
Aggressive Reconnaissance	Prepare for a potential follow-up attack
High Impact Attacks	Ensure that response plans are compliant to recommended guidance and standards (e.g. ISO/IEC)

Table 4: Summary of Observed Threat Trends and Associated Recommendations Discussed in Section 5

2010. This attack was described as the first known use of malware that was crafted to target ICSs specifically and is also the first known use of a cyberweapon [95]. Because of the detrimental effects that Stuxnet had on Iran's nuclear program, this attack was highly publicised and discussed throughout the security community and governments alike. It highlighted the importance of defending ICSs against malicious actors as it was now known how damaging these types of attacks could be [96]. While stakeholders were made aware of ICS Security's importance, malicious actors were also exposed to the possibilities of executing a cyberattack on ICS [97]. This newfound interest in ICS environments from attackers, coupled with the shift in ICS environment construct (e.g. broader inter-connectivity), converged during the middle of our investigated time period. It can therefore be considered that both of these factors contributed to the apparent change in trends that has been observed from 2009 onward.

6. Conclusion and Future Work

Within this paper, we identified, discussed, and analysed forty-three attacks on ICS. During the collation of attacks against ICS, we were unable to identify a single resource that provides enough information to conduct a comprehensive analysis of attacks on ICSs. Although there have been attempts to amalgamate multiple attacks, these too were insufficiently thorough [3, 4, 5, 7, 8, 6, 10, 9]. To resolve this issue we have aggregated multiple sources of information, which we have used to conduct an analysis on forty-three ICS attacks.

During the analysis, we identified four categories: threat actors, initial access, impact, and infrastructure & location. This was accomplished through the use of the MITRE ATT&CK, MITRE ICS ATT&CK framework [74, 75], STIX [73], the CIS Threat Actor Taxonomy [77], and the Centre for the Protection of National Infrastructure's (CPNI) [11] list of Critical Infrastructure sectors. From this analysis, we generated a list of recommendations based on the observed threat trends:

- **Insider Threats** - Ensure that underlying security measures (e.g. access control) are implemented
- **Organised Groups** - Exchange Threat Intelligence regularly with national cybersecurity organisations
- **Social Engineering** - Provide adequate training to all employees and establish a robust security culture
- **Post-Access Techniques** - Regularly monitor vulnerability databases (e.g. NVD) and make use of assurance techniques (e.g. Penetration Testing)
- **IT-Attacks Pivoting to OT** - Segregate critical networks (e.g. Purdue Model)
- **Aggressive Reconnaissance** - Prepare for a potential follow-up attack
- **High Impact Attacks** - Ensure that response plans are compliant to recommended guidance and standards (e.g. ISO/IEC)

Regarding threat actors, we identified a move from internal to external, and from single perpetrators to organised groups (including state-sponsored). This highlights the need to keep abreast of available Threat Actor Intelligence from central resources. As Critical Infrastructure becomes integrated with IoT, we can identify from our analysis that there is a clear trend in the number of spear-phishing attacks used as an initial access technique. As the complexity of systems increased, phishing became a more appealing point of entry [98, 99]. This indicates the demand for training and awareness for all workers as well as the implementation of a robust security culture within an organisation to reduce this attack vector's risk factor. Unlike other trends, we have not identified any distinct shift in the observed impact on systems. We determined that this is due to the motivation behind each individual attack as some, for example, may be used for reconnaissance purposes and others for disruption and sabotage. This

highlights the importance of correctly implementing response and recovery within the domain of ICS [93]. Preceding 2009, there is a range of attacks against different infrastructures and locations regarding ICSs. Initially, we can observe that most threat actors had ties to the organisation (e.g. employees and suppliers) and acted alone. After 2009 we identified a change towards attacks from organised groups, some of which are potentially funded by nation-states. This shift of threat actor correlates with a clear trend of targeting chemical and energy sectors as attacks on these can affect other interdependant sectors. All the trends identified within the analysis can be observed within Figure 2, and have also been summarised into Table 4, alongside recommended actions. To this day, attacks targeting ICS continue to occur, such as the recent attack on a Florida town water supply in February of 2021 [100] or the DarkSide attack on the Colonial Pipeline in the US [101]; highlighting the importance of effectively preparing for such events by understanding the trends behind them.

For the Future Work of this contribution, the development of an online resource, using the methodology we created for the analysis in Section 5, that is regularly updated as new attacks are identified, or existing attacks are elaborated on further will be undertaken. This will provide a 'one-stop' resource for cybersecurity practitioners, allowing them to evaluate their current security strategies based on the identified trends and lessons learnt from historical attacks.

References

[1] CISCO, Ethernet-to-the-factory 1.2 design and implementation guide, https://bit.ly/2KcRtLj (2008).

[2] E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering & System Safety 152 (2016) 137–150.

[3] R. Derbyshire, B. Green, D. Prince, A. Mauthe, D. Hutchison, An analysis of cyber security attack taxonomies, in: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2018, pp. 153–161.

[4] B. Miller, D. C. Rowe, A survey scada of and critical infrastructure incidents., RIIT 12 (2012) 51–56.

[5] K. E. Hemsley, E. Fisher, et al., History of industrial control system cyber incidents, Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States) (2018).

[6] P. Security, Critical infrastructure, https://bit.ly/2VJtPrJ, last Accessed: 02-07-2020 (2018).

[7] Joe Slowik, Stuxnet to crashoverride to trisis: Evaluating the history and future of integrity-based attacks on industrial environments, https://bit.ly/2VM9XEs, last Accessed: 06-12-2020 (2019).

[8] Andrew Ginter, The top 20 cyberattacks on industrial control systems, https://bit.ly/36LfuSe, last Accessed: 06-12-2020 (2018).

[9] SANS, The industrial control system cyber kill chain, https://bit.ly/3oGhS2T, last Accessed: 06-12-2020 (2020).

[10] Kaspersky, Threat landscape for industrial automation systems, https://bit.ly/3mQDmJw, last Accessed: 06-12-2020 (2020).

[11] CPNI, Critical national infrastructure, https://bit.ly/3irNTsV, last Accessed: 04-07-2020 (2020).

[12] E. Byres, M. Fabro, RISI - the repository of industrial security incidents, https://www.risidata.com/Database, last Accessed: 18-02-2020 (2014).

[13] C. Baylon, R. Brunt, D. Livingstone, Cyber security at civil nuclear facilities: Understanding the risk, https://bit.ly/2yhfGde, last Accessed: 02-07-2020 (2015).

[14] D. E. Denning, Cyberterrorism: The logic bomb versus the truck bomb, Global Dialogue 2 (4) (2000) 29.

[15] K. Maguire, Guard tried to sabotage nuclear reactor, https://bit.ly/3cd4f4S, last Accessed: 02-07-2020 (2001).

[16] D. Morain, Hackers victimize cal-iso, https://lat.ms/3bfitC05, last Accessed: 02-07-2020 (2001).

[17] J. Leyden, Uk teenager accused of 'electronic sabotage' against us port, https://bit.ly/2ymdVes, last Accessed: 02-07-2020 (2003).

[18] P. Security, The most famous virus in history: Blaster, https://bit.ly/2Vh88jJ, last Accessed: 02-07-2020 (2014).

[19] John Leyden, Polish teen derails tram after hacking train network, https://bit.ly/3eKROzK, last Accessed: 11-11-2020 (2008).

[20] Chuck Squatriglia, Polish teen hacks his city's trams, chaos ensues, https://bit.ly/2GPiNxs, last Accessed: 11-11-2020 (2008).

[21] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, Scada security in the light of cyber-warfare, Computers & Security 31 (4) (2012) 418–436.

[22] McAfee, Global energy cyberattacks: Night dragon, https://bit.ly/2RN5JL8, last Accessed: 22-06-2020 (2011).

[23] Microsoft, Microsoft security intelligence: Virus:win32/sality.at, https://bit.ly/3ahhznu, last Accessed: 22-06-2020 (2010).

[24] J. Leyden, Mystery lingers over stealthy stuxnet infection, https://bit.ly/2RQ5mzD, last Accessed: 01-07-2020 (2010).

[25] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security & Privacy 9 (3) (2011) 49–51.

[26] Tridium, About tridium: Tridium's history, https://bit.ly/3arDCYN, last Accessed: 01-07-2020 (2015).

[27] K. Zetter, Meet 'flame,' the massive spy malware infiltrating iranian computers, https://bit.ly/2RS8vz3, last Accessed: 01-07-2020 (2012).

[28] S. Bologna, A. Fasani, M. Martellini, Cyber security and resilience of industrial control systems and critical infrastructures, in: Cyber Security, Springer, 2013, pp. 57–72.

[29] P. Security, Mariposa botnet, https://bit.ly/3bprp8e, last Accessed: 01-07-2020 (2010).

[30] ICS-CERT, Ics advisory (icsa-14-178-01): Ics focused malware, https://bit.ly/356F5CM, last Accessed: 02-07-2020 (2014).

[31] R. M. Lee, M. J. Assante, T. Conway, German steel mill cyber attack, Industrial Control Systems 30 (2014) 62.

[32] K. Zetter, Everything we know about ukraine's power plant hack, https://bit.ly/3eEnDJV, last Accessed: 02-07-2020 (2016).

[33] Dragos, Crashoverride: Analysis of the threat to electric grid operations, https://bit.ly/2KxWN8r, last Accessed: 02-07-2020 (2017).

[34] N. Perlroth, Hackers target operator of kansas nuclear power plant, fbi and homeland security say, https://bit.ly/2yLYht4, last Accessed: 01-07-2020 (2017).

[35] The Guardian, Petya cyber-attack: Cadbury factory hit as ransomware spreads to australian businesses, https://bit.ly/319AQoG, last Accessed: 23-03-2020 (2017).

[36] CSO, Petya attack caused $140m hit on cadbury parent mondelēz's q2 revenues, https://bit.ly/3tSMfpn, last Accessed: 23-03-2020 (2017).

[37] A. Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, 2019.

[38] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, C. Glyer, Attackers deploy new ics attack framework "triton" and cause operational disruption to critical infrastructure, Threat Research Blog 14 (2017).

[39] M. Giles, Triton is the world's most murderous malware, and it's spreading, https://bit.ly/2W0Bmm0, last Accessed: 01-07-2020 (2019).

[40] J. Tidy, How a ransomware attack cost one firm £45m, https://bbc.in/3eOnfZw, last Accessed: 01-07-2020 (2019).

[41] J. Slowik, Spyware stealer locker wiper: Lockergoga revisited, https://bit.ly/3neA1Eb, last Accessed: 01-07-2020 (2019).

[42] T. Seals, Sas 2019: Triton ics malware hits a second victim, https://bit.ly/3eVvrqP, last Accessed: 01-07-2020 (2019).

[43] L. Arsene, Oil & gas spearphishing campaigns drop agent tesla spyware in advance of historic opec+ deal, https://bit.ly/2YyEcSa, last Accessed: 01-07-2020 (2020).

[44] S. Fadilpašić, Agent tesla malware receives module for stealing wi-fi passwords, https://bit.ly/3b1qwl2, last Accessed: 01-07-2020 (2020).

[45] E. Kovacs, Israel says hackers targeted scada systems at water facilities, https://bit.ly/3fiHDlQ, last Accessed: 01-07-2020 (2020).

[46] E. Kovacs, Hackers knew how to target plcs in israel water facility attacks: Sources, https://bit.ly/35vwNnQ, last Accessed: 01-07-2020 (2020).

[47] Joby Warrick, Ellen Nakashima, Official: Israel linkted to a disruptive cyber-attack on iranian port facility, https://wapo.st/3kpjGKS, last Accessed: 11-11-2020 (2020).

[48] Rebecca Addison, Israel linked to cyber-attack on iranian port, https://bit.ly/35lOoQR, last Accessed: 11-11-2020 (2020).

[49] B. Dooley, H. Ueon, Honda hackers may have used tools favored by countries, https://nyti.ms/2BdmRUU, last Accessed: 01-07-2020 (2020).

[50] J. Cook, A. Tovey, Honda's global factories brought to a standstill by cyber attack, https://bit.ly/37vqBgD, last Accessed: 01-07-2020 (2020).

[51] Malwarebytes, Honda and enel impacted by cyber attack suspected to be ransomware, https://bit.ly/2YF9Dsa, last Accessed: 01-07-2020 (2020).

[52] G. Herken, Thomas c. reed, at the abyss: An insider's history of the cold war. new york: Ballantine books, 2004. 368 pp (2007).

[53] NITTF, Insider threat program - maturity framework, https://bit.ly/2NkcqFD, last Accessed: 15-03-2020 (2018).

[54] A. K. Sood, R. Enbody, Chapter 4 - system exploitation, in: A. K. Sood, R. Enbody (Eds.), Targeted Cyber Attacks, Syngress, Boston, 2014, pp. 37 – 75. doi:https://doi.org/10.1016/B978-0-12-800604-7.00004-8.
URL http://www.sciencedirect.com/science/article/pii/B9780128006047000048

[55] MITRE, Cve - common vulnerabilities and exposures (cve).
URL https://cve.mitre.org/

[56] E. Kaspersky, The man who found stuxnet–sergey ulasen in the spotlight, Nota Bene (2011).

[57] I. Barzashka, Are cyber-weapons effective? assessing stuxnet's impact on the iranian enrichment programme, The RUSI Journal 158 (2) (2013) 48–56.

[58] E. Nakashima, J. Warrick, Stuxnet was work of U.S. and Israeli experts, officials say (2012).

[59] J. P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (1) (2011) 23–40.

[60] A. Di Pinto, Y. Dragoni, A. Carcano, Triton: The first ics cyber attack on safety instrument systems, in: Proc. Black Hat USA, 2018, pp. 1–26.

[61] Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware (2017).
URL https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

[62] NCSC, TRITON Malware Targeting Safety Controllers (2017).
URL https://www.ncsc.gov.uk/files/TRITON%20Malware%20Targeting%20Safety%20Controllers.pdf

[63] T. Rid, B. Buchanan, Attributing cyber attacks, Journal of Strategic Studies 38 (1-2) (2015) 4–37.

[64] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, S. Sezer, Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid, in: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 2016, pp. 53–63.

[65] T. Pultarova, Cyber security-ukraine grid hack is wake-up call for network operators [news briefing], Engineering & Technology 11 (1) (2016) 12–13.

[66] M. Assante, T. Conway, et al., Analysis of the cyber attack on the ukraine power grid, SANS Ind. Control Syst. (2016).

[67] T. FoxBrewster, Ukraine claims hackers caused christmas power outage, Forbes Security (2016).

[68] R. Lipovsky, A. Cherepanov, Blackenergy trojan strikes again: Attacks ukrainian electric power industry, Online at http//www. welivesecurity. com/2016/01/04/blackenergy-trojan-strikes-again-attacksukrainian-electric-power-industry (2016).

[69] The White House, Remarks by the President on Securing Our Nation's Cyber Infrastructure (2009).
URL https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

[70] A. Venables, S. A. Shaikh, J. Shuttleworth, On the sharing of cyber security information, in: Critical Infrastructure Protection IX, 2015, pp. 3–16.

[71] T. Hegel, Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers (2018).

[72] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Transactions on Industrial Informatics 14 (11) (2018) 4724–4734.

[73] OASIS, Introduction to stix, https://oasis-open.github.io/cti-documentation/stix/intro, last Accessed: 24-11-2020 (2020).

[74] MITRE, Att&ck matrix for enterprise, https://bit.ly/3ggl94C, last Accessed: 03-07-2020 (2020).

[75] Mitre, Att&ck for industrial control systems, https://bit.ly/2ZtH81k, last Accessed: 02-07-2020 (2020).

[76] MITRE, Att&ck ics - overview, https://collaborate.mitre.org/attackics/index.php/Overview, last Accessed: 07-12-2020.

[77] CIS, Cybersecurity spotlight – cyber threat actors, https://www.cisecurity.org/spotlight/cybersecurity-

spotlight-cyber-threat-actors/, last Accessed: 27-11-2020.
[78] Cybersecurity, I. S. Agency, Cyber threat source descriptions, https://bit.ly/3rVEsWZ (2005).
[79] NIST, Nist special publication 800-series general information, https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information, last Accessed: 02/12/2020.
[80] IEC, Iec 62443, Tech. rep.
[81] Cybersecurity, I. S. Agency, Insider threat - cyber, https://www.cisa.gov/insider-threat-cyber, last Accessed: 24-05-2021 (Not Dated).
[82] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, M. Ochoa, Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures, Tech. rep., Singapore University of Technology and Design (2019).
[83] NCSC, About the ncsc - what we do, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, last Accessed: 25-11-2020.
[84] CISA, Cisa - resources, https://us-cert.cisa.gov/resources, last Accessed: 25-11-2020.
[85] Proofpoint, Emerging threats intelligence, https://www.proofpoint.com/us/products/advanced-threat-protection/et-intelligence, last Accessed: 17-12-2020.
[86] Federal Bureau of Investigation, Welcome to infragard, https://www.infragard.org/, last Accessed: 17-12-2020.
[87] E. Byres, D. Hoffman, The myths and facts behind cyber security risks for industrial control systems, in: In Proc. of VDE Kongress, 2004.
[88] NCSC, Ncsc - search results: Phishing, https://www.ncsc.gov.uk/search?q=phishing&start=0&rows=20&articleType=guidance, last Accessed: 26-11-2020.
[89] K. Roer, The security culture framework, https://securityculturefframework.net/, last Accessed: 25-05-2021 (2021).
[90] NIST, Nvd - home, https://nvd.nist.gov/, last Accessed: 27-11-2020.
[91] W. Knowles, J. Such Aparicio, A. Gouglidis, G. Misra, A. Rashid, Assurance techniques for industrial control systems (ics), in: CPS-SPC '15 Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, ACM, 2015, pp. 101–112.
[92] C. Crane, Recent ransomware attacks: Latest ransomware attack news in 2020, https://www.thesslstore.com/blog/recent-ransomware-attacks-latest-ransomware-attack-news/, last Accessed: 26-11-2020.
[93] A. Staves, H. Balderstone, B. Green, A. Gouglidis, D. Hutchison, A framework to support ics cyber incident response and recovery, in: the 17th International Conference on Information Systems for Crisis Response and Management, ISCRAM 2020 ; Conference date: 24-05-2020 Through 27-05-2020, 2020. URL https://www.drrm.fralinlifesci.vt.edu/iscram2020/index.php
[94] M. Analytics, Saudi arabia - economic indicators, https://www.economy.com/saudi-arabia/indicators, last Accessed = 07-12-2020.
[95] J. P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (1) (2011) 23–40.
[96] J. Slowik, Evolution of ics attacks and prospects for future disruptive events, https://bit.ly/2ABnTu7., last Accessed: 01-07-2020 (2020).
[97] D. E. Denning, Stuxnet: What has changed?, Future Internet 4 (3) (2012) 672–687.
[98] M. Törngren, P. T. Grogan, How to deal with the complexity of future cyber-physical systems?, Designs 2 (4) (2018) 40.
[99] M. Alsharnouby, F. Alaca, S. Chiasson, Why phishing still works: User strategies for combating phishing attacks, International Journal of Human-Computer Studies 82 (2015) 69–82.
[100] F. Robles, N. Perlroth, 'dangerous stuff': Hackers tried to poison water supply of florida town, https://nyti.ms/38PzNye (2021).
[101] O. Milman, Largest us pipeline restarts operations after hack shut it down for nearly a week, https://bit.ly/3yxvIdD (2021).