TLP:WHITE

Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER THREAT BULLETIN

The Cyber Threat to Canada's Electricity Sector

Canada

ABOUT THIS DOCUMENT

AUDIENCE

This Cyber Threat Bulletin is intended for the cyber security community. 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.

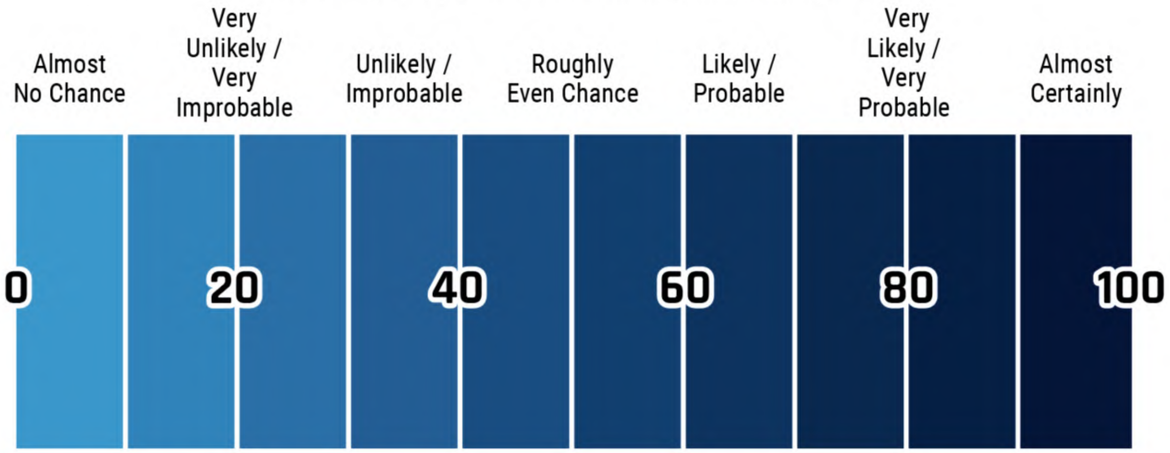
ASSESSMENT BASE AND METHODOLOGY

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 contents of this document are based on information available as of 29 September 2020.

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

- To date, cyber threat activity against Canada's electricity sector has consisted mostly of fraud and ransomware attempts by cybercriminals, as well as espionage and pre-positioning by state-sponsored actors, all of which we expect will very likely continue.
- We judge that cybercriminals are almost certainly improving their capabilities, and are increasingly likely to attempt to access, map, and exploit industrial control systems (ICS) for extortion with customized ransomware. We assess that cybercriminals will likely be capable of targeting electricity sector ICS for extortion within the next three years.
- We judge that it is very unlikely that state-sponsored cyber threat actors will intentionally seek to disrupt the Canadian electricity sector and cause major damage or loss of life in the absence of international hostilities. However, the likelihood of a cyber attack impacting the Canadian electricity sector is higher than it otherwise might be because of the connections between US and Canadian grids: cyber threat actors likely view Canada as an intermediate target through which they can impact the US electricity sector, and the increased levels of threat activity against US grids could result in an event that impacts the Canadian electricity sector.
- High-sophistication cyber threat actors target the supply chain and managed service providers for two purposes: to obtain intellectual property and information about the ICS of a utility; and, as an indirect route to access the networks of electricity utilities. We assess this will almost certainly continue for the next 12 months and beyond.
- We assess that cyber threat actors are likely adapting their activities to new opportunities provided by the transition to smart grid technology. We assess that new forms of smart grid technology will likely increase the vulnerability of ICS to cyber threats.

CANADA’S ELECTRICITY SECTOR

The North American electricity grid has been popularly described as the world’s largest machine and has been growing continuously since its conception in the late 1800s. The modern grid is a continent-spanning system of systems, composed of different technologies and organizations dedicated to the generation, transmission, management, and distribution of electricity. (Figure 1)

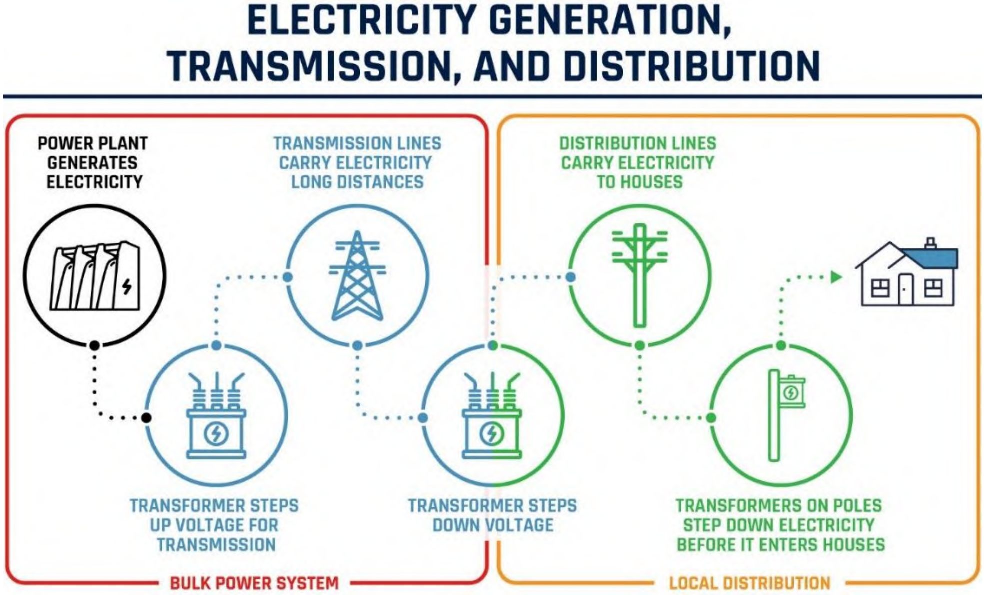

ELECTRICITY GENERATION, TRANSMISSION, AND DISTRIBUTION
POWER PLANT GENERATES ELECTRICITY
TRANSMISSION LINES CARRY ELECTRICITY LONG DISTANCES
DISTRIBUTION LINES CARRY ELECTRICITY TO HOUSES
TRANSFORMER STEPS UP VOLTAGE FOR TRANSMISSION
TRANSFORMER STEPS DOWN VOLTAGE
TRANSFORMERS ON POLES STEP DOWN ELECTRICITY BEFORE IT ENTERS HOUSES
BULK POWER SYSTEM
LOCAL DISTRIBUTION

Figure 1. Simplified organizational diagram of the electricity system

It is hard to overstate the importance of electricity to Canada. Any significant disruption of electricity directly impacts Canada’s national security, public safety, and economy. A power outage in August 2003 that lasted less than a week in northeastern North America caused an estimated $2.3 billion CAD loss to the economy of Ontario, contributed to a 0.7% decrease in Canada’s GDP in August,[1] and very likely led to loss of life.[2] Our reliance on electricity has grown significantly since 2003 and is projected to continue to grow as a result of several factors; most notably, the electrification of the transportation sector.[3]

Cyber threat activity targeting the electricity sector in Canada and worldwide has been on the rise over the past ten years. Organizations in the electricity sector face cyber threat activity from cybercriminals, who are enticed by the prospects of ransom payments, business fraud spoils, and intellectual property. Because of the fundamental importance of the electricity sector, state-sponsored threat actors target the organizations in it to achieve their geopolitical goals. Canada’s largest electricity grids are connected to each other and to US grids, with more than 35 Canada-US transmission line connections, called interties, across all provinces bordering the US. These interties increase the reliability of the system and enable efficiencies, but also increase the likelihood that cyber attacks and other grid problems will be jointly experienced by Canadians and Americans.

Table 1: Electricity Sector Technology Terms

Bulk Power System (BPS)	The generation, transmission, and energy management systems of the grid. Faults in the BPS could affect multiple local distribution regions, potentially crossing provincial and national borders. The BPS does not include elements of the grid involved in lower-voltage, local distribution of electricity.
Information Technology (IT)	Hardware and software for storing, retrieving, and communicating information; used for business and administrative operations.
Operational Technology (OT)	Hardware and software that interface with devices that can cause changes in the physical world; widely used to automate mechanical processes. Used by the electricity sector for industrial control systems.
Industrial Control Systems (ICS)	Specialized OT that monitors and controls mission-critical industrial processes. An important characteristic of an ICS is the ability to sense and change the physical state of industrial equipment.

TARGETING CANADA'S GRID

To date, cyber threat activity against Canada's electricity sector has consisted of fraud and ransomware attempts by cybercriminals, as well as espionage and pre-positioning by state-sponsored actors, all of which we expect will very likely continue. Low-sophistication (see annex for definition) hacktivists, terrorists, and disgruntled individuals could cause embarrassment and reputational damage to Canada's electricity sector (e.g., by defacing websites), but are very unlikely to be able to disrupt the supply of electricity. Cyber threat activity targets local distribution and bulk power system organizations, but threat actors intent on disrupting electricity or extracting a more lucrative ransom are more likely to target organizations involved in the bulk power system (BPS, see Table 1).

Threat Activity: Cybercriminals

We assess that cybercriminals will almost certainly continue to target the Canadian electricity sector to extract ransom, steal intellectual property and proprietary business information, and obtain personal data about customers. We assess that cybercriminals are almost certainly targeting heavy industry and critical infrastructure to increase their chances of obtaining a large ransom. Over the past two years, ransomware attacks with the potential to affect industrial processes have become more frequent in Canada and around the world. Since January 2019, at least seven ransomware variants have contained instructions to terminate ICS processes that would normally run on industrial control workstations.[4]

Notable Cybercriminal Activity Against the Electricity Sector

- On 30 April 2020, the Northwest Territories Power Corporation's business systems and website were encrypted by ransomware.[5]
- On 11 May 2020, cybercriminals reportedly deployed ransomware on the business systems of the UK grid balance authority Elexon, stole and posted sensitive internal data, and caused it to suffer loss of some network functions like email.[6]
- On 7 June 2020, the Buenos Aires, Argentina local distribution utility Edesur S.A. lost some of the functions of their IT systems.[7] In all cases, the ICS network, and ultimately the electricity supply, were unaffected.

Although there are no reported examples of ransomware affecting the ICS of the electricity sector, we assess that ransomware has almost certainly improved its ability to spread through corporate IT networks and threaten adjacent ICS.[8] In some cases, victims have chosen to disable their industrial processes as a precautionary measure during a significant ransomware event. For example, in February 2020, ransomware impacted a US natural gas compression facility, traversing Internet-facing IT networks into ICS responsible for monitoring pipeline operations.[9] In March 2019, a Norwegian aluminum company was impacted by a ransomware event that disrupted its logistical and production data so severely that it prompted the shutdown of ICS and reversion to manual operations.[10] The impact of a ransomware attack on ICS varies according to the specific circumstances of the industrial process and the reaction of the site staff.[11]

We judge that cybercriminals are almost certainly improving their capabilities, and are increasingly likely to attempt to access, map, and exploit the ICS of their targets for extortion with customized ransomware. We assess that cybercriminals will likely be capable of targeting electricity sector ICS for extortion within the next three years.

Other Threat Actors

We judge that it is likely that threat actors who lack access to sophisticated cyber capabilities are more likely to attempt a physical attack, such as the 2014 airplane attack on Hydro-Québec transmission lines that caused nearly $30 million CAD in damages and a short power outage affecting customers in the US and Ontario.[12]

Threat Activity: State-sponsored Actors

State-sponsored cyber threat actors have been targeting parts of the Canadian electricity sector since at least 2012. We judge that, almost certainly, the immediate purpose of this activity has been to collect information and pre-position cyber tools as a contingency for possible follow-on activities, or as a form of intimidation. These early stages of a potential future cyber attack tend to resemble industrial espionage.[13] We assess that it is very likely that state-sponsored actors are using the information gathered from their espionage activities to develop additional cyber capabilities that would allow them to cause a disruption in Canada's electricity sector.

We judge that it is very unlikely that state-sponsored cyber threat actors will intentionally seek to disrupt the Canadian electricity sector and cause major damage or loss of life in the absence of international hostilities. However, the likelihood of a cyber attack impacting the Canadian electricity sector is higher than it otherwise might be because of the connections between US and Canadian grids: cyber threat actors likely view Canada as an intermediate target through which they can impact the US electricity sector, and the increased levels of threat activity against US grids could result in an event that impacts the Canadian electricity sector. US assessments characterize the cyber threat to their critical infrastructure from state-sponsored actors as complex and aggressive[14] and have declared that the threats to their electricity sector BPS by foreign adversaries constitute a national emergency.[15] The actual impact on a Canadian electricity grid stemming from a cyber attack against a US grid would depend on the conditions at the impacted interties and grids, and the responses of the grid operators during the crisis.

Notable State-Sponsored Activity Against the North American Electricity Sector

- In mid-2019, Iranian state-sponsored actors conducted a large-scale espionage campaign on energy sector ICS suppliers, and in late 2019 targeted the US Department of Energy and US National Labs.[16]
- In mid-2019, several US utilities were targeted by Chinese state-sponsored cyber threat actors.[17]
- In 2019, Russian actors behind the Triton malware probed the networks of electricity utilities in the US (see Capability Development box below).[18]
- In 2018, the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) issued alerts about Russian state-sponsored cyber actors who targeted the supply chain to gain access into partner energy sector networks. After obtaining access, the actors conducted network reconnaissance and collected information related to ICS networks.[19]
- From at least 2014 (and possibly as early as 2011) to 2017, Russian state-sponsored cyber actors conducted an extensive cyber espionage campaign against Canadian, US, and European energy sector companies over several years, employing Havex malware to search for ICS components.[20]
- In 2013, a US power producer with a generation plant in Ontario was probed by multiple actors, including Iranian state-sponsored actors, who obtained information on the company's ICS.[21]

Beyond the North American context, state-sponsored activity against critical infrastructure, and especially the electricity sector, has become a regular occurrence. For example, starting in 2012 and continuing to the present, Iranian hacking groups have targeted critical infrastructure multiple times in Saudi Arabia and Israel.[22] In late 2019, malware attributed to North Korea was found in the IT networks of Indian power plants.[23]

The first electricity outages from state-sponsored cyber activity occurred in 2015-2016 in Ukraine. In late 2015, Russian state-sponsored 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.[24] 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 the electricity sector, and its use during international hostilities.

Capability Development

In 2017, Russian actors tested a capability called Triton (a.k.a. Trisis) to modify the performance of an automated ICS safety system at a Middle Eastern oil and gas facility. The same actors were noted to be probing the networks of electricity utility organizations in the US and elsewhere in early 2018, indicating this group's interest in the electricity sector.[25] Although Triton was specific to the software and equipment setup at the Saudi facility,[26] we assess that that these actors or others with similar sophistication would likely be able to modify the capability to target North American systems.

TARGETING THE SUPPLY CHAIN AND MANAGED SERVICE PROVIDERS (MSPs)

Like many other large industrial asset operators, grid operators depend on a supply chain and MSPs (i.e., laboratories, manufacturers, vendors, integrators, and contractors) for non-routine maintenance, modernization, and development of new capacity in the grid. High-sophistication cyber threat actors target the supply chain and MSPs for two purposes: to obtain intellectual property and information about the ICS of a utility; and, as an indirect route to access the networks of electricity utilities. We assess that high-sophistication actors will almost certainly continue to target the supply chain and MSPs of the electricity sector for the next 12 months and beyond.

Obtaining Intellectual Property and Information About the ICS

We assess that high-sophistication cyber threat actors almost certainly target the electricity sector supply chain to obtain intellectual property of commercial value and other sensitive information about clients, such as information about ICS, that they can use to develop cyber attack capabilities. For example, in late 2012, grid software supplier Televent Canada Ltd. warned that cyber actors, later associated with China, had stolen project files related to its ICS software used by grid operators to integrate advanced technology.[27] In 2014, and again in 2017, Russia-associated cyber threat actors undertook an espionage campaign against a variety of supply chain targets in the energy sector, including the electricity sector.[28] More recently, 2019 reports linked Iran to cyberespionage activity against manufacturers, suppliers, and operators of ICS equipment.[29]

Accessing the Networks of Electricity Utilities Indirectly

A supply chain compromise occurs when products are deliberately exploited and altered prior to use by a final consumer.[30] While a supply chain compromise could occur in hardware or software, threat actors have often focused on malicious additions to legitimate software in software distribution or update channels. In 2014, Russian state-sponsored cyber actors compromised the networks of three ICS vendors and replaced legitimate software updates with corrupted packages that included Havex malware. Users of the ICS products downloaded what they believed were updates, and unknowingly installed Havex in their ICSs, giving the cyber threat actors access to various organizations related to the European energy sector.[31] We assess that a supply chain compromise is more likely to affect software than hardware, but that malicious hardware alteration is not out of the range of abilities of the most sophisticated state-sponsored cyber threat actors.

In addition to targeting the supply chain, we assess that it is very likely that foreign state-sponsored actors and cybercriminals are attempting to leverage MSPs' privileged access to their clients' systems as an indirect route into their true targets, the utilities or other companies in the electricity sector. Although this type of activity has not been publicly reported in the electricity sector, we assess that it is likely that it has already occurred or will occur in the next year.

By targeting MSPs, threat actors can scale their activities. 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 over $3 million CAD. On 4 April 2017, the Cyber Centre warned of ongoing malicious cyber activity targeting MSPs internationally,[32] and in 2018 CSE attributed the activity to a Chinese state-sponsored actor.[33] Canada's allies in the UK and US have issued similar warnings, noting the presence of Russian state-sponsored actors on Internet infrastructure such as routers, switches, and firewalls, which they can use to impact ICS. [34]

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 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.[35]

INCREASING VULNERABILITY OF INDUSTRIAL CONTROL SYSTEMS (ICS)

Electricity utilities depend on their ICS to centrally monitor and manage their parts of grid. The operational technology (OT) used in ICS predates the Internet and was designed first and foremost for industrial safety and reliability. Historically, OT remained largely unconnected to the Internet, which made it difficult if not impossible for cyber threat actors to access. In the past few decades, however, many industries, including the electricity sector, have been increasing the management efficiency and reliability of their OT networks by incorporating IT devices and protocols. An unintended consequence of this OT-IT convergence trend is an increase in the exposure and vulnerability of OT to IT cyber threats delivered via the Internet. We assess that the electricity sector's OT (i.e., the ICS) is almost certainly the priority target for cyber threat actors who intend to affect the delivery of electricity.

Even more recently, advanced technology from the IT sector has been applied to grid infrastructure to create devices with enhanced processing and networking capabilities to reduce operational costs, emit less greenhouse gases, and meet increased electricity demand.[36] Called "smart grids", they are intended to adapt intelligently and in real-time to fluctuations in electricity consumption and to "auto-heal" faults. However, smart grid developments tend to increase the vulnerability of OT to cyber threats for a variety of reasons. These reasons include increasing connectivity of OT to the Internet, the complexity of the new devices and their diverse supply chain, and ICS interconnections between organizations that could allow cyber threats to propagate through connected ICS.

Advanced metering infrastructure (AMI) is the first component of the smart grid that has been broadly deployed across Canada.[37] We assess that the cyber threat to AMI (i.e., the smart meters, AMI communications networks, and meter data management systems) as they are currently configured, is likely very low. We judge, however, that the deployment of smart grid technology that incorporates additional OT-IT convergence will likely increase the vulnerability of ICS to cyber threats.[38]

We assess that cyber threat actors are likely adapting their activities to take advantage of this OT-IT convergence and the new opportunities provided by the transition to the smart grid (see Figure 2).

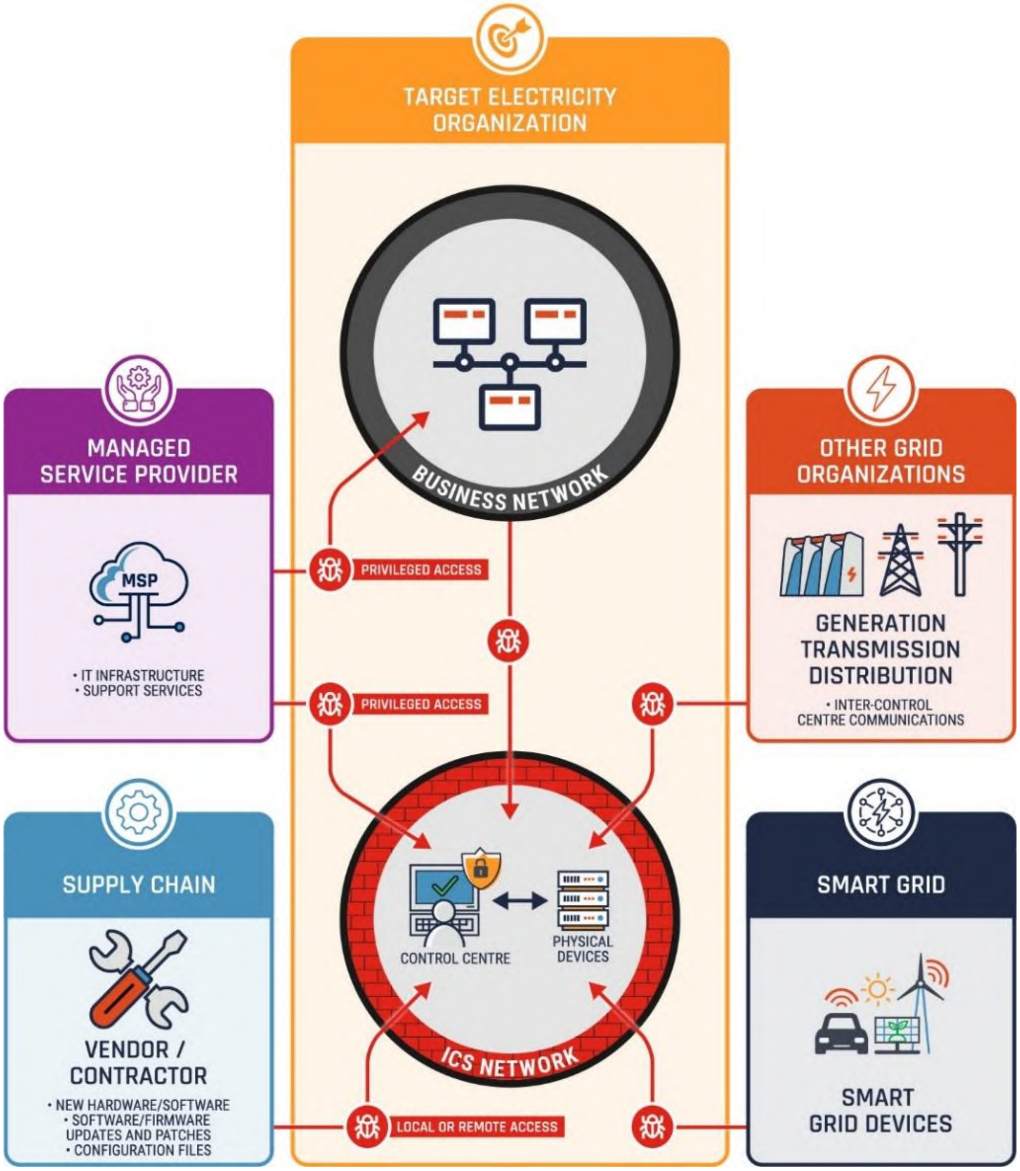


Figure 2. Cyber Routes to OT

CONCLUSION

The cyber threat landscape experienced by the electricity sector in Canada is evolving. In this assessment, we identified trends within the threat landscape, including the accelerating threat from cybercriminals and state-sponsored actors, as well as the introduction of new threat vectors stemming from the adoption of new technology and Internet-connected devices. Many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber security investments will allow electricity sector organization to benefit from new technologies while avoiding undue risks to the safe and reliable provision of electricity to Canadians.

USEFUL RESOURCES

- An Introduction to the Cyber Threat Environment
- 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: DESCRIPTION OF SOPHISTICATION

Level of Sophistication	Sophistication Characteristics	Cyber Threat Actors Observed
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

ENDNOTES

[1] "U.S.-Canada Power System Outage Task Force: Final Report on Implementation of Recommendations." Natural Resources Canada and the US Department of Energy. September 2006. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport(2).pdf

[2] Anderson, G. B., & Bell, M. L. "Lights out: impact of the August 2003 power outage on mortality in New York, NY." *Epidemiology* 23(2), 189–193. 2012. https://doi.org/10.1097/EDE.0b013e318245c61c

[3] "Canada's Critical Infrastructure." Public Safety Canada. 19 May 2020. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

[4] 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.

[5] Strong, W. "NTPC confirms 'cyber attack' from unknown source on Thursday, RCMP investigating." CBC News. Apr 30, 2020. https://www.cbc.ca/news/canada/north/ntpc-apparent-ransomware-attack-1.5551603

[6] Targett, E. "Internal Data Stolen, Leaked, in REvil Attack on Electricity Market's Elexon." *Computer Business Review*. 1 June 2020. https://www.cbronline.com/news/elexon-hack-ransomware-revil

[7] "Honda and Enel impacted by cyber attack suspected to be ransomware." Malwarebytes Blog. 9 June 2020. https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/

[8] "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.

[9] "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.

[10] 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.

[11] "EKANS Ransomware and ICS Operations." Dragos Inc. 3 February 2020. https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[12] Cherry, P. "'Pilot to the stars' nearly crippled entire Hydro-Québec network." *Montreal Gazette*. October 29, 2018. https://montrealgazette.com/news/local-news/pilot-to-the-stars-nearly-crippled-entire-hydro-quebec-network

[13] 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.

[14] "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.

[15] "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

[16] Greenberg, A. "Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount." *Wired*. 20 June 2019; Greenberg, A. "A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems." *Wired*. 20 November 2019. https://www.wired.com/story/iran-hackers-us-phishing-tensions/

[17] Raggi M. D. Schwarz, and G. Mladenov, "TA410: The Group Behind LookBack Attacks Against U.S. Utilities Sector Returns with New Malware" Proofpoint Blog. June 08, 2020. https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new.

[18] Greenberg, A. "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid." *Wired*. 14 June 2019. https://www.wired.com/story/triton-hackers-scan-us-power-grid/

[19] "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.

[20] Nelson, N. "The Impact of Dragonfly Malware on Industrial Control Systems" SANS Institute. 18 January 2016. https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672

[21] "Iranian hackers infiltrated U.S. power grid, dam computers, reports say." CBC News. 22 December 2015. https://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342.

[22] 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/

[23] Gallagher, S. "Indian nuclear power plant's network was hacked, officials confirm." *Ars Technica*. October 30, 2019. https://arstechnica.com/information-technology/2019/10/indian-nuclear-power-company-confirms-north-korean-malware-attack/

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

[25] "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas." Dragos Inc. Blog. 14 June 2019. https://www.dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/.

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

[27] Krebs, B. "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent." Krebs on Security Blog. 26 September 2012. https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

[28] "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.

[29] 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/.

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

[31] Nelson, N. "The Impact of Dragonfly Malware on Industrial Control Systems" SANS Institute. January 18, 2016. https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672.

[32] "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.

[33] "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/media/media-2018-12-20.

[34] "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.

[35] "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

[36] Wadhera, A., J. Ayoub, and M. Roy. "Smart Grid in Canada 2018." Natural Resources Canada. April 2019. https://www.nrcan.gc.ca/maps-tools-publications/publications/energy-publications/publications/smart-grid-canada-2018/22579.

[37] Wadhera, A., J. Ayoub, and M. Roy. "Smart Grid in Canada 2018." Natural Resources Canada. April 2019. https://www.nrcan.gc.ca/maps-tools-publications/publications/energy-publications/publications/smart-grid-canada-2018/22579.

[38] Parks, R.C. "Advanced Metering Infrastructure Security Considerations." SAND2007-7327. Sandia National Laboratories. November 2007. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/20-AMI_Security_Considerations.pdf