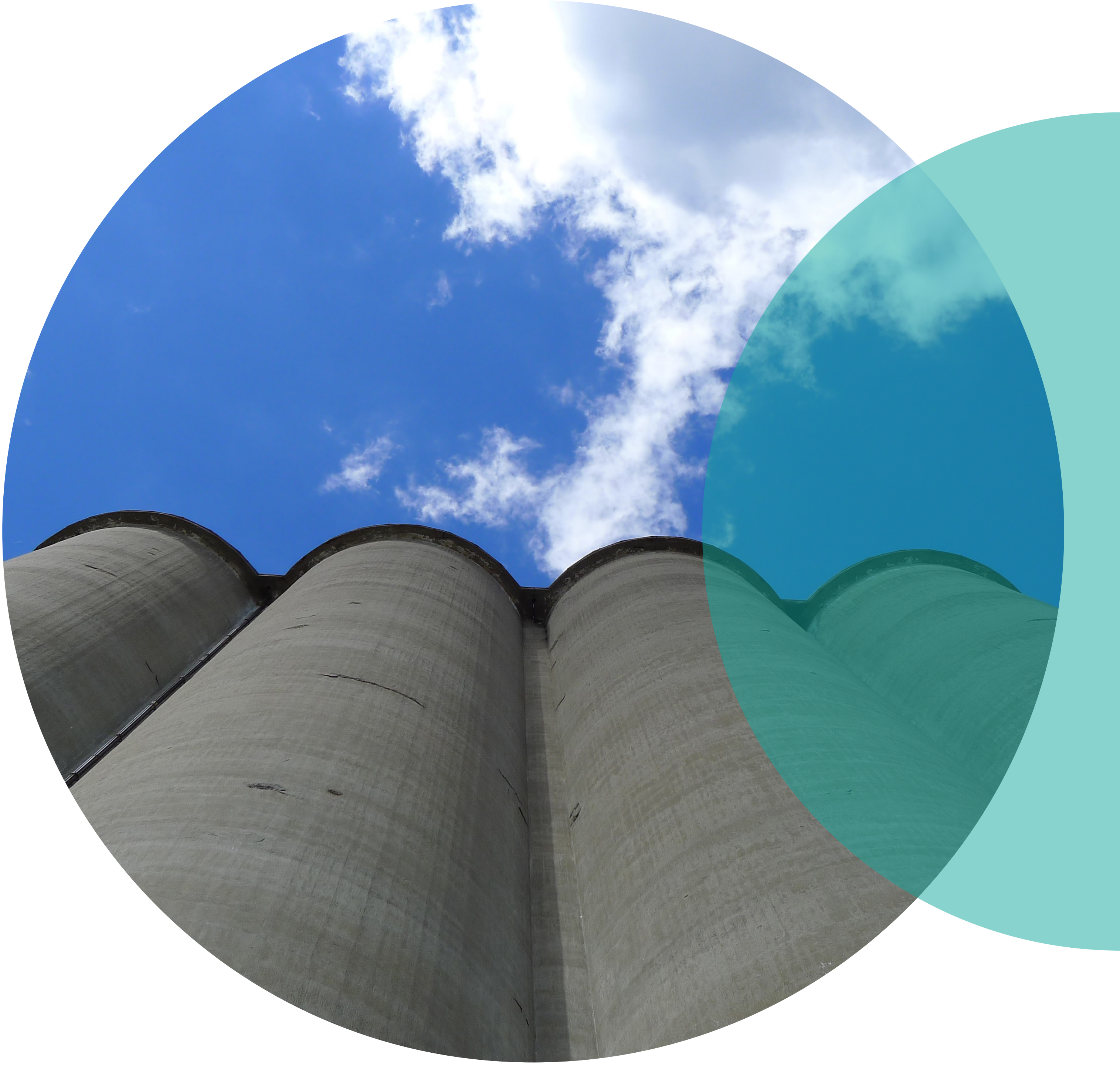
Hybrid CoE Working Paper 18

Defending critical infrastructure: The challenge of securing industrial control systems



Hybrid CoE

Vytautas Butrimas – June 2022

Hybrid CoE Working Papers cover work in progress: they develop and share ideas on Hybrid CoE's ongoing research/workstrand themes or analyze actors, events or concepts that are relevant from the point of view of hybrid threats. They cover a wide range of topics related to the constantly evolving security environment.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

ISBN (web) 978–952–7472–38–5
ISBN (print) 978–952–7472–39–2
ISSN 2670–160X

June 2022

Cover photo: Michael Canzi / Flickr / creativecommons.org/licenses/by-nc/2.0/

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

The responsibility for the views expressed ultimately rests with the authors.

Contents

Acknowledgements

The author would like to thank industry opinion leaders Gary Rathwell, Jacob Brodsky, Robert Radvanovsky, and Joe Weiss for sharing their deep knowledge of and insights into industrial cybersecurity.

Thanks are also due to many people at the International Society of Automation (ISA) and the SCADA and Control Systems Security Group (SCADASEC) for their collaboration, knowledge sharing and support.

Summary

Hybrid warfare and cyber warfare are just some of the forms of aggression demonstrated in human conflicts, which have – in essence – hardly changed in 3,000 years. As we have witnessed in Ukraine in 2022, these new forms of warfare have by no means replaced the traditional forms of war that inflict massive criminal physical violence on civilians and cities. Cyberattacks by advanced and persistent threat actors that now target industrial operations – and most importantly the technologies used to monitor and control physical processes that provide vital services – represent a significant escalation in the level of severity and the scope of modern conflict. Using cyber means to target an industrial operation that is protected by layers of engineering and safety systems requires advanced knowledge of these critical systems. Those that seek to defend these critical assets against such technology-based attacks must realize that the best practices that apply when protecting technology assets used in the home or office are not sufficient for protecting the technologies used to monitor and control a physical process. The defenders of critical infrastructure must have an understanding of these technologies in order to develop effective measures of defence. Only measures based on sound engineering principles and the appropriate design of system architectures will ensure the effective monitoring, control and safety of a physical process.

Introduction

It is sometimes taken for granted in modern societies that light will be available at the flick of a switch, that fresh drinking water will flow when we turn on the tap, that our homes will be heated when we turn the dial, and that the train we catch will take us safely to our destination. It can become a source of great discomfort and anxiety when these services are suddenly denied as in the case of a power outage. Suddenly one realizes that one's well-being is dependent upon a technology that is quite fragile. When it fails, it is like the springing of a trap that we cannot free ourselves from until the denied benefits of the technology are restored. These disrupting events occur frequently but are usually of a relatively short duration, and affect a limited geographical area. Power utilities have specialized crews that are experienced in power restoration work, and that are on call to respond to damaged power cables after a major storm. The additional application over time of new enabling technologies, while making it possible to monitor, control and respond to incidents in today's large cross-border critical infrastructures, has also introduced additional complexity and interdependency that also increases possible points of failure and the potential exposure of society to significant risks to its well-being. The consequences of a cumulative failure in these supporting technologies have been recognized by governments[1] and insurance companies,[2] and even provide plot lines for fiction writers.[3] These vulnerabilities stemming from modern society's dependence on enabling technologies for economic activity, national security and well-being are also being seriously studied by threat actors of various skill levels. These malicious efforts have resulted in successful attempts to exploit weakness through cyberattacks on power grids, petrochemical plants and other industrial operations found in critical infrastructure.

There is, however, an unmet challenge in protecting industrial control systems (ICS) that support critical infrastructure against cyber threats. The difficulty stems from a lack of awareness and understanding about the industrial environments where technology is used not just to protect data but also to monitor and control a physical process governed by the laws of physics and chemistry. Unlike efforts made to secure the data and information-intensive operations that take place in the home or in office environments, the primary focus of the industrial environment is protecting the operation itself. Complicating these protection efforts is the dominance of established cybersecurity best practices for protecting information and communications technologies (henceforth referred to as IT), developed over decades to protect the data and information used in the home and office. For many years, the work conducted in protecting the industrial or manufacturing side has largely functioned in isolation from the development of office IT cybersecurity practices. In 2002, Microsoft's Bill Gates sent a now famous email to Microsoft employees calling for the implementation of secure computing practices for the Windows operating system and other Microsoft software.[4] Much progress has been made in securing the data and

[1] Petermann et al., 'What happens during a blackout: Consequences of a prolonged and wide-ranging power outage'.

[2] Lloyd's, 'Business Blackout'.

[3] Elsberg, *Blackout.*

[4] Wired, 'Bill Gates: Trustworthy Computing'.

information-intensive operations of the home and office since then. However, it was only in the summer of 2021 that the engineering community published its first version of the Top 20 Secure Coding Practices for the Programmable Logic Controller (PLC).[5] PLCs are programmed to perform a specific function such as controlling the operation of a motor or valve at a pumping station running fuel down a pipeline.[6] They are as ubiquitous and as critical a component for the industrial environment as a keyboard, mobile phone and router are in the home and office environments. In recent years, as cyber incidents in the industrial sectors of critical infrastructure have increased, the calls to do something about the cybersecurity of industrial operations found in critical infrastructure have increased, yet the mitigation efforts have sometimes been counterproductive. For example, a well-intentioned attempt to implement a best practice IT cybersecurity policy on a computer found in a nuclear power station tripped the safety systems of the plant, resulting in an emergency shutdown of the reactor.[7]

Cyberattacks have also been used as one of the tools for conducting hybrid warfare and other forms of conflict. In response to the challenge, there have been many attempts by security vendors and governments to propose solutions. However since home office IT cybersecurity practices have become so well established, they continue to influence the work of policymakers when tasked with preparing measures for protecting critical infrastructure. Hence, the proposed mitigation measures to secure industrial environments have not been fully applicable and able to ensure adequate protection from today's threats emanating from cyberspace.

This Hybrid CoE Working Paper will attempt to illuminate the underappreciated role of ICSs in critical infrastructure, and present examples that demonstrate the vulnerabilities of industrial operations to cyber incidents. In addition, ways will be presented to develop more effective policies that will improve the safety, security, availability and resilience of the critical technologies that play a key role in supporting modern economic activity, national security, and the well-being of society.

[5] Admeritia, 'PLC Security Top 20 List'.

[6] AutomationDirect, 'What is a PLC?'.

[7] Kesler, 'The vulnerability of nuclear facilities to cyber attack', 21.

What are industrial control systems?

Critical infrastructure is defined here as an essential service, asset or technology that – if degraded or denied – can have an adverse effect on economic activity, national security or the well-being of society.[8] The energy sector is a key infrastructure where energy is produced, distributed and duly used to support economic activity, national security and the well-being of society. While data and information are important, an even more important role is played by the special technologies used here to monitor and control physical processes found in power distribution grids and petrochemical plants governed by the laws of physics and chemistry. Industrial control systems (ICS) work in the unique domain of industrial or manufacturing operations found closest to the physical process.

There are many competing terms for these systems,[9] but for the purpose of this paper a control system used in an industrial or manufacturing environment will be defined as:

- **Mostly computer-based, used by infrastructures and industries to monitor and control sensitive processes and physical functions;**
- **Systems that collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment;**
- **Hardware and software closest to the actual physical process such as programmable logic controllers (PLCs), remote terminal units (RTUs), actuators, drives, sensors, transmitters and field devices.**[10]

How information technology (IT), operation technology (OT) and industrial control systems (ICS) differ from each other

Control system technology differs from the IT used in an energy company's billing and administrative departments, where the activity is data- or information-centric. It also differs from the operational technology (OT) used in the control room that uses IT to monitor the physical process. The workstations in the control room use control software that processes the acquired information and presents it using a human machine interface (HMI). The software used to collect and present data about the state of a physical process is called supervisory control and data acquisition, or SCADA. The technologies that are closest to the actual physical process, that monitor and control those processes according to pre-set parameters, and that can report this information to the control room are called industrial control systems or ICS.

The devices found in ICS have computer-like qualities, but unlike the general purpose PC found in our offices, these devices are designed to perform a specific task. A PLC is a computer-like device that has a Central Processing Unit (CPU), a memory, and communication ports, and can be programmed to perform specific actions. However, it will not do well as a word processor as it does not have a familiar-looking keyboard. Rather, it is programmed by another computer to monitor some specific physical process and execute an action or actions according to received information about the physical process.

[8] NIST, 'Critical infrastructure'.

[9] For a more detailed discussion of terminologies used to describe control systems, see: Infracritical, 'Debate over IT, OT and Control Systems'.

[10] Brodsky & Radvanovsky, 'Introduction', 3–5.

PLCs are often used in factories and industrial plants to control motors, pumps, lights, fans, circuit breakers and other machinery.[11] A PLC can not only receive data from a monitored device but can send data to another control device, where another action can be initiated automatically or by a human operator in the control room.

Sensors are the starting points for monitoring and sending data about the physical process to the control systems such as a PLC. In a way, they are like the five senses of the human body that note and send information about the state of the environment to the brain, and become part of human understanding about the state of the world, and inform action. In much the same way, a process sensor will note and transmit information about the flow rate and pressure of the fuel being pumped down a fuel pipeline. The control system will note and record this information provided by the sensor and automatically apply pre-programmed corrective action if necessary to maintain the desired state, namely the pipeline pressure or flow rate.

Since control systems are so dependent on sensors, it is of vital importance that the sensor provides accurate information about the part of the physical process it is assigned to monitor and report on. Failures in sensors resulting from technical defects or from attempts to compromise them can lead to disastrous results. For example, the two Boeing 737 Max plane crashes that occurred in October 2018 in Indonesia, and in Ethiopia in March 2019, resulting in the loss of passengers, crew and plane, were caused by a bad flight sensor sending bad data to a flight control system. The flight control system was designed in such a way that the sensor data was so trusted that it had the authority to override the judgment of the pilot.[12]

Since sensors are simple low-technology devices used to monitor and report on a specific parameter (temperature, flow rate, pressure, liquid level, presence of a toxic substance or gas), it is difficult to design security into them. For example, it would be quite expensive to upgrade or replace thousands of sensors on a pipeline with security technologies such as encryption. Upgrading an existing sensor also entails the risk that the capability of that sensor to perform its allocated function may be degraded. In short, there is little cybersecurity at the sensor level. This was one of the conclusions of the International Society of Automation Committee 99 task group,[13] in which the author participated in 2018 and which investigated the cybersecurity of field devices such as sensors, drives and actuators in 2017.[14] According to one of the leaders of this task group:

> "Process sensors have no inherent cyber security and yet have hardware backdoors directly to the Internet. The cyber security gap includes no capability for passwords, single-factor (much less multi-factor) authentication, encryption, keys, signed certificates, etc. Despite the lack of any cyber security, these devices are the 100% trusted input to OT networks and manual operation. Moreover, process sensors have no cyber forensics."[15]

[11] Gates, 'A Beginner's PLC Overview'.

[12] Leggett, 'What went wrong inside Boeing's cockpit?'.

[13] Weiss, 'Sensor security issues are a global issue'.

[14] Weiss, 'The Need to Change the Paradigm of Control Systems Cyber Security'.

[15] Weiss, 'It is not possible to meet Senate cyber disclosure requirements or CISA OT recommendations'.

These three industrial environments – IT, OT and ICS – have different requirements, and hence a one-size-fits-all approach based on IT security best practice will not work. The approach can in fact lead to damage to property, loss of life, and harm to the environment. For example, a commonly applied IT cybersecurity best practice is based on ensuring the confidentiality, integrity, and availability of data and information. Confidentiality (meaning that only an authorized user will be given access) is achieved through the application of a strong password policy that includes long alphanumeric characters and symbols that regularly require changing by the user. In the ICS environment, safety comes first since physical processes in hazardous environments are involved. A strong password policy to manage authorized access to an ICS system may in times of emergency lead to failed authentication due to errors made in keying in the complex password at a time when the operator may be under stress in dealing with an emergency. Confidentiality may be less of a priority, and the risk of a shorter and easier to remember password that is seldom changed may be the password policy of choice of an operator responsible for monitoring and controlling a physical process found in an industrial operation.

The importance of trust amid increasing demand for operational data stemming from employing larger numbers of sensors and ensuring their integrity, while supporting an industrial operation, is of great relevance to Industry 4.0 / the Industrial Internet of Things (IIoT) based proposals for improving industrial enterprise efficiencies and competitiveness. Industry 4.0 refers to the next stage in industrial development following steam power, the assembly line, and digitalization. Called the 4th Industrial Revolution, proponents of Industry 4.0 with some help from enhanced machine-to-machine connectivity and artificial intelligence (AI) envisage the new sources of data supporting:

- **Uniquely identifiable and locatable products at all times;**
- **Some self-autonomy or awareness in the product itself that can even contribute to its own manufacture;**
- **The capability to recognize signs of wear and tear throughout the product life-cycle;**
- **The collection of information in order to optimize logistics, deployment, maintenance, and integration with business management applications.**[16]

Since so much depends upon the accuracy and timely operation of sensors in physical operations of critical infrastructure, the gap in the protection of these electronic intelligent devices is in danger of widening as Industry 4.0, Machine to Machine (M2M), IIoT and AI- driven policies and programmes become more popular and more widely implemented. Examples of important questions raised about giving machines autonomy include how to determine that a change caused by a machine has been authorized, and who will ensure that the change makes good engineering sense.[17]

[16] German Federal Ministry of Education and Research, 'Recommendations for implementing the strategic initiative INDUSTRIE 4.0'.

[17] Langner, 'Brave new industrie 4.0'.

A process control or industrial environment requires a different approach to cybersecurity

There are significant differences in terms of the consequences resulting from failure of the IT processing data and information in the office, and the failure of ICS to monitor and control a physical process found in a power grid or petrochemical facility. An IT failure in the office of an energy company essentially halts the typical daily activities of the office. This could lead to denial of access to billing and accounting data from workstations or databases. Employees in the office call up the IT department and sit idly while they wait for them to bring the network back online, restore workstation PCs from backups, or restore access to the Internet.

In 2012, the world's largest energy company, Saudi Aramco, suffered a massive cyberattack (effectively a denial-of-computer attack, or what this author refers to as a DOC), resulting in the total loss of the data on the hard drives of 30,000 computers and servers due to a wiper virus planted in their systems by a cyberattacker. While the ICS technologies used in the oil field, pipeline and refinery operations were unaffected, the attack nevertheless halted the administrative operations of the company. Tankers waited offshore to receive fuel because the digitally stored billing and accounting information on the damaged computers in the offices was unavailable. In this and in similar cyberattacks, the recovery of business operations was possible through the purchase of new hard drives and the reinstallation of the data from backups. No physical harm to people, property or the environment occurred as a result of IT failure in the office.[18]

A failure in a control system where safety, not the protection of data, is the chief concern can harm people, and damage expensive industrial equipment, property and the environment. The explosion of the Deep Water Horizon oil drilling platform in the Gulf of Mexico and the subsequent loss of human life and property, and harm to the environment in April 2010 could have been avoided if the safety systems had not failed.[19] This was an accident, but intentional and successful attempts to disrupt control systems have also occurred. Below are some examples.

Stuxnet

In the summer of 2010, cybersecurity practitioners became aware of a disturbing change in cyberattacks: the targeting of control systems used to monitor and control a physical process. The appearance of Stuxnet was a watershed moment in cybersecurity that in many ways significantly impacts our efforts to protect industrial operations today. Up until then, cyberattacks were chiefly thought to be focused on IT systems using Microsoft Windows or Linux operating systems and software-based applications used in the home and office. Conducted over several years, the Stuxnet cyberattacks that targeted the ICS of a nuclear enrichment facility marked a turning point in cyberspace and for international security policy as they were believed by many to have been committed by a state.[20] Here, one saw for the first time an operation using a state designed and delivered digital weapon which, in addition to attacking the MS Windows operating system and software, also changed process control data, disabled

[18] Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back'.
[19] Mullins, 'The eight failures that caused the Gulf oil spill'.
[20] Butrimas, 'National Security and International Policy Challenges in a Post Stuxnet World'.

safety systems, and succeeded in seizing control and oversight of a physical process (centrifuges used for nuclear enrichment) from the operator in the control room.[21] The Stuxnet affair has become a classic industrial cybersecurity case, and the methods used have been copied and improved upon in subsequent cyberattacks on critical infrastructure.

Cyberattack on a steel mill that resulted in physical damage

In 2014 the Federal IT Department of Germany noted a successful cyberattack on a steel mill in its annual report on cyber incidents. The cyberattack caused the uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage.[22] These attacks, while making use of malware to penetrate IT systems in the office, went one step further and were able to cross into the industrial control environment and seize control of a physical process from the operator, as had happened during the Stuxnet attack years earlier.

[21] Langner, 'To kill a centrifuge'.

[22] Federal Office for Information Security, 'The State of IT Security in Germany 2014', 31.

Applications of cyberattack techniques in a hybrid war

Techniques such as those used in the Stuxnet attack can also be used in the context of hybrid war, where conventional combat methods do not play a primary role. Instead, an expanded set of hard-to-attribute but nevertheless coercive tools of political, economic and psychological pressure are chosen by the aggressor,[23] including the employment of cyber means to bring about a kinetic effect in the victim's critical infrastructure, such as a blackout, or to cause some other denial or degradation of a critical service vital to the well-being of society. This section looks at some applications.

Cyberattacks against critical infrastructure sectors in Ukraine 2015–2017

The cyberattacks on Ukraine's power grid in December 2015 and 2016 occurred in the context of the political-military conflict over Russia's illegal annexation of Crimea in 2014. This conflict, which featured a variety of attacks, ranging from destructive physical attacks by military forces to information warfare, psychological operations, economic disruptions and cyberattacks has been described as "hybrid warfare".[24]

On 23 December 2015, the operators of a regional power grid in Ukraine watched as the cursor on their control screens started moving and within minutes opened breakers at 30 substations, plunging a quarter of a million people into a blackout. The attackers also sought to inhibit the operators' ability to respond to and recover from this attack by installing a compromised code that damaged the communication devices used by the SCADA to monitor and control the affected substations. Simultaneously, a denial-of-service attack (DOS) targeted the utility's telephone system, which made it hard not only for customers to inform their service provider that they were without power, but also inhibited the operators' understanding of the extent of the blackout.[25] The attack ended with the application of wiper "killdisk" malware, which wiped the data on the control systems.[26]

An even more sinister cyberattack, with the potential for long-term damage to expensive equipment used in the power grid, occurred a year later when part of Kyiv lost electrical power. The subsequent investigation again revealed the same long-term stealth techniques of undetected intrusion and reconnaissance but, most significantly, found that the preventative relays had additionally been targeted.[27] Preventative relays act as safety systems for power grids and perform the function of disconnecting bulk power equipment when there is an imbalance in the power transmission and distribution system, as can occur during a power disruption or blackout.[28] One possible motive for disabling a protective relay could be to make power restoration efforts more dangerous and expensive.[29] A compromised relay could complicate and make restoring power more

[23] Butrimas et al., 'Hybrid warfare against Critical Energy Infrastructure: The Case of Ukraine', 2.
[24] Ibid.
[25] Butrimas, 'Guide for protecting industrial automation against cyber incidents in critical energy infrastructure', 6.
[26] CISA, 'Cyber-Attack Against Ukrainian Critical Infrastructure'.
[27] Slowik, 'CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack', 5.
[28] Electgo, 'What is a relay, its function, types and relay wiring'.
[29] Butrimas, 'Guide for protecting industrial automation against cyber incidents in critical energy infrastructure', 7.

costly by eliminating the protection devices during power restoration operations.[30]

In the summer of 2017, malware called NotPetya, which some have described as a "weapon of mass disruption",[31] targeted Ukraine's financial infrastructure. NotPetya malware was a ransomware program that attacked accounting software used by the private sector to pay taxes to the Ukrainian government. However, perhaps unintentionally, it caused significant collateral damage as it spread outwards from Ukraine, hitting industrial/manufacturing targets in Africa and Europe. Most notably, the worldwide shipping operations of Maersk came to a standstill. In another sinister twist, while the data destruction and infection spreading part of the code worked, the ransomware section of the code that handled payment (after which the victim could unlock the encrypted files) did not work. This "programming error" by the attacker resulted in there being no means by which the victim could make the ransom payment.[32] For some commentators, this indicated that the perpetrators were not interested in financial gain but rather in spreading the destructive malware as rapidly and as widely as possible.[33] In the context of the hybrid war in Ukraine, this attack had an additional economic and perhaps political element. The malware initially attacked the accounting software used not only by Ukrainian business but also by some of the branch offices of international corporations that did business in Ukraine. Hence, the cyberattack could have had an additional damaging effect on the economy of Ukraine by discouraging foreign businesses to invest or do business in the country.

Cyberattacks on critical infrastructure associated with the Russian invasion of Ukraine in 2022

Up to the time of writing, five weeks after the Russian invasion of Ukraine, cyberattacks against Ukraine have mostly disrupted office IT-related operations such as distributed denial-of-service attacks (DDoS) – a denial-of-service technique that uses numerous hosts to perform the attack on another computer or computer network resource[34] – on Ukrainian government institutions, and have thus far refrained from cyber operations directly targeting the control systems of critical energy infrastructure, as was carried out with some success in 2015 and 2016.

In the invasion of Ukraine launched on 24 February, the attacker apparently did not opt for the advantages of stealth and deniability. They did not care whether it was known that they had fired tank shells and missiles at thermal and nuclear power plants. They chose to shoot at the plant, occupy it with boots on the ground, and then shut down the operation by openly using military and other violent means. It could be that these capabilities to disrupt energy sector operations are already in place and are waiting for the order to execute, or are being held in safe keeping for future use in another country that Russia may cause a conflict with.[35] This would be consistent with other sophisticated cyberattacks on critical infrastructure, which

[30] Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event', 5.
[31] Spaniel & Hunter, 'Weapons of Mass Disruption'.
[32] Butrimas, 'Guide for protecting industrial automation against cyber incidents', 8.
[33] Greenberg, 'The Untold Story of NotPetya'.
[34] NIST, 'DDOS'.
[35] Robertson, 'Where Are the Devastating Russian Cyber Attacks?'.

after investigation have shown that the intrusion into and compromise of the targeted systems took place many months before the attack was executed. The knowledge and capability gained from the successful cyber weapon "experiments" conducted using Ukraine's electrical infrastructure from 2015–2017 could be saved for future use during a conflict with other countries that use the same western-made control systems and equipment.

One of these prepared cyber weapons may actually have been used at the start of the Russian military invasion of Ukraine. Reports soon started to circulate about cyberattacks that resulted in satellite communications failures in Europe. Viasat/Eutelsat service providers and customers reported attacks on control systems used to remotely manage and control windfarms, which resulted in physical damage to over 5,800 satellite communication terminals.[36] The conclusions of some analysts point to evidence corroborating that the initial attack was directed at Ukrainian satellite terminals, which then subsequently spread to other Viasat/Eutelsat customers in Europe such as Enercon, a wind farm operator in Germany.[37]

At the same time, and perhaps in response to denial-of-service cyberattacks on government and private institutions, the Ukrainian government called on local business people and cybersecurity experts to help organize a unit of hackers to defend against Russia.[38] In this sense, cyberattacks, albeit directed at office IT systems and websites, are being used as a part of hybrid warfare by both sides in addition to traditional military methods of attacking civilian and military targets. Several private individuals and groups, including the long quiet collective entity called Anonymous, have entered the conflict and engaged in cyberattacks on Russian government institutions in support of Ukraine.[39]

Attempts to compromise safety systems at petrochemical plants

Returning to the summer of 2017, the safety instrumented systems (SIS) made by Schneider Electric caused two unplanned shutdowns of one of the world's largest petrochemical facilities in Saudi Arabia.[40] The first cyberattack, as with many other incidents of this kind, came with no warning or hint that something was wrong. The plant's IT department noticed nothing, no alarms registered on the plant's ICS, and nor did the manufacturer discover anything wrong with the affected safety controllers, which were checked and returned to the customer. Only after the second shutdown, two months later, was it determined,[41] after outside experts performed an industrial cyber-forensic investigation,[42] that a cyberattack had long been underway inside the plant.[43] The attempt to compromise a safety system represents a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are

[36] Henry, 'Europe Cyberattack Results to "Massive" Internet Outage'.
[37] Targett, 'Viasat says KA-SAT outage caused by a "cyber event!"'.
[38] Schectman et al., 'Ukrainian cyber resistance group targets Russian power grid'.
[39] Seibt, 'Ukraine conflict presents a minefield for Anonymous and hacktivists'.
[40] Perlroth & Krauss, 'A Cyberattack in Saudi Arabia Had a Deadly Goal'.
[41] Gutmanis, 'Triton – A Report From The Trenches'.
[42] Ibid.
[43] Blake Sobczak, 'The inside story of the world's most dangerous malware'.

used in an industrial process to protect property and – most importantly – people from serious harm resulting from an industrial process that has exceeded set parameters. These parameters are used to program an automatic response in the safety system to restore a system to a safe state when changes in temperature, flow rates, pressure, frequency, or other system state indicators exceed set levels. These are the systems that respond automatically, for example by opening or closing valves on a pipeline when pressures or flow rates exceed pre-set parameters.[44]

Security service providers and their customers are compromised and hacked through the supply chain

One indication of the evolving complex challenges in defending critical infrastructure against advanced threat actor intrusions is the supply chain cyberattack that spread from SolarWinds, a cybersecurity service provider's website, in December 2020.[45] The initial discovery was made by security service provider FireEye in its announcement about a security breach and the digital theft of its own penetration testing tools.[46] It further discovered a trail of malware that found its way to SolarWinds networking software. Customers who downloaded updates from the vendor's website potentially compromised 18,000 office IT and industrial control system environments that included heating, ventilation and air-conditioning control (HVAC) systems.[47]

Ransomware attack on a fuel pipeline company office causes shutdown of pipeline operations

A good example of the complex and potentially disruptive relationship between the cybersecurity of IT operations in the office and the linked ICS operations monitoring and controlling a physical process is the ransomware attack on the Colonial Pipeline Company in the first week of May 2021.[48] According to early reports, ransomware was planted on the administrative IT side (billing, accounting) of the company, which resulted in loss of the data and other information required to process and operate the business side of the enterprise.[49] It is paramount to note that the control systems on the operations side of the pipeline, which monitor and control the physical processes inside the pipeline, were not directly affected by this ransomware. However, without the billing and accounting information about supply and distribution of the fuel, the operator was forced, out of caution, to shut down the pipeline.[50] In terms of ensuring the safety, reliability and performance of the physical operations of the pipeline, the failure on the IT side should not have forced an emergency shutdown of the pipeline. Industry best practices and standards were available that could have addressed possible flaws in the system architecture that could have led to a better outcome. For example, the International Society of Automation (ISA) ISA 95 standard addresses

[44] Ortega & Butrimas, 'Securing the Industrial Internet of Things', 46.
[45] Muncaster, 'FireEye breach', 8–9.
[46] Ibid.
[47] Weiss & Hunter, 'The SolarWinds Hack Can Directly Affect Control Systems'.
[48] Panettieri, 'Colonial Pipeline Cyber Attack'.
[49] Bertrand et al., 'Colonial Pipeline did pay ransom to hackers'.
[50] Osborne, 'Colonial Pipeline attack: Everything you need to know'.

enterprise integration including transfer of information between plant instrumentation and corporate information systems.[51] If applied in the system design phase, this could have reduced the problems encountered by the company and public during the incident. The ISA/IEC 62443 Standard for Industrial Automation and Control Systems[52] could also have supported the development of the Corporate Cybersecurity Programme, which could have addressed cybersecurity measures at the global level.

[51] International Society of Automation, 'ISA95, Enterprise-Control System Integration'.

[52] International Society of Automation, 'Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems'.

Are the mitigation measures to protect control systems working?

The effectiveness of policies, regulations and mitigation measures implemented in response to the growing number of cyber incidents and cyberattacks on critical infrastructure has been burdened by a lack of understanding about the engineering and control systems required to monitor and control a physical process where safety, not the protection of data, is the chief priority. This has resulted in the poorly thought-out application of IT cybersecurity-centric polices that work well for data-centric office and home environments, but fall short of addressing the safety and security of process-centric industrial environments. In August 2021, the main US Government agency responsible for critical infrastructure protection, the Cybersecurity and Infrastructure Security Agency (CISA), announced the creation of the Joint Cyber Defense Collaborative (JCDC). The main activity of the JCDC will be to "design and implement comprehensive, whole-of-nation cyber defense plans to address risks and facilitate coordinated action", as well as "defending our country's national critical functions from cyber intrusions".[53] There are no representatives from either operators or manufacturers of technologies used to monitor and control a physical process on the list of participating private sector institutions. Instead, we see IT security, networking and communications companies on the list of partners, namely Amazon Web Services, AT&T, CrowdStrike, FireEye Mandiant, Google Cloud, Lumen, Microsoft, Palo Alto Networks, and Verizon.[54]

In February 2022, the CISA issued a document titled "Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure". The recommendations provided in these guidelines ostensibly addressing critical infrastructure focus on measures to safeguard the confidentiality, integrity and availability of information, namely against misinformation, disinformation, and malinformation (MDM).[55] However, these information-centric measures are not appropriate for ensuring the safety, availability and resilience of the technologies used to monitor and control physical operations found in critical infrastructure. It seems that the authors did not rely to any great extent on engineering expertise, as the accents on protecting the physical process are missing in favour of protecting the data or information.

In spring 2022, another US Government agency tasked with developing policies for protecting critical infrastructure, the Transportation Security Administration (TSA), issued cybersecurity regulations to oil and gas pipeline operators. Operators have been quite surprised at the proposals, and fear that while they apply well to personal computers, they are not appropriate for pipeline control systems, "while other rules could require months or even years of painstaking upgrades that could interrupt pipeline operations".[56]

This lack of understanding by policymakers about the atypical cybersecurity requirements of control systems and industrial operations is not limited to North America. One example is the proposed "Network Code for cybersecurity aspects of cross-border electricity flows" being drafted and issued for comment by the European Network of Transmission System

[53] CISA, 'CISA launches new joint cyber defense collaborative'.
[54] Ibid.
[55] CISA, 'Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure'.
[56] Geller, "'TSA has screwed this up": Pipeline cyber rules hitting major hurdles'.

Operators for Electricity (ENTSO-E).[57] The information bias is evident throughout the document and generally overlooks addressing cyber threats to control systems. For example, cyber threats are defined as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact *network and information systems*, the users of such systems and other persons".[58] There is very little relevant language in this draft document that describes what is needed to protect control and safety systems. The information-centric nature of the document, which is aimed at improving the security of electric power grids, is demonstrated by performing a simple word count. The word "information" is used 192 times, "network" and "networks" are used 40 times, while terms that describe physical processes found in the electricity sector, such as "operational technology" or "OT", appear just twice and even then in the context of "computers and data networks".[59]

Another example of an EU document that exhibits the disconnect between IT and Control System cybersecurity approaches for protecting critical infrastructure is the European Union's Directive of July 2016 concerning measures for a high common level of security for network and information systems across the Union, the so-called NIS Directive.[60] The predominant language is in terms of "security and network information systems", a phrase that appears 65 times in the document. While seeming to address operators of essential services that are listed in Annex II, the document does not go far enough in clearly addressing their protection if such office IT data-centric language is used.[61] The predominant provisions for security and network information systems do not fully address the physical process concerns of safety, reliability and resilience that are important to the operators of power grids, fuel pipelines and petrochemical plants, as well as other critical infrastructure sectors.

In an environment where we are witnessing targeted attacks on the technologies that are used to monitor and control physical processes found in critical infrastructure, these well-meaning but flawed efforts by policymakers to mitigate these dynamic threats are unlikely to place any major impediments on the adversary's ability to craft cyberattacks against critical infrastructure as the few examples mentioned in this paper have attempted to demonstrate.

[57] ENTSO-E , 'Network Code on Cybersecurity aspects of cross-border electricity flows'.
[58] Ibid, 7.
[59] Ibid, 9.
[60] 'EU Network and Information Security directive'.
[61] Ibid.

Conclusions and recommendations

The above discussion leads to the following conclusions:

- **Technologies that ensure the safety, reliability and efficiency of industrial operations are being targeted by highly persistent and skilled threat actors (the physical process is being targeted, not just the data).**
- **As a result of a lack of understanding by IT-centric policymakers, cybersecurity approaches based on protecting data and information fall short of protecting critical energy and other infrastructures.**
- **In spite of best efforts to implement cybersecurity best practices, victims continue to be surprised when a breach occurs.**

The control systems that support critical infrastructure operations can be defended against advanced and persistent threats emanating from cyberspace. Developing an effective defence requires a conscientious effort to answer three security policymaking questions.

1. "What must we protect?" It would be a mistake for an operator of critical infrastructure such as a power grid to think that it would suffice to just protect the data or information found in its IT systems and networks. This choice may handicap measures to protect the technologies used to monitor and control the physical process, which are less concerned with protecting data and need to be focused on safety, integrity and reliability instead.
2. "What are the likely threats?" This is the second question that needs to be answered after the assets are chosen. If the operator decides that the threats largely originate from socially motivated hacktivists disrupting websites with denial-of-service attacks, such as Anonymous, or cyber criminals attempting to extort the company with ransomware, then the protective measures may be inadequate to defend against the more advanced persistent threat (APT) actors who do not seek financial gain, but rather to disrupt or destroy technologies used to control a physical process. Incorrect answers to the first two questions will result in a severely flawed answer to the last security question.
3. "How will identified assets be protected from identified threats in the most cost- effective way?"[62] The key lesson to be learned from this process of answering the three security questions is best illustrated by the children's tale of the "Three Little Pigs". In the story, each pig went through this question and analysis process, but only one of them performed it correctly. It was the third pig who, in addition to considering the threats of the "wind" and the "rain" arrived at by his other two neighbours, who respectively built homes out of "straw" and "wood", took special account of the additional possibility of an attack from the "wolf". In the end, his house made of brick saved him and his two homeless neighbours.

[62] Butrimas, 'Towards a cyber-safe critical infrastructure: answering the 3 questions'.

There are methodologies that organize the process of answering the three security questions just described. One of them is **for the operator of critical infrastructure to develop and implement a Corporate Cybersecurity Programme (CCP).** This programme takes into account the security priorities of both the IT side of the enterprise and those of the industrial or physical process monitoring and control side. One guide that introduces and provides advice on how to develop a CCP has been published by Gary Rathwell from the International Society of Automation.[63] **Ensuring that the process will be successful requires the full participation of the plant control and safety engineers, who know how the physical process works.** Their participation is the missing ingredient in developing an effective CCP.

These CCP and other mitigation measures are still not enough if we wish to protect the control systems used in critical infrastructure. Many of the most dangerous cyberattacks on critical infrastructure presented in this paper are understood to have been perpetrated by states and those they sponsor.[64] These attacks are highly resourced, drawing upon the skillsets and intelligence that only a state can summon. Even with best practices implemented, the isolated operator of critical infrastructure cannot be expected to defend their critical assets when they are targeted by a state. For this reason, confidence and security-building measures for managing state behaviour in cyberspace have been proposed by security policy organizations such as the UN and the OSCE.[65] **A necessary proposal is for states to agree, at least in peacetime, to refrain from directing malicious cyber activities at the critical infrastructure of other states.** To ensure some soft enforcement, the agreement should also include **the creation of an organization of willing experts and institutions to monitor and report on violations.**[66] In international relations there are examples where similar action in the form of an agreement with some enforcement mechanism was taken by the international community to address a commonly recognized threat. The Convention Prohibiting the Use of Chemical Weapons and the creation of an organization to monitor and report on violations of an agreement signed by nations representing 97% of the world's population is a worthy model that can be applied for promoting responsible behaviour in cyberspace.[67]

Last of all is to **challenge your assumptions about your capabilities to defend your control system technologies by putting your capabilities to the test.** This provides a good opportunity to spot weaknesses and fortify your systems for the day when the real event happens. One example is the US Government's Plum Island exercise, where an authentic power grid was set up, subjected to a complete blackout, and then

[63] International Society of Automation, 'New White Paper: Implementing an Industrial Cybersecurity Program for Your Enterprise'.

[64] CISA, 'Alert (AA22–083A) Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector'.

[65] Meyer, 'Confidence-Building Measures in Cyberspace', 291–293.

[66] Butrimas, 'Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: Living dangerously', 129–130.

[67] Organization for the Prohibition of Chemical Weapons, 'Chemical Weapons Convention'.

efforts to restore service were evaluated. It was of course possible to restore power, but what they found was that it was almost impossible to re-energize the system if someone was attacking and thwarting their efforts from cyberspace.[68]

[68] Marks, 'Pentagon Researchers Test "Worst Case Scenario" Attack on U.S. Power Grid'.

Author

Mr Vytautas Butrimas works as the Research and Lessons Learned Division's Subject Matter Expert at the NATO Energy Security Centre of Excellence (NATO ENSEC COE) in Vilnius, Lithuania.

Bibliography

[Unless otherwise indicated, all links were last accessed on 12 May 2022.]

Admeritia. 'PLC Security Top 20 List'. https://www.plc-security.com/index.html.

AutomationDirect. 'What is a PLC?'. https://library.automationdirect.com/what-is-a-plc/.

Bertrand, Natasha, Evan Perez, Zachary Cohen, Geneva Sands and Josh Campbell. 'Colonial Pipeline did pay ransom to hackers, sources now say'. CNN, 13 May, 2021. https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html.

Brodsky, Jacob and Robert Radvanovsky. 'Introduction'. In *Handbook of SCADA/Control Systems Security 2nd Edition*, ed. Jacob Brodsky, Robert Radvanovsky. Boca Raton: CRC Press Taylor & Francis Group, 2016, 3–5.

Butrimas, Vytautas. 'National Security and International Policy Challenges in a Post Stuxnet World'. *Lithuanian Annual Strategic Review*, Volume 12, Issue 1, (2014): 11–16.

Butrimas, Vytautas, Jaroslav Hajek, Sukhodolia Oleksandr, Bobro Dmytro and Sergii Karasov. 'Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine'. NATO ENSEC COE (Energy Highlights, 2011), 2. https://enseccoe.org/data/public/uploads/2021/03/nato-ensec-coe-hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf.

Butrimas, Vytautas. 'Guide for protecting industrial automation against cyber incidents in critical energy infrastructure'. Guide (NATO ENSEC COE, 25 January 2022), 6–8. https://enseccoe.org/data/public/uploads/2022/01/d1_guide-for-protecting-industrial-automation-and-control-systems-against-cyber-incidents.pdf.

Butrimas, Vytautas. 'Towards a cyber-safe critical infrastructure: answering the 3 questions'. Scadasec, 21 February, 2018. https://scadamag.infracritical.com/index.php/2018/02/21/towards-cyber-safe-critical-infrastructure-answering-3-questions/.

Butrimas, Vytautas. 'Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: Living dangerously'. In *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen. London: Routledge, 2020, 129–130.

CISA. 'Alert (AA22–083A) Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector'. 24 March, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22–083a.

CISA. 'CISA launches new joint cyber defense collaborative'. 5 August, 2021. https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative.

CISA. 'Cyber-Attack Against Ukrainian Critical Infrastructure'. ICS Alert (IR-ALERT-H-16–056–01). 25 February, 2016. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16–056–01.

CISA. 'Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure'. CISA Insights. February 2022. https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf.

Electgo. 'What is a relay, its function, types and relay wiring'. 17 October, 2019. https://www.electgo.com/what-is-a-relay/.

Elsberg, Marc. *Blackout.* Sourcebooks Landmark, 2017.

ENTSO-E. 'Network Code on Cybersecurity aspects of cross-border electricity flows'. 28 October, 2021. https://consultations.entsoe.eu/system-operations/network-code-on-cybersecurity/supporting_documents/211110_NCCS_Legal%20Text_For_Public_Consultation.pdf.

Federal Ministry of Education and Research (Germany). 'Recommendations for implementing the strategic initiative INDUSTRIE 4.0'. Final Report, 2013, 21.

Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI). 'The State of IT Security in Germany 2014'. Report, November 2014, 31. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3.

Gates, Stephen. 'A Beginner's PLC Overview, Part 1 of 4: Introduction to PLCs'. Automation.Com. 28 November, 2017. https://www.automation.com/en-us/articles/2017/a-beginners-plc-overview-part-1-of-4-introduction#:~:text=Programmable%20Logic%20Controllers%20(PLCs)%20are,-circuit%20breakers%20and%20other%20machinery.

Geller, Eric. "'TSA has screwed this up": Pipeline cyber rules hitting major hurdles'. *Politico*. 17 March, 2022. https://www.msn.com/en-us/news/us/tsa-has-screwed-this-up-pipeline-cyber-rules-hitting-major-hurdles/ar-AAVc7gL?fr=operanews.

Greenberg, Andy. 'The Untold Story of NotPetya, the most Devastating Cyber Attack in History'. *Wired*. 22 August, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Gutmanis, Julian. 'Triton – A Report From The Trenches'. Filmed January 2019 at S4 Events, Miami, FL, video, https://youtu.be/XwSJ8hloGvY.

Henry, Joseph. 'Europe Cyberattack Results to "Massive" Internet Outage', *Tech Times*. 5 March, 2022. https://wwwtechtimescom.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5–800-wind-turbines.htm.

Infracritical. 'Debate over IT, OT and Control Systems'. 22 November, 2019. http://icsmodel.infracritical.com/.

International Society of Automation. 'ISA95, Enterprise-Control System Integration'. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95.

International Society of Automation. 'New White Paper: Implementing an Industrial Cybersecurity Program for Your Enterprise'. 11 January, 2022. https://www.isa.org/news-press-releases/2022/january/new-white-paper-implementing-an-industrial-cyberse .

International Society of Automation. 'Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems'. June 2020. https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf.

Kesler, Brent. 'The vulnerability of nuclear facilities to cyber attack'. *Strategic Insights*, Volume 10, Issue 1 (Spring 2011): 21. http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.

Langner, Ralph. 'To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve'. The Langner Group. November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Langner, Ralph. 'Brave new industrie 4.0'. S4XEUROPE, Digital Bond, Video. June 2016. 19:51, https://www.youtube.com/watch?v=ZrZKiy2KPCM.

Leggett, Theo. 'What went wrong inside Boeing's cockpit?'. BBC News. Updated 27 January 2020. https://www.bbc.co.uk/news/extra/IFtb42kkNv/boeing-two-deadly-crashes.

Lloyd's. 'Business Blackout: The insurance implications of a cyber-attack on the US power grid'. Emerging Risk Report, 2015. https://assets.lloyds.com/assets/pdf-business-blackout-business-blackout20150708/1/pdf-business-blackout-business-blackout20150708.pdf.

Marks, Joseph. 'Pentagon Researchers Test "Worst Case Scenario" Attack on U.S. Power Grid'. Nextgov. 13 November, 2018. https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/.

Meyer, Paul. 'Confidence-Building Measures in Cyberspace'. In *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen. London: Routledge, 2020, 291–293.

Mullins, Justin. 'The eight failures that caused the Gulf oil spill'. *New Scientist*. 8 September 2010. https://www.newscientist.com/article/dn19425-the-eight-failures-that-caused-the-gulf-oil-spill/#ixzz7Ooult4a8.

Muncaster, Phil. 'FireEye breach: a tipping point in nation state attacks'. *Infosecurity*, Vol 18, (2021): 8–9. https://www.infosecurity-magazine.com/magazine-features/fireeye-breach-tipping-point/.

NIST. 'Critical infrastructure', Glossary. https://csrc.nist.gov/glossary/term/critical_infrastructure.
NIST. 'DDOS', Glossary. https://csrc.nist.gov/glossary/term/ddos.

Official Journal of the European Union. 'EU Network and Information Security directive', Annex II. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&-from=EN#d1e32–27–1.

Organization for the Prohibition of Chemical Weapons. 'Chemical Weapons Convention'. https://www.opcw.org/chemical-weapons-convention.

Ortega, Óscar Recacha and Vytautas Butrimas. 'Securing the Industrial Internet of Things: Policy Considerations for reducing cyber risks to industrial control and safety systems'. Operational Highlights, no. 13. NATO ENSEC COE, 2020, 46. https://www.enseccoe.org/data/public/uploads/2020/03/nato-ensec-coe-operational-highlights-no13.pdf.

Osborne, Charlie. 'Colonial Pipeline attack: Everything you need to know'. ZDNET. 13 May, 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/.

Panettieri, Joe. 'Colonial Pipeline Cyber Attack'. MSSPAlert. June 7, 2021, https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/.

Perlroth, Nicole. 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back'. *New York Times*. 23 October, 2012. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Perlroth, Nicole and Clifford Krauss. 'A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try'. *The New York Times*. 15 March, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

Petermann, Thomas, Harald Bradke, Arne Lüllmann, Maik Poetzsch and Ulrich Riehm. 'What happens during a blackout'. Final report. Office of technology assessment of the German Bundestag, 2011. https://publikationen.bibliothek.kit.edu/1000103292.

Robertson, Tom. 'Where Are the Devastating Russian Cyber Attacks?'. *The National Interest*. 28 February 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/where-are-devastating-russian-cyber.

Schectman, Joel, Christopher Bing and James Pearson. 'Ukrainian cyber resistance group targets Russian power grid, railways'. Itnews. 2 March, 2022. https://www.itnews.com.au/news/ukrainian-cyber-resistance-group-targets-russian-power-grid-railways-576775?utm_source=desktop&utm_medium=email&utm_campaign=share.

Seibt, Sébastian. 'Ukraine conflict presents a minefield for Anonymous and hacktivists'. *France24*. 23 March, 2022. https://www.france24.com/en/europe/20220323-ukraine-conflict-presents-a-minefield-for-anonymous-and-hacktivists.

Slowik, Joe. 'CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack'. Dragos Inc. 15August, 2019, 5. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Sobczak, Blake. 'The inside story of the world's most dangerous malware'. *E&E News*. 7 March, 2019. https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/.

Spaniel, Drew & Joyce Hunter. 'Weapons of Mass Disruption'. Whitepaper, Institute for Critical Infrastructure Technology. 28 July 2020. https://icitech.org/weapons-of-mass-disruption-an-assessment-of-the-threat-disruptionware-poses-to-energy-sector-continuity/.

Targett, Ed. 'Viasat says KA-SAT outage caused by a "cyber event"'. *The Stack*. 28 February, 2022. https://thestack.technology/viasat-ka-sat-outage-cyber/.

Weiss, Joe. 'The Need to Change the Paradigm of Control Systems Cyber Security'. 1st Global Cybersecurity Observatory. https://cyberstartupobservatory.com/the-need-to-change-the-paradigm-of-control-system-cyber-security-part-3-new-sensor-technology/.

Weiss, Joe. 'It is not possible to meet Senate cyber disclosure requirements or CISA OT recommendations'. Control. 8 March, 2022. https://www.controlglobal.com/blogs/unfettered/it-is-not-possible-to-meet-senate-cyber-disclosure-requirements-or-cisa-ot-recommendations/.

Weiss, Joe. 'Sensor security issues are a global issue – yet they are not being addressed and people are dying'. Control. 7 November, 2018. https://www.controlglobal.com/blogs/unfettered/sensor-security-issues-are-a-global-issue-yet-they-are-not-being-addressed-and-people-are-dying/.

Weiss, Joe & Bob Hunter. 'The SolarWinds Hack Can Directly Affect Control Systems'.
Lawfare.
22 January, 2021. https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems.

Wired. 'Bill Gates: Trustworthy Computing'. 17 January, 2002. https://www.wired.com/2002/01/bill-gates-trustworthy-computing/.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats