Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER THREAT BULLETIN
The Cyber Threat to Operational Technology

Canada

ABOUT THIS DOCUMENT

AUDIENCE

This Cyber Threat Bulletin is intended for leaders with an operational technology asset to protect, and the general reader with an interest in the cybersecurity of operational technology.

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

CONTACT

For follow up questions or issues please contact Canadian Centre for Cyber Security at contact@cyber.gc.ca.

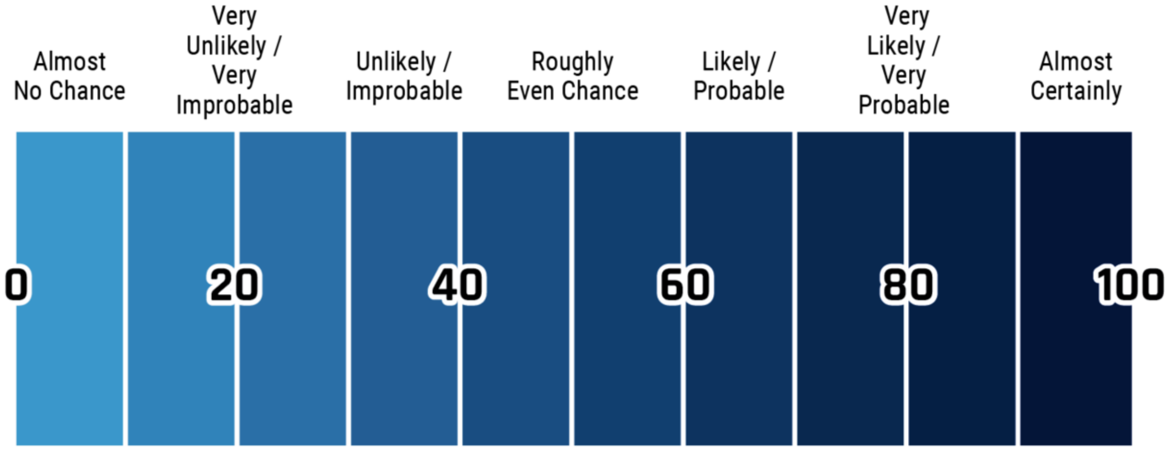
ASSESSMENT BASE AND METHODOLOGY

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Canadian Centre for Cyber Security (the Cyber Centre). Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. CSE's foreign intelligence mandate provides us with valuable insight into adversary behavior in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The assessments and analysis are based on information available as of 1 November 2021.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



KEY JUDGEMENTS

- We assess that the digital transformation of operational technology (OT)—the process of infusing OT with technology derived from the information technology (IT) domain—is almost certainly providing cyber threat actors with new opportunities to access and disrupt OT systems by exploiting the increased computing power and connectivity of OT devices. We judge that this almost certainly includes the OT systems in Canada's critical infrastructure (CI).

- 2020 saw a spike of cyber threat activity against OT systems and OT asset owners around the world. This increase in malicious activity consisted mostly of fraud and ransomware attempts by cybercriminals against OT asset owners' IT networks, as well as a lower level of sabotage attempts by state-sponsored actors. We expect that these trends will very likely continue in the next 12 months.

- We judge that cybercriminals are almost certainly improving their capabilities, and are very likely to attempt to target high-value Canadian organizations with large OT assets, including those in CI, in search of larger ransom payments and valuable data. Cybercriminals are also increasingly likely to directly access, map, and exploit OT for extortion with custom ransomware.

- We assess that the OT in critical infrastructure is almost certainly subject to the cyber threats experienced by any large, valuable organization, and in addition, is almost certainly a strategic target for state-sponsored cyber activity for power projection in times of geopolitical tensions.

- We assess that state cyber actors very likely have an interest in obtaining information on the OT in Canada's critical infrastructure, and pre-positioning cyber tools within it as a contingency for potential future sabotage, in part because of integration with North America-wide systems. We judge that, in the absence of international hostilities, it is very unlikely that state-sponsored cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause significant damage or loss of life.

- Sophisticated cyber threat actors target the OT supply chain and service providers for two purposes: to obtain sensitive information about the OT of their actual target; and, as an indirect route to access the networks of OT targets. We assess that supply chain targeting by medium- to high-sophistication cyber threat actors will almost certainly continue in the next 12 months.

- We assess that software supply chain compromises are very likely an active, increasing threat to OT security, and that activity affecting popular software vendors highlights the potential aggregate impact of a critical vulnerability in widely-used OT products.

CONTENTS

Introduction....4
The Digital Transformation of OT....4
OT Cybersecurity vs. IT Cybersecurity....4
OT Exposure in Canada: A Snapshot....5
The OT of the Future: Cyber-Physical Systems....6
The Role of OT in Critical Infrastructure....6
The Cyber Threat to OT....7
Direct vs Indirect Targeting....7
Direct Threats....7
Threats to OT from Cybercriminals....8
Threats from State-Sponsored Actors....9
Other Actors....11
Indirect Cyber Threats to OT from the Supply Chain....12
Obtaining Sensitive Information About OT....12
Accessing OT Systems Indirectly....12
Conclusion....13
Useful Resources....14
Annex A: Description of Sophistication....15
Annex B: Data Collection and analysis....15
Annex C: OT-related Cyber Security Incidents....15
State-Sponsored Incidents Impacting OT....15
Cybercrime Incidents Impacting OT....17
OT Incidents from Other Actors....19
Endnotes....20

THE CYBER THREAT TO OPERATIONAL TECHNOLOGY

INTRODUCTION

Operational technology (OT) plays an essential role in the management of Canada’s critical infrastructure (CI), and as a result, the cybersecurity of OT is very important to Canada’s national security. OT—the hardware and software used to monitor and make changes in the physical world—originated primarily in industry, and commonly refers to the devices controlling industrial equipment.[1] OT is extensively used to automate industrial processes in diverse sectors like manufacturing, resource extraction, and essential services such as electricity, natural gas, and water. Due to functional gains from the digital transformation of these devices (see Table 1) OT is being used to automate many other sectors like building management, municipal services, transportation, healthcare, and others.

Table 1: OT Terms: What we mean when we say…

Information Technology (IT)	Hardware and software for storing, retrieving, and communicating information; the familiar computers and communications equipment used for business and administrative tasks.
Operational Technology (OT)	Hardware and software integrated into devices used to monitor and cause changes in the physical world; widely used in heavy industry and critical infrastructure for industrial control systems.
Industrial Control Systems (ICS)	Specialized OT that monitors and controls mission-critical industrial processes. An important characteristic of ICS is its ability to sense and change the physical state of industrial equipment.
Embedded systems	A computer system that controls the operation of a physical device or machine, often highly optimized for reliability, efficiency, size, and cost.
Digital Transformation of OT	Integrating OT devices with embedded systems and a network connection to allow automated decision-making, data exchange, and efficient centralized management.
The Industrial Internet of Things (IIoT)	IIoT is a form of industrial OT that allows for a higher degree of autonomy by using smart devices, Internet communications and cloud computing services.
Cyber-Physical Systems (CPS)	Advanced OT, where the physical environment is deeply connected with the information world; systems that measure and control the physical world to achieve a particular goal.

The Digital Transformation of OT

OT came into existence before the Internet, and originally consisted of proprietary systems for industrial process control. These systems were not designed with information security in mind since they were not exposed to external threats. In the past 25 years, however, OT has adopted data processing and communications protocols from information technology (IT) to create safer, smarter, and more efficient operations. The global market for smart OT devices in 2019 was estimated to be about $205.5 billion CAD, growing at about 8% per year.[2] This digital transformation is occurring in almost all organizations with OT assets.[3] Many Canadian organizations are adopting this global trend. We judge that it is highly likely that a significant proportion of Canada’s OT is becoming accessible from the internet and other untrusted networks, and, that this will almost certainly increasingly expose these OT systems to cyber threats.

OT Cybersecurity vs. IT Cybersecurity

OT systems have fundamentally different operating conditions than IT systems. For example, OT devices manage equipment that may be exposed to extreme conditions such as very high temperatures and pressures, dangerous chemicals, radiation, or high voltages. The failure of an OT device could trigger the shutdown of an entire industrial process, which could be very costly. Because of this, OT design has always prioritized personal safety and process reliability (“uptime”) rather than data security, which IT networks do. Industrial assets have long lifespans, and processes tend to be stable over time, so OT devices typically have a much longer service life, often measured in decades, than IT devices. OT systems are usually managed by different groups of people than IT networks, with different backgrounds and priorities. As a result of these characteristics and conditions, OT hardware and software may be upgraded and patched less frequently, communication protocols may lack basic encryption, authentication or integrity protection features. Similarly, OT systems generally do not have security functions like intrusion detection which could delay communications, leading to a degradation of performance and safety of the system.

Historically, OT asset owners countered cyber threats by segregating or "air-gapping" OT systems from IT systems and the Internet to prevent malicious access to OT devices. However, for various reasons, such as extraction of billing and performance data, as well as device configuration and maintenance, OT systems are now nearly always permanently connected to the owner's IT network and, increasingly, directly to the Internet.[4] We assess that the design characteristics of OT systems, and the long-term trend to network previously offline OT systems have almost certainly increased their susceptibility to cyber threat activity.

Table 2. Shodan results for the top 10 OT network ports, by number of Internet-connected devices in Canada, March 2021.*

Rank	OT Network Port	Approximate Number of Devices Online	Primary Use
1	2222	39,500	General industrial automation
2	20000	24,000	Utilities
3	9600	13,500	Manufacturing
4	5007	13,000	Manufacturing
5	4000	13,000	Oil and Gas
6	1883	4,500	IIoT, Manufacturing
7	1911	3,000	Building automation and control
8	47808	3,000	Building automation and control
9	44818	2,500	General industrial automation
10	18245	2,000	General industrial automation

OT Exposure in Canada: A Snapshot

In March 2021, roughly 128,000 network ports associated with OT services responded to scans from Shodan (a search engine for Internet-connected devices) from about 62,800 unique internet protocol (IP) addresses that geolocated to Canada. About 13% of those IP addresses advertised a software version with at least one publicly-reported vulnerability from the Common Vulnerabilities and Exposures (CVE) list—a reliable, but not absolute indicator of vulnerability. We assess that this likely represents a range of Canada-based industrial OT devices that are accessible via the Internet, including equipment typically used by highly-automated CI sectors, and that a small but significant proportion of these devices are likely exploitable through known vulnerabilities (see Table 2 for the top 10). The IP addresses geolocated to every province and territory, with the highest concentrations in Ontario and Quebec. We assess that the picture of the OT attack surface from Shodan is almost certainly an under-representation of actual OT communications on public networks, since Shodan does not discover devices that use the Internet for communications, but are not directly connected. The United Kingdom (UK) and the United States (US) have issued warnings of the presence of state-sponsored cyber threat actors on Internet infrastructure such as routers, switches, and firewalls.[5] We assess that these capabilities could likely be used by cyber threat actors to collect and analyze OT communications, and to identify potentially-vulnerable devices that are not listed in widely-available databases like Shodan.

* The data for this analysis comes from a query of Shodan scans for IP addresses identified as based in Canada for the month of March 2021, filtered for port numbers associated with industrial OT applications and protocols, or were tagged as ICS by Shodan. Network port number is not an absolute indicator of use, because ports can be administratively assigned to other uses. TCP 2222, for example, is often used for SSH (Secure Shell protocol).

The OT of the Future: Cyber-Physical Systems

Cyber-Physical Systems (CPS) are the intended end state of the digital transformation of OT. CPS merge advanced OT components featuring tight integration of computing, networking, and physical process management with the global information infrastructure and large-scale analytics into high-level smart-systems, such as smart factories, smart grids, and smart cities. Critical infrastructure is projected to lead in the deployment of CPS. We assess that the transition of OT to CPS will likely increase the ways that cyber threat actors might value the OT target. This could potentially come from the generation of large quantities of valuable data or follow-on access to connected clients. We assess that the transition to CPS will very likely facilitate malicious OT access, due to the expansion of the attack surface of vulnerable entry points. We assess that these changes will likely alter the cost-benefit analysis of targeting decisions by cyber threat actors. The increased value of these targets, combined with easier access, will likely lead to a large increase in the cyber threat activity against OT, including that in CI and all other sectors transitioning to CPS.

The Role of OT in Critical Infrastructure

We assess that the digital transformation of OT to CPS will likely increasingly expose Canadian CI to cyber threats. Canada's CI (see box "Critical Infrastructure") includes many large industrial assets, such as electricity generation stations and the grid, water treatment facilities, oil and gas pipelines, and factories. OT is central to the management and control of these industrial processes and assets. Canadian CI has been characterized as massive, geographically dispersed, and highly-interconnected.[6] To increase the reliability and economy of critical services, the owners and providers have embraced digital transformation of the OT assets in critical infrastructure.

Cyber sabotage of OT systems in Canadian CI poses a costly threat to owner-operators of large OT assets, and could conceivably jeopardize national security, public and environmental safety, and the economy. In early May 2021, for example, Colonial Pipeline, operator of one of the largest refined products pipelines in the US, suffered an incident attributed to DarkSide, a Russia-based ransomware group. Although the activity was reported to be restricted to the IT systems, the company chose to shut down its operations, which resulted in record price increases, panic-buying and gasoline shortages.[7] A ransomware incident in late May 2021 forced the meat processing company, JBS, to halt production in multiple facilities in three countries, including a meat processing plant in Brooks, Alberta, threatening food security at a time of high demand.[8]

Critical Infrastructure: the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. [9]

THE CYBER THREAT TO OT

Direct vs Indirect Targeting

Cyber threat actors have a choice of several routes through which to direct cyber threat activity against OT. Cyber threat activity, by definition, is digital information intended to harm the security of an information system.[10] There are two common methods of moving digital information between domains—online and offline.[11] Online threats move through the network, and offline threats are stored on digital media, such as a USB key, and moved manually.

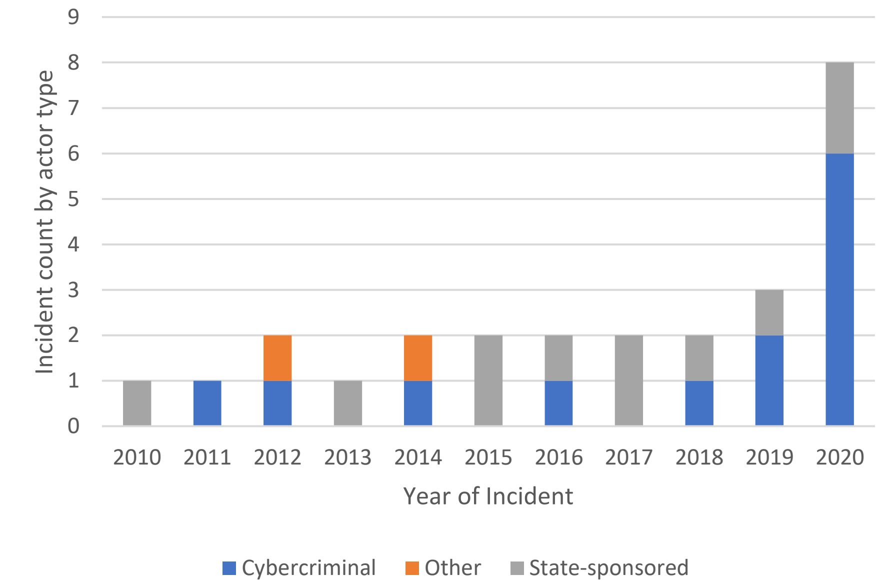
We assess that a threat actor of medium to high sophistication (see Annex A for details of sophistication) will almost certainly consider different targeting options for both online and offline threat activity. This includes targeting an organization directly, by exploiting Internet-connected devices in the organization's OT system, or moving laterally through OT network connections to an organization's IT network. Another option is indirect targeting of an OT system, through targeting second and third parties in the OT supply chain of products and services. We judge that the complexity of supply chain targeting very likely limits medium- to low-sophistication actors to direct targeting.

Direct Threats

The cyber threat to OT from direct targeting derives from two main sources: financially-motivated, medium-sophistication cybercrime groups, and politically-motivated, high-sophistication state-sponsored cyber threat actors. Other potential actors, such as terrorists, hacktivists, and thrill seekers tend to be low-sophistication and present a much lower threat.[12]

From the beginning of 2010 to the end of 2020, the Cyber Centre noted 26 significant publicly-reported cyber incidents from around the world where OT was targeted or affected (Figure 1).[†] We assess that these incidents are likely representative of significant OT cyber incidents, but very likely do not include numerous low-impact incidents that many organizations are exposed to, but do not report.

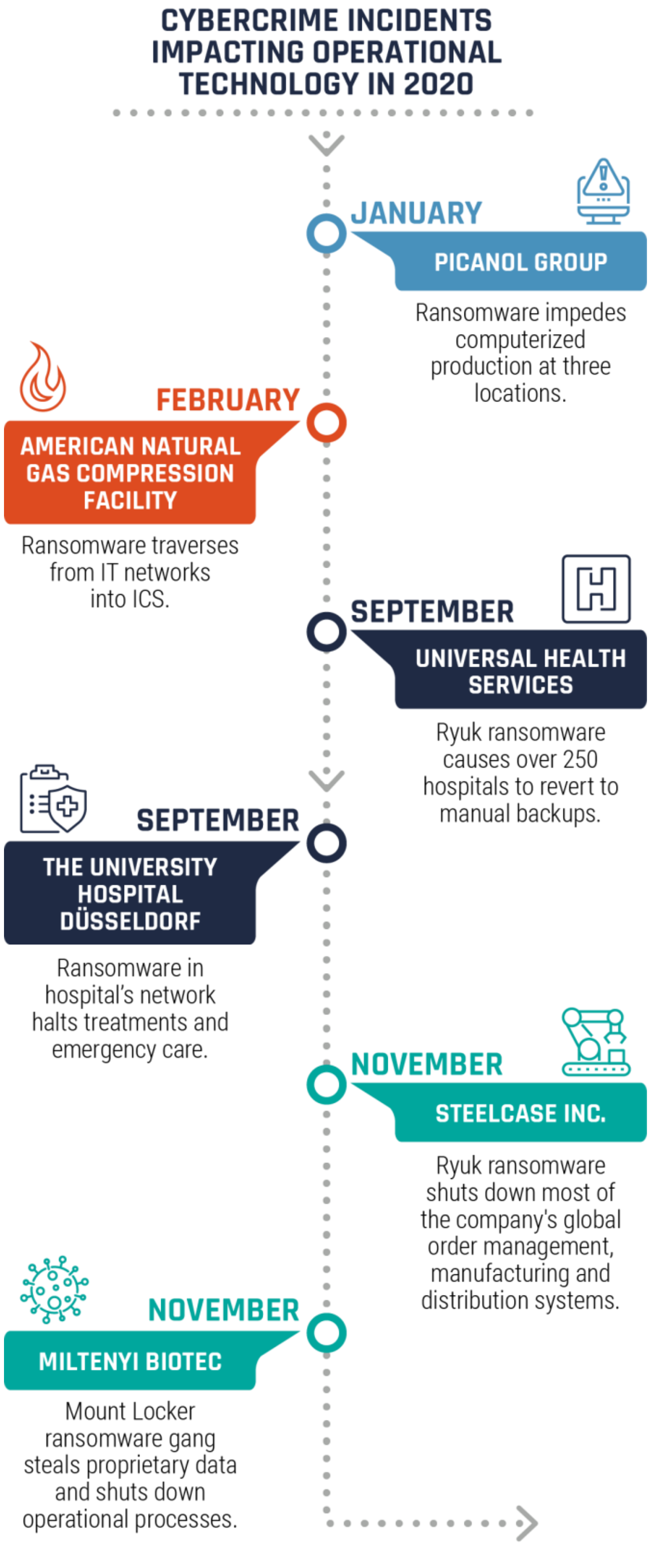
Figure 1. Publicly-reported cyber incidents targeting OT, by actor type.



From 2010 to 2019, there were on average about 2 significant incidents per year, but in 2020, that number increased to 8. We assess that the 2020 spike in cyber activity that affected OT was almost certainly due to an increase in criminal actor activity against large industry, where the OT effect was a by-product of targeting IT networks, as well as OT targeting by states.

While we have observed an increase in activity, we assess that overall sophistication of cyber activity against OT has very likely not changed over time. We judge that the cyber threat activity impacting OT targets has to date consisted of a mix of fraud and ransomware attempts by cybercriminals, as well as espionage and pre-positioning of cyber tools by state-sponsored actors. Hacktivists, thrill seekers, and disgruntled individuals appear to have only caused small-scale disruptions in OT performance.

[†] See Annex B for data collection, coding, and analysis, and Annex C for a list of included incidents.



CYBERCRIME INCIDENTS IMPACTING OPERATIONAL TECHNOLOGY IN 2020

JANUARY — PICANOL GROUP: Ransomware impedes computerized production at three locations.

FEBRUARY — AMERICAN NATURAL GAS COMPRESSION FACILITY: Ransomware traverses from IT networks into ICS.

SEPTEMBER — UNIVERSAL HEALTH SERVICES: Ryuk ransomware causes over 250 hospitals to revert to manual backups.

SEPTEMBER — THE UNIVERSITY HOSPITAL DÜSSELDORF: Ransomware in hospital's network halts treatments and emergency care.

NOVEMBER — STEELCASE INC.: Ryuk ransomware shuts down most of the company's global order management, manufacturing and distribution systems.

NOVEMBER — MILTENYI BIOTEC: Mount Locker ransomware gang steals proprietary data and shuts down operational processes.

Threats to OT from Cybercriminals

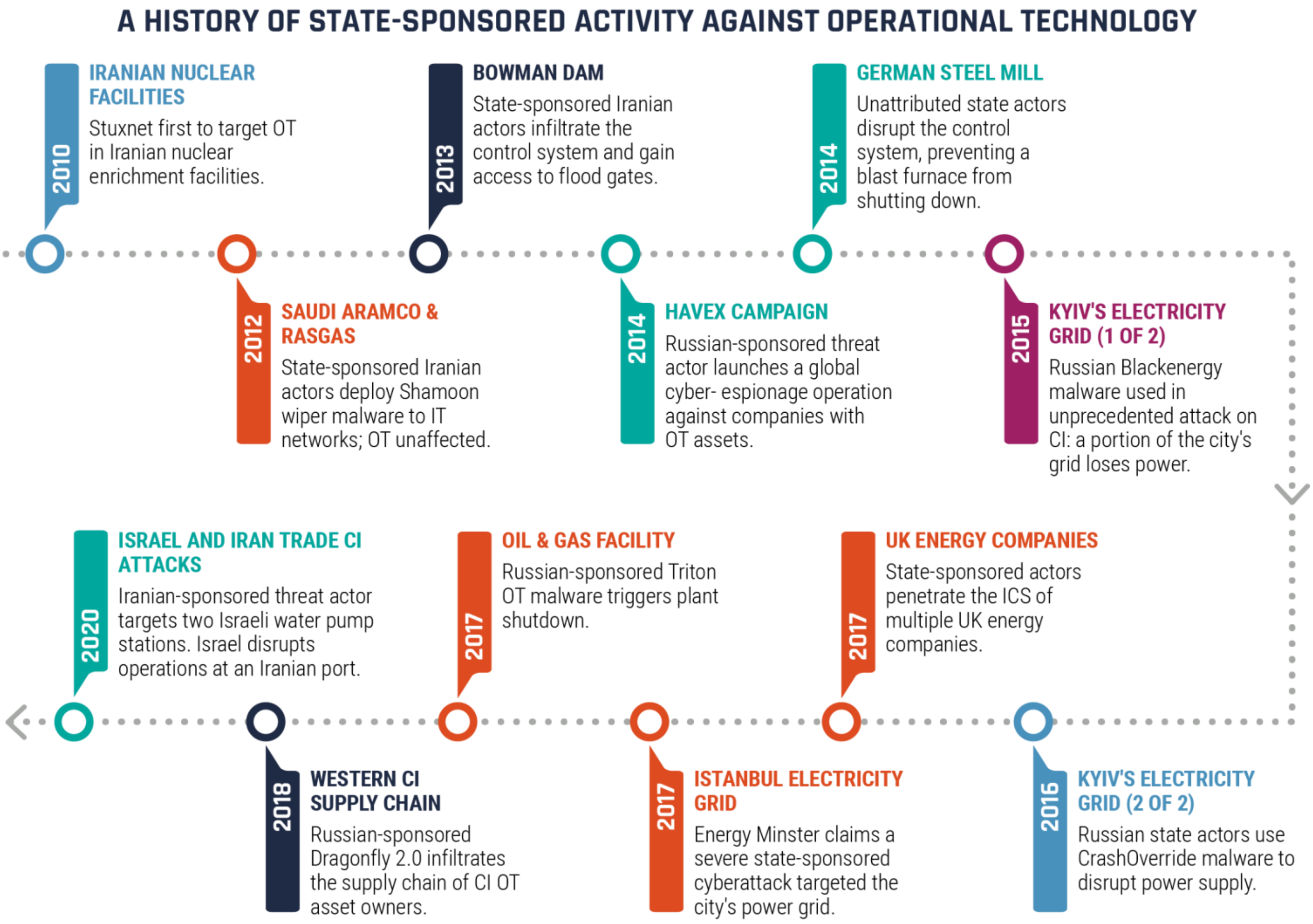
We assess that cybercrime groups will almost certainly continue to target large organizations with OT assets, including organizations in Canada, in medium-sophistication attacks to try to extract ransom, steal intellectual property and proprietary business information, and obtain personal data about customers. In 2020, we assessed that cybercriminals will almost certainly continue to scale up their ransomware operations and attempt to coerce larger payments from victims by threatening to leak or sell their data online.[13] We assess that cybercriminals are almost certainly increasingly targeting heavy industry and the essential services in CI in order to increase their chances of obtaining a large ransom.

Even if the cyber activity is contained in the IT network of an OT asset owner, there is still a possibility of an OT shutdown.[14] In 2020, ransomware attacks that affected OT systems spiked (Figure 1); the incidents were severe enough to force at least six OT asset owners to shut down some or all of their industrial OT operations for safety or business reasons. The impact of a ransomware attack on an OT asset owner varies according to the specific circumstances of the industrial process and the reaction of the site staff. For example, in March 2019, a Norwegian aluminum company was impacted by a ransomware event that disrupted logistical and production data, and the company decided to shut down those OT systems with limited manual mode operations, in some cases relying on paper copies of orders.[15] During Fall 2020, a wave of ransomware hit the healthcare sector,[16] including a September incident where Ryuk ransomware locked the computers in more than 250 US hospitals, forcing staff to revert to manual processes and delaying medical procedures.[17]

We have previously assessed that ransomware operators have almost certainly improved their ability to impact large corporate IT networks to the point that they can detect connected OT systems.[18] In January 2019, a ransomware variant called EKANS or SNAKE emerged, with instructions to terminate OT processes that would normally only run on OT workstations.[19] Ransomware can also migrate to OT through network misconfiguration (see “Emerging OT Vulnerability” text box). In February 2020, ransomware impacted a US natural gas compression facility, traversing Internet-facing IT networks into the OT system responsible for monitoring pipeline operations, prompting a shutdown.[20] We assess that cybercriminals are aware of OT systems, and are almost certainly improving their capabilities to eventually attempt to access, map, and exploit the OT of their targets for extortion with customized ransomware.

Emerging OT Vulnerability: Identity and Access Management (IAM) Spanning IT and OT

IAM synchronization between IT and OT networks (for ease of administration) is an emerging OT vulnerability. Cyber actors are learning to exploit IAM servers to facilitate lateral movement in a network. Synchronizing or mirroring the IAM service into an otherwise protected OT network gives these actors access to vulnerable OT assets. An incident using this method was reportedly the cause of a US pipeline shutdown from ransomware in 2019.[21]



A HISTORY OF STATE-SPONSORED ACTIVITY AGAINST OPERATIONAL TECHNOLOGY

2010 **IRANIAN NUCLEAR FACILITIES**
Stuxnet first to target OT in Iranian nuclear enrichment facilities.

2012 **SAUDI ARAMCO & RASGAS**
State-sponsored Iranian actors deploy Shamoon wiper malware to IT networks; OT unaffected.

2013 **BOWMAN DAM**
State-sponsored Iranian actors infiltrate the control system and gain access to flood gates.

2014 **HAVEX CAMPAIGN**
Russian-sponsored threat actor launches a global cyber- espionage operation against companies with OT assets.

2014 **GERMAN STEEL MILL**
Unattributed state actors disrupt the control system, preventing a blast furnace from shutting down.

2015 **KYIV'S ELECTRICITY GRID (1 OF 2)**
Russian Blackenergy malware used in unprecedented attack on CI: a portion of the city's grid loses power.

2016 **KYIV'S ELECTRICITY GRID (2 OF 2)**
Russian state actors use CrashOverride malware to disrupt power supply.

2017 **UK ENERGY COMPANIES**
State-sponsored actors penetrate the ICS of multiple UK energy companies.

2017 **ISTANBUL ELECTRICITY GRID**
Energy Minster claims a severe state-sponsored cyberattack targeted the city's power grid.

2017 **OIL & GAS FACILITY**
Russian-sponsored Triton OT malware triggers plant shutdown.

2018 **WESTERN CI SUPPLY CHAIN**
Russian-sponsored Dragonfly 2.0 infiltrates the supply chain of CI OT asset owners.

2020 **ISRAEL AND IRAN TRADE CI ATTACKS**
Iranian-sponsored threat actor targets two Israeli water pump stations. Israel disrupts operations at an Iranian port.

Threats from State-Sponsored Actors

We assess that OT is almost certainly targeted by states for a variety of possible reasons: espionage, theft of commercial intellectual property (IP), messaging of intent, and prepositioning for sabotage. The Cyber Centre is aware of low frequency state-sponsored cyber threat activity targeting Canadian OT-related organizations in critical infrastructure since at least 2012.

We assess that large OT asset owner-operators, especially the utilities in critical infrastructure, are not likely targets for the theft of commercial IP, because the commercially-valuable IP primarily resides in the supply chain. We judge that the purpose of cyber activity against CI OT asset owners was likely to collect information and pre-position cyber tools as a contingency for possible follow-on activities, or as a form of influence, from a demonstration of state cyber power. These early stages of a potential future cyber attack tend to resemble industrial espionage.[22] We assess that it is very likely that state actors are using the information gathered from their espionage activities to develop additional cyber capabilities that would allow them to sabotage OT used in Canada's critical infrastructure sectors.

In the past decade, state-sponsored cyber activity against OT, especially the OT in critical infrastructure, has become a regular feature of global cyber threat activity. In 2013, one of the first reported events was an infiltration of the US Bowman Avenue Dam control systems,attributed to Iran.[23] Two years later, in 2015, an undisclosed state-sponsored actor launched a sophisticated social engineering campaign against an unnamed German steel mill. The operation disrupted the facility's controls systems, preventing a blast furnace from shutting down properly, and caused physical destruction.[24]

The first state-sponsored cyber activity to sabotage critical services occurred in 2015 and 2016 against the electricity grid in Ukraine. In late 2015, Russian cyber actors were able to de-energize seven substations from three Ukrainian regional distribution companies for three hours, causing a power outage that affected 225,000 customers. A year later, a cyber incident at Ukraine's national power company, Ukrenergo, caused a one-hour outage in northern Kyiv.[25] These incidents, conducted in the context of the Russia-Ukraine conflict, were a turning point in the history of cyber activity against the electricity sector, demonstrating the impact of a cyber attack against critical infrastructure, and its use during international hostilities.

Escalating tensions between Iran and Israel led to state-sponsored operations against each other's critical infrastructure in 2020. Iranian-sponsored actors likely launched unsuccessful cyber campaigns at Israel's water infrastructure, targeting command and control and other OT systems of two Israeli water facilities. Had these activities succeeded, the operation would have triggered pump shutdowns and left thousands without water.[26] In response, Israel allegedly compromised a prominent Iranian port terminal, disrupting operations and knocking computers offline for several days.[27]

We assess that the OT in critical infrastructure is almost certainly a strategic target for state-sponsored cyber activity, especially for power projection in times of geopolitical tensions. We judge that it is very unlikely that state-sponsored cyber threat actors will intentionally seek to sabotage Canadian critical infrastructure and cause destruction or loss of life in the absence of international hostilities. For economic and reliability reasons, Canada's CI is integrated with that of the US, and we assess that this also likely increases the chance that a service disruption from a cyber attack against the US would be jointly felt by both Canadians and Americans. US assessments characterize the cyber threat to their critical infrastructure from state-sponsored actors as complex and aggressive[28] and have declared that the threats to their critical infrastructure OT by foreign adversaries and sophisticated cyber criminals constitute a national emergency.[29]

State-Sponsored Cyber Capability Development

In 2017, Russian cyber threat actors tested a capability called Triton (a.k.a. Trisis) to modify the performance of a Safety Instrumented System (SIS) at a Middle Eastern oil and gas facility. An SIS is a specialized OT device designed to independently detect out-of-range conditions in an industrial process and if needed, initiate a safe shutdown of the equipment. The actors gained remote access for the facility and reprogrammed the SIS controllers, inadvertently causing them to enter a failed state, resulting in an automatic shutdown of the industrial process and subsequent investigation.[30] Malicious modification of an SIS by itself can trigger a disruptive shutdown, but in combination with tampering with other OT, could have destructive consequences.[31] Triton was designed to prevent safety systems from functioning correctly, and although it was specific to the software and equipment versions at the facility,[32] we assess that these actors would likely be able to modify their capability to target similar systems, and that actors of similar sophistication would likely be able to use these methods to develop a similar capability.

Other Actors

We assess that cyber threat actors who presently lack access to sophisticated cyber capabilities, such as terrorists, hacktivists, and thrill seekers are more likely to engage in disruptive, nuisance-level OT activity, such as the 2014 Daktronics Vanguard roadside signs incident, where individuals gained unauthorized access to digital highway signs and posted false warnings.[33] Pre-built cyber tools and training in their use are becoming readily available via the Internet (see box “Advanced Cyber Tools”), and we judge that there is an even chance that low sophistication actors with the intent to disrupt OT could adopt these tools to mount a successful sabotage attack.

Advanced Cyber Tools and Skills are Becoming Accessible to More Threat Actors

We assess that the wide availability of free, stolen, commercial and criminal cyber capabilities and services is likely lowering the threshold of sophistication necessary to target and sabotage OT. In the National Cyber Threat Assessment 2020,[34] we assessed that the development of commercial markets for cyber tools and talent has reduced the time it takes for states to build cyber capabilities and increased the number of states with cyber programs. Some of these vendors are developing OT-specific capabilities for sale to clients. As more states have access to commercial cyber tools, states that are interested in sabotaging OT, but previously lacked the capability, can now more readily undertake this type of cyber activity. The proliferation of commercial tools to state cyber programs also makes it more difficult to identify, attribute, and defend against this cyber threat activity.

There are OT-specific exploit modules in free cyber tools as well, such as the open source Metasploit framework developed and released by researchers and security professionals for testing OT network defences. These tools are widely available to actors of all sophistication levels and include documentation and tutorials in their use.[35] The Cyber Centre is aware of high-impact crimeware such as Trickbot, Qakbot, Dridex, etc., using the leaked commercial cyber tool Cobalt Strike to target large organizations and critical infrastructure in Canada. Both Metasploit and Cobalt Strike are in wide use by states and criminal groups to facilitate cyber espionage and ransomware activity.[36] In addition, a large illegal market for cyber tools and services is greatly reducing the start-up time for cybercriminals and enabling them to conduct more complex and sophisticated campaigns. Many online marketplaces allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrimes, including espionage, distributed denial of service (DDoS) attacks, and ransomware attacks, any of which could be used by actors intending to sabotage OT systems.

Indirect Cyber Threats to OT from the Supply Chain

We assess that medium- to high-sophistication cyber threat actors are increasingly likely to consider targeting OT indirectly, by first targeting the OT supply chain. Cyber threat actors target the OT supply chain for two general purposes: to obtain commercially-valuable intellectual property and information about the OT in use; and, as an indirect route to access an OT network. Large industrial asset operators, including those operating CI, depend on a diverse supply chain of products and services from laboratories, manufacturers, vendors, integrators, and contractors, as well as Internet, cloud, and managed service providers for daily operation, maintenance, modernization, and development of new capacity. OT asset owners' dependency on the supply chain is a critical vulnerability that gives cyber actors inside information on, and opportunities for access to otherwise protected OT systems. We assess that medium- and high-sophistication actors will almost certainly continue to target the OT supply chain for these purposes for the next 12 months and beyond.

Obtaining Sensitive Information About OT

We assess that high-sophistication cyber threat actors almost certainly target the OT supply chain to obtain sensitive information about clients' OT assets that they can use to develop cyber sabotage capabilities. For example, in 2014, and again in 2017, Russia-associated cyber threat actors undertook an espionage campaign against a variety of supply chain targets that were later linked to exploitation of energy sector targets.[37] In 2019, reports linked Iran to cyberespionage activity against manufacturers, suppliers, and operators of ICS equipment.[38]

Accessing OT Systems Indirectly

A supply chain compromise occurs when products are deliberately exploited and altered prior to use by a final consumer.[39] While a supply chain compromise could occur in hardware or software, threat actors have often focused on malicious additions or injections to legitimate software in distribution or update channels (see box on dependency confusion/substitution attacks). Frequently, threat actors tamper with the end product of a given vendor so that it carries a valid digital signature, and unwitting end-users obtain the signed product through trusted download or update sites.[40] In 2014, Russian state-sponsored cyber actors compromised the networks of three OT vendors and replaced legitimate software updates with corrupted packages that included Havex malware. Users of the OT products downloaded what they believed were updates, and unknowingly installed Havex in their OT systems, giving the cyber threat actors access to various organizations related to the European energy sector.[41]

Emerging Supply Chain Cyber Threat: Substitution Attacks on Public Source Code.

Most software is an assembly of components from both private and public sources.[42] Public sources provide developers with a wide range of high-quality, free code, but many large public code sharing systems allow authors to share their software "packages" without proof of identity. The availability of quality, free software makes development more efficient, but dependencies on public sources are a potential source of malware.

One method of exploiting the development process is called the "substitution attack" (or "dependency confusion") where public sources are manipulated to fetch similarly named but malicious versions of packages.[43] An ethical hacker recently fooled e-commerce company Shopify into installing a benign package called "shopify-cloud" into their software, and after notifying the company of the breach, received a bug bounty.[44] Substitution attacks could allow a malicious cyber actor to put malware into numerous OT devices, covertly, without access to either the manufacturer or the target OT system.

In December 2020, FireEye discovered a global intrusion campaign, almost certainly the work of the Russian Intelligence Services (SVR),[45] who created malicious updates of the widely-used SolarWinds Orion network monitoring and management software by exploiting access to the company's build process.[46] The updates were deployed to more than 16,000 SolarWinds clients,[47] and the actors were able to compromise a smaller subset of target networks with additional malware for cyber espionage, including, potentially, critical infrastructure organizations and other private sector OT asset owners,[48] as well as members of the OT supply chain.[49] We assess that software supply chain compromises are very likely an active, increasing threat to OT security, and that activity affecting large-scale software vendors highlights the potential aggregate impact of a critical vulnerability in widely-used OT products. We judge that supply chain compromises are very likely to be in software rather than hardware, but a malicious hardware alteration is not out of the range of abilities of the most sophisticated state-sponsored cyber threat actors (see box US supply chain security order).

US Supply Chain Security Order

Executive Order (EO) 13920 of 1 May 2020 authorizes the US government to work with the electricity sector to secure the US bulk power system (BPS) supply chain by eliminating high-risk foreign components. This EO prohibits the acquisition, transfer, or installation of BPS equipment with "foreign interests." This EO also requires that such equipment in use by US asset owners be identified, isolated, and replaced.[50]

In addition to targeting the supply chain, it is very likely that foreign state-sponsored actors and cybercriminals are attempting to leverage service providers' privileged access to their clients' systems as an indirect route into their true targets, including OT systems. For example, since at least 2019, ransomware operators have compromised MSPs and used remote management software to automatically install ransomware on multiple client networks at once. In August 2019, the cybercriminals responsible for REvil ransomware compromised a US MSP to infect 22 US municipalities and demanded cryptocurrency valued at $3 million CAD at the time. On 4 April 2017, the Cyber Centre warned of ongoing malicious cyber activity targeting MSPs internationally,[51] and in 2018, Canada and its Allies attributed the activity to a Chinese state-sponsored actor.[52] We assess that as OT systems evolve to CPS, OT systems will become increasingly integrated into service provider systems, and so subject to provider security measures, which may not consider OT-specific threats in their assessments.

CONCLUSION

The cyber threat landscape experienced by the OT asset operators in Canada is evolving, and cyber threat actors continue to adapt their activities to try to stay ahead of defenders. In this assessment, we show that cyber threats to OT are also threats to Canada's essential services and critical infrastructure. We identify trends within the OT threat landscape, including the growing threat from cybercriminals, the threat from state-sponsored actors, as well as the introduction of new threat vectors stemming from the adoption of new technology and Internet-connected devices.

As noted in the National Cyber Threat Assessment 2020, many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats continue to succeed today because they exploit deeply-rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada against cyber threats and related influence operations requires addressing both the technical and social elements of cyber threat activity. Cyber security investments will allow Canadians to benefit from new technologies while ensuring that we do not unduly risk our safety, privacy, economic prosperity, and national security.

The Cyber Centre is dedicated to advancing cyber security and increasing the confidence of Canadians in the systems they rely on daily, offering support to CI and other systems of importance to Canada. We approach security through collaboration, combining expertise from government, industry, and academia. Working together, we can increase Canada's resilience against cyber threats. Cyber security investments will allow OT asset operators to benefit from new technologies, while avoiding undue risks to the safe and reliable provision of critical services to Canadians.

USEFUL RESOURCES

- An Introduction to the Cyber Threat Environment
- National Cyber Threat Assessment 2020
- Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector
- Cyber Threat Bulletin: Modern Ransomware and Its Evolution
- Baseline Cyber Security Controls for Small and Medium Organizations
- Top 10 IT Security Actions for Internet Connected Systems
- Cyber Centre's Advice on Mobile Security
- Ransomware: How to Prevent and Recover
- Protect Your Organization from Malware
- IoT Security for Small and Medium Organizations
- Security Review Program Fact Sheet
- Cyber Security Considerations for Contracting with Managed Service Providers
- Malicious Cyber Activity Targeting Managed Service Providers
- Application Allow Lists Explained
- Security Vulnerabilities and Patches Explained
- Joint Report on Publicly Available Hacking Tools
- Cyber Security Tips for Remote Work
- Security Tips for Organizations with Remote Workers
- Focused Guidance Surrounding COVID-19, List of Publications per Audience
- COVID-19 and Malicious Websites
- Canadian Shield – Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic
- Have You Been Hacked?
- Protecting Your Organization from Denial of Service Attacks
- Spotting Malicious Email Messages
- Implementing Multi-Factor Authentication
- How Updates Secure Your Device
- Steps to Address Data Spillage in the Cloud
- Protecting High-Value Information
- Supply Chain Security for Small and Medium-sized Organizations
- Technology Supply Chain Guidelines
- Using Your Mobile Device Securely
- Security Considerations for Mobile Device Deployments
- Best Practices for Passphrases and Passwords
- Don't Take the Bait: Recognize and Avoid Phishing Attacks
- Little Black Book of Scams
- Keyloggers and Spyware
- Doppelganger Campaigns and Wire Transfer Fraud

ANNEX A: DESCRIPTION OF SOPHISTICATION

Level of Sophistication	Sophistication Characteristics	Typical Cyber Threat Actors
Low	• Uses a single, simple cyber capability • Single target • Little or no planning involved • Likely impact: nuisance, no lasting effect on anybody	States, hacktivists, cybercriminals, thrill-seekers
Medium	• A few cyber capabilities used competently • More than one target • Planning required • Likely impact: Multiple people affected, divert time and resources to dealing with activity	States, cybercriminals
High	• Several cyber capabilities used expertly • Numerous targets • Extensive, long-term planning and coordination • Likely impact: numerous people affected and forced to divert significant time and resources to counter the activity	States, cybercriminals

ANNEX B: DATA COLLECTION AND ANALYSIS

To quantify the cyber threat to OT, the Cyber Centre collected data on global cyber incidents from available open-source cyber incident databases, international media outlets, and vendor reporting, and collated a list of significant cyber incidents that occurred between 2010 to 2020. Details for each incident were examined, including date, victims, and sectors impacted. Threat actor type and motive, and sophistication of the incident were also assessed. If the victim organization owned an OT system, the Cyber Centre attempted to determine whether the OT asset was impacted (directly or indirectly) by the cyber activity. This includes OT shutdowns indirectly resulting from cyber activity in administrative IT networks.

ANNEX C: OT-RELATED CYBER SECURITY INCIDENTS

State-Sponsored Incidents Impacting OT

Year	Target	Description	Alleged Origins	Sophistication Assessed
2010	• Natanz Nuclear Facility and Bushehr Nuclear Power Plant • Location: Iran	Stuxnet first to target OT in Iranian nuclear enrichment facilities. The malware disrupted the industrial computers at Iran's uranium enrichment plants, dropping productivity by 30% over the course of a year. TTPs: Stuxnet malware, Zero-day exploits.[53]	State-sponsored	High
2012	• Saudi Aramco and RasGas • Location: Saudi Arabia, Qatar	State-sponsored Iranian actors deploy Shamoon wiper malware to IT networks, deleting data on 30,000 computers and infecting (without causing damage) OT control systems. TTPs: Shamoon Malware. [54]	Iran	Medium

Year	Target	Description	Alleged Origins	Sophistication Assessed
2013	• Bowman Avenue Dam • Location: United States	Iranian cyber threat actors gain access to the Bowman dam's flood gate control system, but were not able to have any effect because the flood gates were offline for maintenance. TTPs: Undisclosed Malware, Spear-phishing. [55]	Iran	Low
2014	• Organizations with OT assets • Location: United States and Europe	Russian state-sponsored threat actor Dragonfly launches a global cyber-espionage operation against US and European companies with OT assets. TTPs: Havex Remote Access Trojan (RAT), Watering Hole Attacks. [56]	Russia	High
2015	• An unnamed steel mill • Location: Germany	Cyber threat actors infiltrated a German steel mill via a social engineering campaign, and caused physical destruction by disrupting controls systems that prevented the blast furnace from shutting down properly. TTPs: Spear-Phishing, Social Engineering. [57]	Likely state-sponsored	High
2015	• Oblenergos • Location: Ukraine	Russian Blackenergy malware used in unprecedented attack on Ukrainian critical infrastructure. Coordinated incidents targeted and damaged several regional distribution power companies' SCADA systems, resulting in a 3–6-hour outage affecting approximately 225,000 Ukrainians. TTPs: Blackenergy Malware, Spear-Phishing, DoS.[58]	Sandworm (Russia)	High
2016	• Ukrenergo • Location: Ukraine	Russian malware used to shut down remote terminal units from the Pivnichna power transmission facility, resulting in a partial blackout and a 20 percent power consumption loss in Kyiv. TTPs: Industroyer/ Crashoverride Malware. [59]	Sandworm (Russia)	High
2017	• National Electricity Network • Location: Turkey	The Turkish Energy Minister stated a severe cyber incident targeted electricity transmission and producing lines, causing widespread electricity cuts across Istanbul. TTPs: Undisclosed. [60]	Unattributed	High
2017	• Unnamed Energy Companies • Location: United Kingdom	UK GCHQ issued an alert indicating hackers penetrated industrial control systems of UK energy companies. TTPs: Undisclosed Malware, Spear-Phishing.[61]	State-sponsored	High
2017	• An unnamed oil and gas facility • Location: Middle East	Cyber threat actors gained remote access to a SIS engineering workstation, and reprogrammed an SIS unit with Triton malware; errors prompted an automatic shutdown of the industrial process. TTPs: Triton/Trisis Malware.[62]	Xenotime (Russia)	High

Year	Target	Description	Alleged Origins	Sophistication Assessed
2018	• Western critical infrastructure supply chain, including Wolf Creek Nuclear Operating Corporation • Location(s): United States	A supply chain incident where threat actors breached third-party entities and moved laterally to high-value asset owners within the energy sector; they stole confidential data on ICS and other processes. TTPs: Spear-Phishing Waterhole Domains, Host-Based Exploitation. [63]	Energetic Bear / DragonFly (Russia)	High
2020	• Upper Galilee and Mateh Yehuda region water pumps • Location: Israel	Israel successfully defended against two cyber incidents targeting the control systems of water treatment plants, pumping stations, and sewage in the country. TTPs: Undisclosed.[64]	Jerusalem Electronic Army (Iran)	Medium
2020	• Shahid Rajaee port terminal • Location: Iran	Hackers disrupted operations the port, knocking computers offline for several days; impeding traffic. TTPs: Undisclosed.[65]	Israel	High

Cybercrime Incidents Impacting OT

Year	Target	Description	Alleged Origins	Sophistication Assessed
2011	• An unnamed power plant • Location: Brazil	A virus infected all of the power plant's machines using the Alstrom ALSPA system, disrupting operations and management systems. TTPs: Conficker virus.[66]	Unattributed	Low
2012	• Two unnamed power plants • Location: United States	An employee unknowingly inserted an infected USB into the network, keeping the plant offline for three weeks. TTPs: Mariposa Malware.[67]	Unattributed	Low
2014	• An unnamed public utility • Location: United States	Hackers took advantage of weak password security and broke into the system; however, scheduled maintenance disconnected the mechanical devices from the control system. TTPs: Brute Force.[68]	Unattributed	Low
2016	• An unnamed water treatment company • Location: Unknown	Hackers stole confidential financial records and accessed the water district's valve and flow control application responsible for manipulating hundreds of PLCs that control water treatment chemical processing. TTPs: SQL Injection, Spear-Phishing.[69]	Unattributed	Low
2018	• Colorado Department of Transportation • Location: United States	Ransomware shut down 2,000 computers for several days, costing the department an estimated 1.7 million (USD). TTPs: SamSam Ransomware.[70]	Unattributed	Medium

Year	Target	Description	Alleged Origins	Sophistication Assessed
2019	• Norsk Hydro • Location: Norway, International	The incident disrupted operations (logistical and production), forcing some of the company's aluminum plants to switch to manual processes. The financial impact is approximately $71 million. TTPs: LockerGoga Ransomware.[71]	Unattributed	Medium
2019	• City Power (Johannesburg) • Location: South Africa	The ransomware shut down IT systems, affecting more than 250,000 people through regional blackouts, and prevented customers from purchasing prepaid electricity. TTPs: Undisclosed Ransomware.[72]	Unattributed	Medium
2020	• Picanol Group • Location: Belgium, Romania, Chile	At three satellite locations, the incident halted computerized production as the company did not have access to its systems—an estimated 196 plant days lost. TTPs: Undisclosed Ransomware.[73]	Unattributed	Medium
2020	• An unnamed natural gas compression facility • Location: United States	The facility shut down operations for two days once the ransomware traversed from IT networks into ICS responsible for monitoring pipeline operations, impacting assets on the OT system like human-machine interfaces (HMIs), data historians, and polling servers. TTPs: Undisclosed Ransomware, Spear-Phishing.[74]	Unattributed	Low
2020	• Universal Health Services (UHS) • Location: United States	The incident caused over 250 hospitals to revert to manual backups, divert ambulances, and reschedule surgeries; it may have contributed to four deaths. • TTPs: likely Ryuk Ransomware, Phishing, Emotet Trojan.[75]	Likely WIZARD SPIDER	Medium
2020	• The University Hospital Düsseldorf (UKD) • Location: Germany	Through an unpatched vulnerability, hackers penetrated the hospital's network with ransomware, forcing planned and outpatient treatments and emergency care to have to occur elsewhere. TTPs: Undisclosed Ransomware, Code Exploit.[76]	Unattributed	Low
2020	• Steelcase Inc. • Location: United States	The incident caused an operational shutdown of most of the company's global order management, manufacturing and distribution systems, significantly delaying shipments. Plant-days lost is an estimated 140 days. TTPs: Ryuk Ransomware.[77]	Likely WIZARD SPIDER	Medium
2020	• Miltenyi Biotec • Location: Germany, International	The organization shut down operational processes for two weeks worldwide; hackers stole approximately 150 GB of company data. TTPs: Mount Locker Ransomware.[78]	Mount Locker ransomware gang	Low

OT Incidents from Other Actors

Year	Target	Description	Alleged Origins	Sophistication Assessed
2012	• An undisclosed air conditioning company and the US government • Location: United States	Hackers accessed a backdoor into the ICS system that allowed access to the key control mechanism for the company's internal heating, ventilation, and air conditioning (HVAC) units. TTPs: Undisclosed Malware, Code Exploits.[79]	Thrill-seeker	Low
2014	• Daktronics Vanguard roadside signs • Location: United States	Threat actors hacked into roadside signs and posted bogus warnings. TTPs: Code exploits.[80]	Thrill-seeker	Low

ENDNOTES

[1] Perkins, E. “Operational Technology Security – Focus on Securing Industrial Control and Automation Systems.” *Gartner*. 14 March 2014. https://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security-focus-on-securing-industrial-control-and-automation-systems/

[2] Williams, H. "Size of the global industrial automation market from 2019 to 2026 (in billion US dollars).” Chart. October 31, 2020. *Statista*. Accessed 13 May 2021. https://www.statista.com/statistics/1219772/industrial-automation-market-size-worldwide/

[3] HfS Research. “Adoption rate of intelligent automation (IA) technologies in organizations worldwide in 2019*.” Chart.” *Statista*. 18 April 2020. Accessed 13 May 2021. https://www.statista.com/statistics/1114893/adoption-rate-intelligent-automation-organizations/

[4] “Stop Malicious Cyber Activity Against Connected Operational Technology.” National Security Agency Cybersecurity Advisory. 29 April 2021. https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF; “Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks,” *Fortinet*, May 7, 2018. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

[5] “Russian state-sponsored cyber actors targeting network infrastructure devices.*” US Department of Homeland Security, US Federal Bureau of Investigation, and UK National Cyber Security Centre*. 15 April 2018. https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

[6] Graham, A. “Canada's Critical Infrastructure: When is Safe Enough Safe Enough?” *MacDonald-Laurier Institute*. December 2011. http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

[7] Krauss, C., N. Chokshi, and D.E. Sanger. "Gas Pipeline Hack Leads to Panic Buying in the Southeast." *New York Times*. 11 May 2021. https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html

[8] “Cyberattack closes JBS meat-packing facilities in Canada, US and Australia.” *CBC* Business News. 01 July 2021. https://www.cbc.ca/news/business/jbs-meat-cyberattack-1.6048942

[9] “Canada’s Critical Infrastructure.” *Public Safety Canada*. 19 May 2020. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

[10] “An Introduction to the Cyber Threat Environment.” *Canadian Centre for Cyber Security*. 18 November 2020. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

[11] Ginter, A. “Secure Operations Technology.” *Abterra Technologies, Inc*. 2019.

[12] “An Introduction to the Cyber Threat Environment.” *Canadian Centre for Cyber Security*. 18 November 2020. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

[13] “Cyber Threat Bulletin: Modern Ransomware and Its Evolution.” Canadian Centre for Cyber Security. 18 September 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution

[14] “Ransomware Against the Machine: How Adversaries Are Learning to Disrupt Industrial Production by Targeting IT and OT.” *FireEye*. 24 February 2020. https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

[15] Ilascu, I. “LockerGoga Ransomware Sends Norsk Hydro Into Manual Mode.” *Bleeping Computer*. 19 March 2019. https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/; Hotter, A. “How the Norsk Hydro cyberattack unfolded.” *American Metal Market*. 22 August 2019. Aug 22, 2019. https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html

[16] “Ransomware Activity Targeting the Healthcare and Public Health Sector.” *US Cybersecurity and Infrastructure Security Agency* Alert (AA20-302A). 28 October 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[17] Hope, A. “Ryuk Ransomware Attack Disrupts Universal Healthcare Services Operations Resulting in Ambulance Diversions and Alleged Deaths.” *CPO Magazine*. 8 October 2020. https://www.cpomagazine.com/cyber-security/ryuk-ransomware-attack-disrupts-universal-healthcare-services-operations-resulting-in-ambulance-diversions-and-alleged-deaths/

[18] "Cyber Threat Bulletin: Modern Ransomware and Its Evolution." Canadian Centre for Cyber Security. 13 August 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution

[19] Greenberg, A. "Mysterious New Ransomware Targets Industrial Control Systems." *Wired*. 3 February 2020. https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Brubaker, N. et. al. "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families." *FireEye* Threat Research Blog. 15 July 2020. https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

[20] "Ransomware Impacting Pipeline Operations." *US Cybersecurity and Infrastructure Security Agency* Alert (AA20-049A). 18 February 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-049a

[21] Jackson-Higgins, K. "Ryuk Ransomware Hit Multiple Oil & Gas Facilities, ICS Security Expert Says." *DarkReading*. 23 January 2020. https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865

[22] Assante, M.J. and R.M. Lee. "The Industrial Control System Cyber Kill Chain." *SANS Institute*. 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

[23] Yadron, D. "Iranian Hackers Infiltrated New York Dam in 2013." *Wall Street Journal*. 20 December 2015. https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

[24] "Hack attack causes 'massive damage' at steel works." *BBC News*. 22 December 2014. https://www.bbc.com/news/technology-30575104

[25] "CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations." *Dragos Inc*. 12 June 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[26] "Cyber attacks again hit Israel's water system, shutting agricultural pumps." *Times of Israel*. 17 July 2020. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

[27] Warrick, J., and E. Nakashima. "Officials: Israel linked to a disruptive cyberattack on Iranian port facility." *The Washington Post*. 18 May 2020. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

[28] "National Counterintelligence Strategy of the United States of America 2020-2022 Executive Summary." *US National Counterintelligence and Security Center*. https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022_Executive_Summary.pdf

[29] "Securing the United States Bulk-Power System Executive Order." *Office of Electricity, US Department of Energy*. September 15, 2020. https://www.energy.gov/oe/bulkpowersystemexecutiveorder

[30] Johnson, B., D. Cuban, M. Krotofil., D. Scali, N. Brubaker, and C. Glyer. "Threat actors Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure." *FireEye*. 14 December 2017. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[31] Di Pinto, A. Y. Dragoni, and A. Carcano "TRITON: The First ICS Cyber Attack on Safety Instrument Systems. Understanding the Malware, Its Communications and Its OT Payload" *Nozomi Networks*. 2018. https://www.nozominetworks.com////downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf

[32] "TRISIS Malware Analysis of Safety System Targeted Malware" *Dragos Inc*. 14 December 2017. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

[33] "Daktronics Vanguard Default Credentials (Update A)." *US Department of Homeland Security* (ICS-ALERT-14-155-01A). 5 June 2014. https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-155-01A

[34] "National Cyber Threat Assessment 2020." *Canadian Centre for Cyber Security*. 16 November 2020. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

[35] E.g. https://scadahacker.com/resources/msf-scada.html

[36] Sheridan, K. “Cobalt Strike & Metasploit Tools Were Attacker Favorites in 2020.” *DarkReading*. 7 January 2021. https://www.darkreading.com/risk/cobalt-strike-and-metasploit-tools-were-attacker-favorites-in-2020/d/d-id/1339854

[37] “Dragonfly: Western energy sector targeted by sophisticated attack group.” *Symantec Enterprise Blog*. 20 October 2017. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks; “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors” *US Department of Homeland Security and US Federal Bureau of Investigation Alert* (TA18-074A). March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A

[38] Greenberg, A. “A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems.” *Wired*. 20 November, 2019. https://www.wired.com/story/iran-apt33-industrial-control-systems/

[39] MITRE ATT&CK Framework. *The MITRE Corporation*. https://attack.mitre.org/

[40] Ohm, M., H. Plate, A. Sykosch, and M. Meier (2020) “Backstabber’s Knife Collection: A Review of Open Source Software Supply Chain Attacks.” In: Maurice C., Bilge L., Stringhini G., Neves N. (eds) *Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA 2020. Lecture Notes in Computer Science, vol 12223. Springer, Cham. https://doi.org/10.1007/978-3-030-52683-2_2

[41] Nelson, N. “The Impact of Dragonfly Malware on Industrial Control Systems” *SANS Institute*. January 18, 2016.https://www.sans.org/white-papers/36672/

[42] “3 Ways to Mitigate Risk When Using Private Package Feeds.” *Microsoft*. 29 March 2021. https://azure.microsoft.com/en-us/resources/3-ways-to-mitigate-risk-using-private-package-feeds/

[43] Claburn, T. “Apple, Microsoft, PayPal among 35 organizations compromised by evil twin dependencies attack.” *The Register*. https://www.theregister.com/2021/02/10/library_dependencies_attack/

[44] Birsan, A. “Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies.” *Medium*. 9 February 2021. https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[45] Statement on SolarWinds Cyber Compromise. *Global Affairs Canada*. 15 April, 2021. https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html

[46] “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.” *Fireeye Threat Research*. 13 December 2020. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[47] “SolarWinds Corp. SEC filing.” *United States Securities and Exchange Commission.* 14 December 2020. http://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf

[48] “Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.” *The Cybersecurity and Infrastructure Security Agency*. 15 April 2021. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[49] Walton, R. SolarWinds fallout could last for years, as power industry secures vulnerable equipment: Dragos CEO. *Utility Dive*. 05 February 2021. https://www.utilitydive.com/news/solarwinds-fallout-could-last-for-years-as-power-industry-secures-vulnerab/594598/

[50] “President Trump Signs Executive Order Securing the United States Bulk-Power System.” *US Department of Energy.* 15 May 2020 https://www.energy.gov/articles/president-trump-signs-executive-order-securing-united-states-bulk-power-system

[51] “Malicious Cyber Activity Targeting Managed Service Providers.” *Canadian Centre for Cyber Security* Alert AL17-004. 04 April 2017. https://cyber.gc.ca/en/alerts/malicious-cyber-activity-targeting-managed-service-providers

[52] “Canada and Allies Identify China as Responsible for Cyber-Compromise.” *Communications Security Establishment* (CSE) media release. 20 December 2018. https://cse-cst.gc.ca/en/information-and-resources/announcements/canada-and-allies-identify-china-responsible-cyber

[53] Fildes, J. “Stuxnet worm 'targeted high-value Iranian assets” *BBC News*. 23 September 2010. https://www.bbc.com/news/technology-11388018; Melman, Y. “Computer Virus in Iran Actually Targeted Larger Nuclear Facility.” *Haaretz*. 28 September 2010. https://www.haaretz.com/1.5118389

[54] Finkle, J. “Exclusive: Insiders suspected in Saudi cyber attack.” *Reuters*. 7 September 2012. https://www.reuters.com/article/net-us-saudi-aramco-hack/exclusive-insiders-suspected-in-saudi-cyber-attack-idUSBRE8860CR20120907

[55] Yadron, D. “Iranian Hackers Infiltrated New York Dam in 2013.” *Wall Street Journal*. 20 December 2015. https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

[56] “ICS Focused Malware (Update A).” *The Cybersecurity and Infrastructure Security Agency* (ICS-ALERT-14-176-02A). 27 June 2014 https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-176-02A

[57] “Hack incident causes 'massive damage' at steel works.” *BBC News.* 22 December 2014. https://www.bbc.com/news/technology-30575104

[58] “Cyber-Incident Against Ukrainian Critical Infrastructure.” *US Department of Homeland Security* (Ir-ALERT-H-16-056-01). 25 February 2016. https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

[59] Zinets, N. “Ukraine hit by 6,500 hack incidents, sees Russian cyberwar.” *Reuters*. 29 December 2016. https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC

[60] “Major cyber-incident on Turkish Energy Ministry claimed.” *Hürriyet Daily News*. 31 December 2016. https://www.hurriyetdailynews.com/major-cyber-incident-on-turkish-energy-ministry-claimed-107981

[61] Cox, J. “GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets.” *Vice*. 7 July 2017. https://www.vice.com/en_us/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets

[62] Johnson, B., D. Cuban, M. Krotofil., D. Scali, N. Brubaker, and C. Glyer. “Threat actors Deploy New ICS Incident Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure.” *FireEye*. 14 December 2017. https://www.fireeye.com/blog/threat-research/2017/12/threat actors-deploy-new-ics-incident-framework-triton.html

[63] “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” *US Department of Homeland Security and US Federal Bureau of Investigation* Alert (TA18-074A). 15 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A

[64] Cyber incidents again hit Israel’s water system, shutting agricultural pumps.” Times of Israel. 17 July 2020.

https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

[65] Warrick, J., and E. Nakashima. “Officials: Israel linked to a disruptive cyber incident on Iranian port facility.” The Washington Post. 18 May 2020. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

[66] Branquinho, M. “Recent malware infections on control system networks in Brazil.” *TI Safe*. September 2011. https://www.slideshare.net/tisafe/apresentao-tcnica-infeces-por-malware-no-brasil

[67] “Malware Infections in the Control Environment.” *US Department of Homeland Security* (ICS-CERT Monitor: October/November/December 2012). December 2012. https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

[68] “Internet Accessible Control Systems at Risk.” *US Department of Homeland Security* (ICS-CERT Monitor: January-April 2014). https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf

[69] Leyden, J. “Water treatment plant hacked, chemical mix changed for tap supplies.” *The Register*. 24 March 2016. https://www.theregister.com/2016/03/24/water_utility_hacked/

[70] Chuang, T., and D. Migoya, “SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers.” *The Denver Post*. 21 February 2018 https://www.denverpost.com/2018/02/21/samsam-virus-ransomware-cdot/21

[71] “Cyber-incident on Hydro.” *Norsk Hydro*. March 2019. http://hydro.com/en/media/on-the-agenda/cyber-incident/

[72] “Ransomware hits Johannesburg electricity supply.” *BBC News*. 26 July 2019. https://www.bbc.com/news/technology-49125853

[73] “Press release: cyber incident - update January 31, 2020.” *Picanol*. 31 January 2020. https://www.picanol.be/news/press-release-cyber-incident-update-january-31-2020

[74] “Ransomware Impacting Pipeline Operations.” *The Cybersecurity and Infrastructure Security Agency* (AA20-049A). 18 February 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-049a

[75] Crawford, J. “Statement from Universal Health Services.” *Universal Health Services*. 29 October 2020. https://www.uhsinc.com/statement-from-universal-health-services/; Gatlan, S. “Universal Health Services lost $67 million due to Ryuk ransomware attack.” *Bleeping Computer*. 1 March 2020. https://www.bleepingcomputer.com/news/security/universal-health-services-lost-67-million-due-to-ryuk-ransomware-attack/.

[76] Tidy, J. “Police launch homicide inquiry after German hospital hack.” *BBC News*. 18 September 2020. https://www.bbc.com/news/technology-54204356

[77] “Steelcase BC Form 8-K.” *United States Securities and Exchange Commission*. 12 November 2020. https://beta.documentcloud.org/documents/20404615-steelcase-bc-form-8-k#document/p3/a2004430

[78] Gatlan, S. “Biotech research firm Miltenyi Biotec hit by ransomware, data leaked.” *Bleeping Computer*. 13 November 2020 https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/

[79] “Situation Information Report.” *Federal Bureau of Investigation* (FBI). 23 July 2012. https://info.publicintelligence.net/FBI-AntisecICS.pdf

[80] “Daktronics Vanguard Default Credentials (Update A).” *US Department of Homeland Security* (ICS-ALERT-14-155-01A). 5 June 2014. https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-155-01A

CAT. D96-81/2021E-PDF
ISBN 978-0-660-41268-9

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada