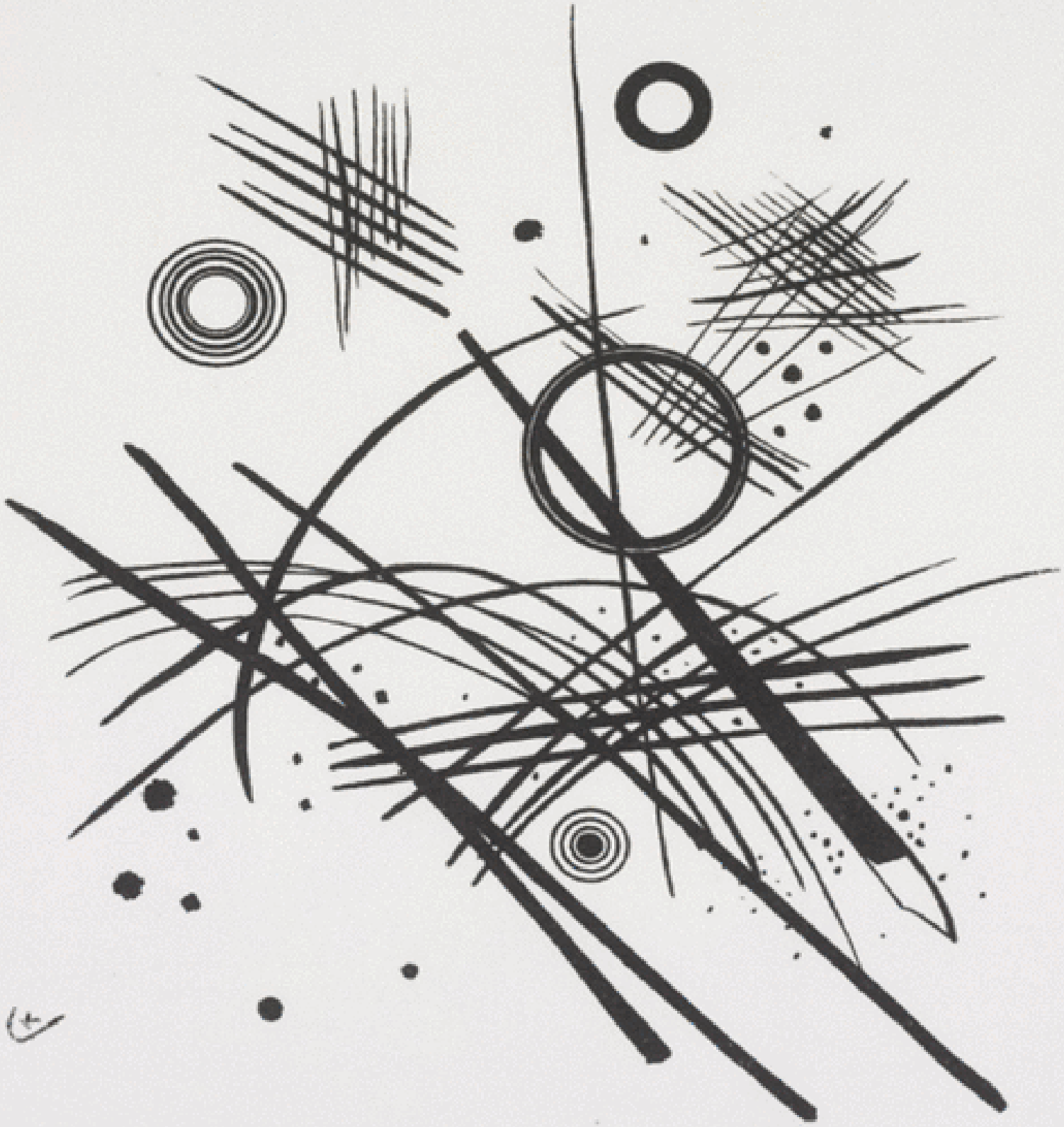
CYBER PEARL HARBOR!

The looming threat of cyber-attacks on Industrial Control Systems

BY: Daniel Simonds



Global TechnoPolitics Forum

CYBER PEARL HARBOR

The looming threat of cyber-attacks on Industrial Control Systems

Daniel Simonds

www.TechnoPoltics.org

June 2021

GLOBAL TECHNOPOLITICS FORUM

The conclusions and recommendations of any Global TechnoPolitics Forum publication are solely those of its authors and do not reflect the views of the Forum, its management, board of advisors, donors, or scholars.

This report is written and published in accordance with the Global TechnoPolitics Forum Policy on Intellectual Independence.

The Global TechnoPolitics Forum is a (501C) (3) nonprofit educational organization with a mission to **shape the public debate and facilitate global coordination at the intersection of technology and geopolitics.** It achieves this mission through: convenings, research, and community building.

Acknowledgements:

Cover art credit: "Wassily Kandinsky - Black Lines (1924) "

Please direct inquiries to: Global TechnoPolitics Forum: info@technopolitics.org

TABLE OF CONTENT

FOREWORD

"Cyber Pearl Harbor" is dramatic language because, after all, each time the United States or another country is attacked, that alerts them to where they are vulnerable. In this paper, Daniel Simonds focuses on cyber-attacks on critical infrastructure operational technology (OT), specifically Industrial Control Systems (ICSs). He outlines what ICS attacks are. Because they can cause physical damage -- like the 2010 Stuxnet attack on Iran, which destroyed centrifuges -- not only do they merit a vigorous response, they can constitute an act of war. The threat in the virtual world could lead to war in the physical world, and for that reason the threat of ICS attacks deserves not just serious attention from policymakers, but steps Simonds outlines to reduce America's vulnerability.

The Global Techno Politics Forum is an innovative new organization that strives to shape the public debate and facilitate global coordination at the intersection of technology and geopolitics. The Forum is independent and nonpartisan, and the analyses and suggestions in this paper are the authors' alone. Yet, the Forum's work is very much that of the team, and we salute the entire team for this effort.

Gregory Treverton ***Pari Esfandiari*** ***Maura Godinez***

Chairman ***President*** ***Senior Director of Programs & Studies***

ACRONYMS AND TERMINOLOGY

cybersecurity professional / information security professional (there can be crossover in an IT department between those who do broad IT security and management and those who do strictly cybersecurity): a professional who protects computer systems and networks that store confidential data, sensitive data and information from misuse, unauthorized access and destruction.

malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a system.

cyber-attack: any attempt to expose, alter, disable, destroy, steal or gain information by attaining unauthorized access through the use of cyber means.

Industrial Control Systems (ICS): a collective term used to describe different types of control systems (software, hardware and instrumentation) used to control and operate industrial processes.

logic bomb: malicious code that executes predetermined actions when certain conditions are met (subset of malware).

remotely accessed malware: malware that allows for unauthorized remote access to a victim's device.

network: a group of devices connected wirelessly or by cables for the purpose of communicating with each other.

operational technology (OT): hardware or software that monitors or controls industrial processes.

information technology (IT): the use of systems to manage data and information.

State(s): a politically organized nation or country.

systems: hardware, software or a combination of both that in a structure communicate with each other.

virus: malicious code that can copy itself spreading from device to device (subset of malware).

Payload: The malware used in a cyber-attack that executes the intended malicious effect of the attack.

Keystroke: the depression of a key on a keyboard.

Attribution: the process of tracking down, identifying and placing blame on the perpetrator of a cyber-attack or other malicious cyber activity.

Advanced Persistent Threat (APT): a threat actor (generally a State actor or State sponsored actor) who attains and maintains unauthorized access for extended periods of time.

antivirus software: software that has been designed to detect and destroy computer viruses.

firewall: a type of network security that monitors, controls and can prevent incoming and outgoing network traffic based upon certain network security rules.

internet: a global network consisting of many interconnected networks with different levels of providers who connect the networks at varying distances.

intranet: a local or restricted network that does not access or communicate with other networks.

air-gapped: a computer or device that has no connection to the internet.

The Tallinn Manual: a non-binding application of international law to cyber conflicts and cyber warfare written between 2009 and 2012 by approximately 20 international law and cybersecurity scholars and practitioners known collectively as the Tallinn Group.

IIoT: The industrial internet of things is interconnected industrial sensors, instruments, and other devices networked together with computers' industrial applications and software.

FRAMING THE THREAT

In 2012, then-Secretary of Defense Leon Panetta warned that soon the United States might face the threat of a "cyber Pearl Harbor," without describing what a cyber Pearl Harbor would look like. This paper assumes that a cyber Pearl Harbor would be an adversarial attack whose effects would draw the United States into a war. The only difference would be that the attack would be conducted in cyberspace.

This paper will explore why the effects of a cyber-attack targeting an Industrial Control System (ICS) could justify a forceful response as an act of self-defense legally protected by Article 51 of the UN Charter. This use of responsive force has the potential to escalate a conflict between the victim of the ICS attack and the adversary.

The purpose of this paper is to demonstrate why cyber-attacks on critical infrastructure[1] operational technology (OT), specifically Industrial Control Systems (ICSs), are a serious threat deserving policymakers' immediate attention.

JUSTIFYING FORCEFUL RESPONSES AND EVEN WARS

HOW DOES ICS FIT INTO OT

Operational technology (OT) is different from information technology (IT) because OT controls processes in the physical world, while IT manages data. OT refers explicitly to systems (hardware and software) that manage industrial operations. These operations can include industrial processes such as production lines, mining and dam operations, fuel enrichment monitoring, or electrical grid management. Industrial Control Systems (ICS) lie within the OT sector.

Industrial Control Systems can generally be separated into two categories; a continuous process control system that typically utilizes programmable logic controllers (PLCs) or a discrete process control system (DPC) that could use a PLC or another process control device.

Continuous and discrete process control systems are often managed by Supervisory Control and Data Acquisition (SCADA) systems.[2] SCADA is the software that provides operators and engineers, using a digital graphic interface (computer or user interface screen display), the ability to observe and receive data regarding the status of industrial processes. SCADA also

[1] "Critical Infrastructure Sectors." *Cybersecurity and Infrastructure Security Agency CISA*, October 21, 2020.
[2] Williamson, Graham. "OT, ICS, SCADA – What's the Difference?" KuppingerCole, 2015.

provides the operator access to control functions of industrial processes if adjustments need to be made to the process under control.[3]

SCADA specifically acts as a central component in the ICS because it receives data from and can relay commands to peripheral hardware that directly controls the industrial process. An example of peripheral hardware with which SCADA communicates is a PLC. In an industrial setting, a PLC is hardware that utilizes some software to monitor the state of input devices and makes decisions based upon a customizable program to then control the state of output devices. [4]

It is worth mentioning that in an industrial setting, a competitor to SCADA and PLC-based control systems is the distributed control system or DCS. DCS is a combination of software and hardware that "connects industrial controllers, sensors, and operator terminals or computers in an industrial facility."[5] What makes DCS unique is that in a DCS its data acquisition and control functions are performed by "distributed processors that are situated nearby the peripheral industrial devices or instruments from which data is being gathered." [6]

There is some debate about the use of DCS vs SCADA and PLC; however, it is generally acknowledged by industry experts that each of them has different and/or better functionality for different industrial organizations depending on the size and extent of the industrial operation, yet each is vulnerable to cyber-attacks.[7]

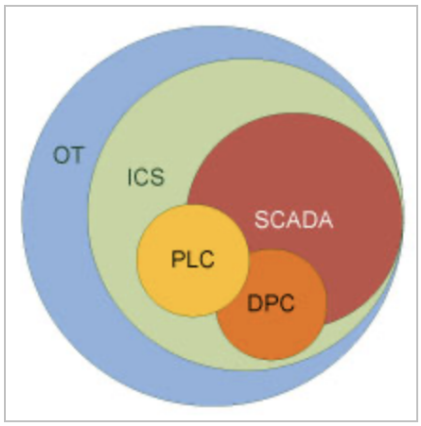


Image 1: visualization of where ICS falls in OT. [8]

[3]Team, Securicon. "What's the Difference Between OT, ICS, SCADA and DCS? - Insight from Securicon." Securicon, 18 Feb. 2020.
[4]Team, Securicon. "What's the Difference Between OT, ICS, SCADA and DCS? - Insight from Securicon." Securicon, 18 Feb. 2020.
[5]"What Are the Differences Between DCS and SCADA?" RealPars, 29 July 2020.
[6]"What Are the Differences Between DCS and SCADA?" RealPars, 29 July 2020.
[7]Team, Securicon. "What's the Difference Between OT, ICS, SCADA and DCS? - Insight from Securicon." Securicon, 18 Feb. 2020.
[8] Williamson, Graham. "OT, ICS, SCADA – What's the Difference?" KuppingerCole, 2015

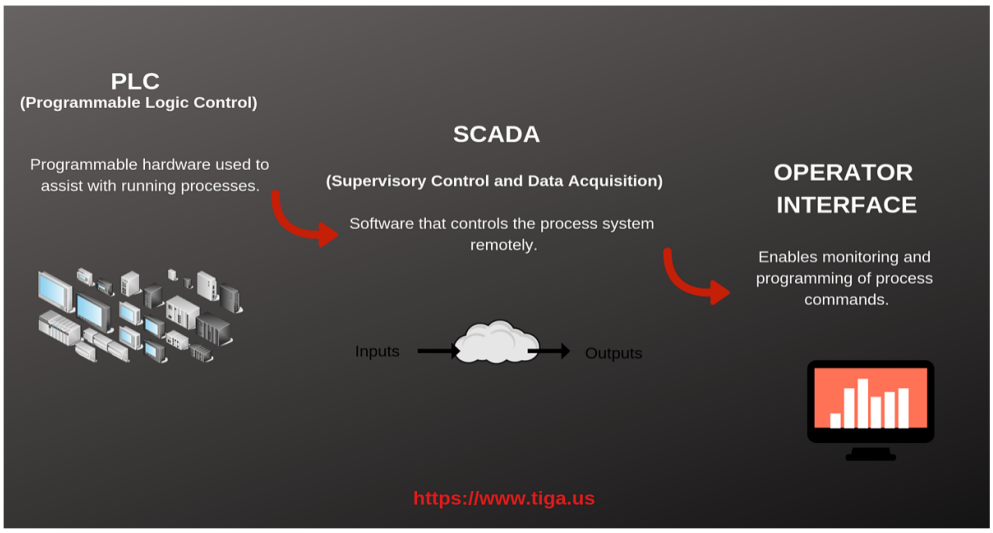


Image 2: visualization of communication between PLC, SCADA, and the operator interface [9]

CAUSING PHYSICAL DAMAGE

Cyber-attacks on operational technology (OT), specifically Industrial Control Systems (ICSs), can cause physical harm or damage. This is because ICS networks control physical industrial processes. If these networks are targeted by a cyber-attack, the physical processes can be maliciously manipulated so that they fail or perform not how they are intended, causing physical harm and damage.

For example, one of the most important examples of an ICS attack that caused physical damage is the "**Stuxnet**" cyber-attack on the Natanz Iranian nuclear facility that was discovered in 2010. Stuxnet is widely agreed upon to be the first successful use of a cyberweapon that caused physical damage.[10] Information security experts agree that Stuxnet had two major functions. One function targeted the Natanz facility's Industrial Control System (ICS). Specifically, the Programmable Logic Controllers (PLCs) within the facilities ICS were targeted by the perpetrators and used to make the nuclear centrifuges spin at speeds they were not intended to. This led to the centrifuges eventually tearing themselves apart. The other function targeted the facility's Supervisory Control and Data Acquisition (SCADA) and mirrored what regular operations of the centrifuges looked like so that the operators could not tell that anything was wrong[11]. Using International Atomic Energy Agency (IAEA) data, the Institute for Science and International Security (ISIS) concluded that at some point between late 2009 and early 2010,

[9] Tiga. "What Is The Difference Between PLC And SCADA?" *TIGA*, Feb. 2019
[10] Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'." Wired, Conde Nast, 4 June 2017.
[11] Broad, William J., et al. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times, The New York Times, 15 Jan. 2011.

Stuxnet destroyed around 1,000 IR-1 centrifuges of the 9,000 IR-1 centrifuges at the Natanz facility.[12]

CROSSING THE LINE

The risk that an ICS attack could draw the United States into a war emanates from its ability to cause physical damage and harm. Under international law, all countries who are signatories to the UN are barred from the use of force by Article 2(4)[13] unless it is approved by the UN Security Council or is done in self-defense. A country's use of self-defense is protected by Article 51 of the UN Charter.[14] As there has yet to be a UN security council ruling that has justified the use of force in response to a cyber-attack of any nature, this paper acknowledges that the most likely situation where the effects of a cyber-attack would justify a use of force is when the effects of a cyber-attack trigger a states' right to use force in self-defense protected by Article 51.

To understand why an ICS cyber-attack could trigger a state's right to self-defense under Article 51, it is essential to understand the term "armed attack" and what it entails. The term armed attack is used in Article 51 of the United Nations Charter as the determining factor for when a state can use force in self-defense against another state: "all Members shall refrain . . . from the threat or use of force against . . . any state," except when the use of force is approved by the Security Council or, under Article 51, is used in "self-defense if an armed attack occurs against a Member."[15] It is generally accepted in customary international law that an armed attack is any action which "causes death or injury (including illness and severe suffering) to individuals or damage or destruction of objects."[16] Therefore for a cyber-attack to trigger a state's right to self-defense, the effects of that attack must harm people or cause physical damage. A state's right to self-defense when subjected to a cyber-attack that causes physical harm or damage is corroborated by the Tallinn Manual in Chapter 14 section two, "self-defense:" "a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense."[17] Knowing that ICS cyber-attacks can cause physical harm or damage, the information above demonstrates that under international law, the United States could legally respond to an ICS cyber-attack that caused physical harm or damage with physical force.

---

[12] Albright, David, et al. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." Institute for Science and International Security, Feb. 2011.
[13] "Chapter I." *United Nations,* 2020.
[14] "Chapter VII." *United Nations,* 2020.
[15] "Chapter VII." *United Nations,* 2020.
[16] "Chapter VII." *United Nations,* 2020.
[17] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2 Feb. 2017.

AN UPWARD TREND

To date, ICS cyber-attacks, especially those that can cause physical harm or damage, such as Stuxnet, have been infrequent in comparison to IT cyber-attacks. Two factors that may explain this are the complexity of creating and deploying an ICS attack (requiring knowledge of the ICS network)[18] and the implications of launching a cyber-attack whose effects could prompt forceful retaliation protected by Article 51. However, the infrequency of ICS attacks so far should not be mistaken for them not occurring more frequently in the future. Attacks targeting ICS have increased in number yearly since 2000.[19] Already this year, 2021, there has been an ICS cyber-attack targeting a water treatment facility in Florida with the intent to poison the treated water, a cyber-attack on an Israeli water treatment facility, and an attack on an Indian power grid.[20,21,22] Information security experts also believe that ICS attacks will increase and occur more frequently in the future as escalating geopolitical tensions increase and[23] advanced persistent threat (APT) groups, including those who attack various industrial sectors, continue to grow.[24, 25]

Furthermore, ICS has become a more appealing target for cybercriminals who can use or sell ICS vulnerabilities as ICS vulnerabilities have become more evident[26] and as ransomware such as Ryuk and Emotet can potentially bridge the IT/OT gap.[27] While cybercriminals will most likely target OT/ICS for financial purposes and nation-states will target ICS for sabotage, defending against both types of attacks will be equally important as it is likely that in the future there will be more cyber-attacks targeting ICS disguised as ransomware but which actually are pursuing different goals than ransomware.[28]

---

[18] "Sanger, David E. "Iran Fights Malware Attacking Computers." The New York Times, The New York Times, 25 Sept. 2010.
[19] Hemsley, Kevin E., and Dr. Ronald E. Fisher. "History of Industrial Control System Cyber Incidents." History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV, 31 Dec. 2018
[20]Evans, Jack. "Someone Tried to Poison Oldsmar's Water Supply during Hack, Sheriff Says." Tampa Bay Times, Tampa Bay Times, 10 Feb. 2021.
[21] Sanger, David E., and Emily Schmall. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out." *The New York Times*, The New York Times, 28 Feb. 2021.
[22] "Connect the Dots on State-Sponsored Cyber Incidents - Attack on Israeli Water Utilities." *Council on Foreign Relations*, Council on Foreign Relations
[23]"Dragos 2019 YEAR IN REVIEW: LESSONS LEARNED FROM THE FRONT LINES OF ICS CYBERSECURITY.", Dragos, 2020.
[24] Hemsley, Kevin E., and Dr. Ronald E. Fisher. "History of Industrial Control System Cyber Incidents." History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV, 31 Dec. 2018.
[25] "ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020
[26] "ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020
[27] "Dragos 2019 YEAR IN REVIEW: LESSONS LEARNED FROM THE FRONT LINES OF ICS CYBERSECURITY.", Dragos, 2020.
[28] "ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020.

OVERARCHING CYBER-WAR STRATEGY

Beyond the adverse effects ICS cyber-attacks can have as individual events, ICS cyber-attacks are a component of waging cyber-war. Cyber-war, as defined by Richard Clark and Robert Knake in the book C*yber War, is* "actions by a nation-state to penetrate another nation's computers or networks to cause damage or disruption."[29] Cyber-war is important because the United States' strength as a technologically advanced nation is also a large weakness. This is because the United States' IT and OT infrastructure is an easy target for countries which are less militarily capable but who can use cyber capabilities to cripple the United States without ever deploying military forces. Clark describes that the coordinated actions in cyberspace employed in a cyber-war would target the United States critical infrastructure, affecting civilians in various capacities, target our military's ability to communicate and operate incoordination, and would cripple our financial sector.[30] ICS cyber-attacks in a coordinated cyber-war strategy are important because they are what would be used to target critical infrastructure to cause "damaging effects."

ELECTRICITY GRID HACKS PART OF CHINA'S STRATEGY

There is evidence that our adversaries have cyber-war strategies that implement cyber-attacks on critical infrastructure and that they have taken actions to prepare the cyber battlefield for the implementation of these strategies. For instance, the book *Unrestricted Warfare,* a translation of an unofficial strategy written by two high-ranking PLA officials -- Col Qiao Liang and Col Wang Xiangsu -- details how less militarily sophisticated countries can look beyond traditional military operations to take on status quo world powers. In this book, there is a section stating that if a war were to break out with a nation possessing full information technology, a combination methodology could be used to undermine the technological advancements and then usurp the advanced nation militarily. This methodology as found in *Unrestricted Warfare* is provided below.

"If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are

[29] Clarke, Richard A. cyber-war. HarperCollins, 2011.
[30] Clarke, Richard A. cyber-war. HarperCollins, 2011.

completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the Army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty."[31]

This statement demonstrates how the Chinese military is aware of the decisive role targeting critical infrastructures plays in warfare with a more militarily and technologically sophisticated country such as the United States. Additionally, China's awareness may have escalated to action as a United States intelligence leak to the media in 2009 stated that the Chinese had penetrated the United States power grid and left behind "tools" that, if used, could cause failures in the power grid that could bring the whole grid down.[32]

UKRAINE IS JUST PRACTICE FOR RUSSIA

Similar to *Unrestricted Warfare,* in 2013, Russian chief of the General Staff, General Valery Gerasimov, published an article in a relatively obscure Russian military policy journal that outlined his observations on "a new, whole-of-government style of warfare—one that blurs the line between war and peace."[33] This article, known as the Gerasimov Doctrine, emphasized "hybrid warfare"[34] that utilizes proxies, disinformation, and other measures short of war. Two demonstrations of Russian hybrid warfare are the use of disinformation and cyber-attacks against Georgia in 2008, and, more importantly, the Russian attacks on the Ukrainian power grid in 2015 and 2016.[35] The cyber-attacks against Ukraine's power grid are unique because they were the first known successful cyber-attacks on an electrical grid.[36] An interagency team composed of personnel from the United States National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), United States Computer Emergency Readiness Team (US-CERT), United States Department of Energy, the Federal Bureau of Investigation, and the North American Electric Reliability Corporation, concluded that Ukraine's power grid was more secure than the United States'. Most importantly, information security experts have said they believe Russia is using

[31] Qiao, Liang . Unrestricted Warfare: China's Master Plan to Destroy America (pp. 148-149). Shadow Lawn Press. 1999.
[32] Clarke, Richard A. cyber-war. HarperCollins, 2011.
[33] Nicole Ng, Eugene Rumer. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture." Carnegie Endowment for International Peace, 03 July. 2019.
[34] Nicole Ng, Eugene Rumer. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture." Carnegie Endowment for International Peace, 03 July. 2019.
[35] J. Assante, Michael, et al. "Analysis of the cyber-attack on the Ukrainian Power Grid." *E-ISAC and SANS*, Kaspersky Labs, Mar. 2016.
[36] Volz, Dustin. "U.S. Government Concludes cyber-attack Caused Ukraine Power Outage." Reuters, Thomson Reuters, 25 Feb. 2016.

Ukraine to test and perfect cyber-war techniques that could be eventually intended for the U.S.[37]

CHALLENGES

Because ICS attacks are most likely of all cyberattacks to escalate into war, the tactics, techniques, and procedures used for ICS attacks could be considered cyber weapons. Once cyber weapons are used, their code and construction can become publicly exposed, as was the case with the Stuxnet malware.[38] States are investing massive amounts of time and energy into creating and fielding complex cyber weapons, including for ICS attacks. If/when they become public, cybercriminals can see and copy them. For instance, the BlackEnergy malware attributed to the Russian military hacking organization Sandworm has been distributed throughout the Russian underground crime networks as it has also more recently been used by Russian cybercriminals to steal credit card data.[39] In the words Roel Schouwenberg, a senior researcher for Kaspersky Lab, "Regular cybercriminals look at something that Stuxnet is doing and say, that's a great idea, let's copy that."

Cyber weapons are also hard to track compared to conventional weaponry and nuclear weapons. Cyber weapons at their base level are code, whereas nuclear weapons are physical items, and thus easier to track because they require specific physical resources which can also be observed and tracked. Militaries, intelligence organizations, NGOs, and international agencies such as the IAEA track conventional weaponry and nuclear arms so that they don't fall into the wrong hands. Private cybersecurity firms, military commands such as USCYBERCOM, and intelligence agencies, track cyber attacks and cyber threat actors. What is lacking is an international cyber coalition or international cyber agency capable of tracking and protecting countries that do not have adequate defense resources against cyber weapons.

The potential for a cyber weapon's code to become publicly available makes the sale and reuse of cyber weapons developed by nation-states to terrorists, state proxies, or criminal organizations (who may be more willing to deploy them) of major concern to policymakers. Rising ransomware attacks on industries and the Colonial Pipeline attack, in particular, show the increasing vulnerability of ICS to criminals.[40]

---

[37] "Experts Suspect Russia Is Using Ukraine As A Cyberwar Testing Ground." NPR, NPR, 22 June 2017.
[38] "Stuxnet Analysis by Langner, Based on Reverse Engineering of the Payload." *Langner*, 23 July 2020,
[39] "Russian Malware Used by 'Privateer' Hackers against Ukrainian Government." The Guardian, Guardian News and Media, 25 Sept. 2014.
[40] Team, Waterfall. "Ransomware Targets Largest Gasoline Pipeline in USA." *Waterfall Security*, 13 May 2021.

VULNERABILITIES

Although ICS network security is inherently more secure than most IT network security due to less accessibility to the network (air gaps/firewalls), it is still deceivingly weak. The industrial network security firm Waterfall Solutions applied a capabilities-based threat assessment to the ICS network of a wastewater treatment plant "protected to first-generation ICS security best practices, published roughly 2003-2013." In this assessment, Waterfall Solutions concluded that the network security of the water treatment plant was not able to defeat 16 of the top 20 ICS cyber-attacks that range in sophistication from "ICS Insider" and "IT insider" to the "Stuxnet virus" and targeting the "hardware supply chain." When the capabilities-based assessment was repeated on an Industrial Internet of Things IIoT ICS network design for the water treatment system, the results showed that the network security was even weaker as 18 of the top 20 ICS cyber-attacks were not defeated.

Many of the ICS network weaknesses and challenges with securing ICS networks, all of which can be factored into explaining why the 2003 - 2013 best practice ICS security standards fail to protect an ICS from the majority of cyber-attacks that target ICS, have been identified by the industrial cybersecurity firm Dragos in their ICS/OT security "Year in Review" reports.

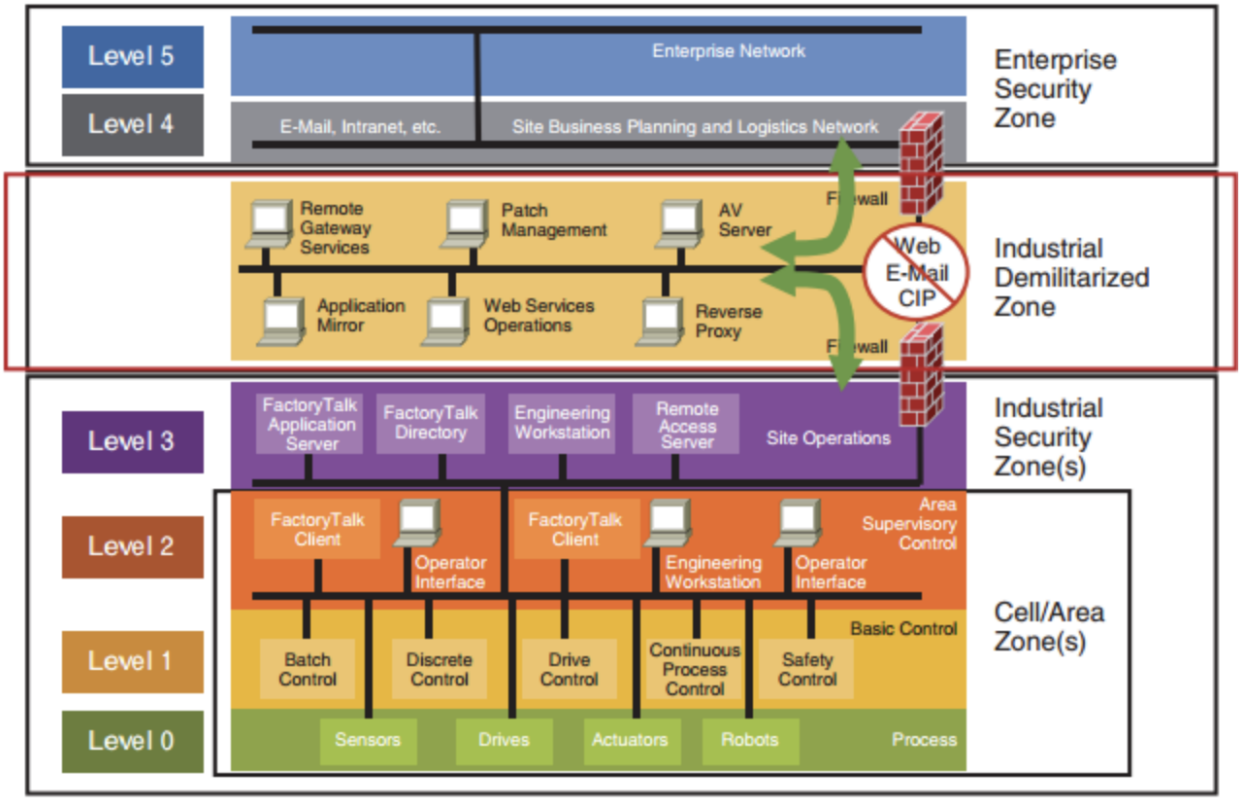
Since 2016, Dragos has published yearly reviews on ICS security that identify numerous existing ICS/OT security challenges, threats, and weaknesses. In the "2020 Year in Review" report, Dragos identified multiple industry-wide current ICS/OT security challenges. The identified challenges are as follows: IT/OT convergence; the growing OT threat landscape; lack of OT visibility; lack of accurate asset inventory and network mapping; cyber operational vulnerabilities; monitoring to track changes, errors, intrusions, and ongoing attacks; and vulnerable flat or not well-segmented networks.[41]

After examining identified ICS vulnerabilities, Dragos recognized that twenty-three percent of ICS vulnerabilities were because of products that bordered the enterprise and its network. These products include networking communication equipment, VPNs, data historians, or firewalls commonly deployed in ICS networks and ICS surrounding networks. Dragos also identified that ICS-targeting APTs, VANADINITE, and PARISITE, in particular, have leveraged these network bordering vulnerabilities for initial access to ICS. These border product vulnerabilities are important because they pose a risk to industrial operators and their workstations as they can provide immediate access to the ICS network and bypass network security controls such as firewalls and other means of segmentation.[42]

[41] "Dragos 2020 Year In Review Lesson Learned Webinar." YouTube, YouTube, 2 Apr. 2021.
[42] "Year in Review." *Dragos*, 1 Jan. 2021.

In the "2020 Year in Review" report, Dragos identified that most of the vulnerabilities in ICS networks that were targeted in 2020 were located deep within the ICS network. These vulnerabilities were located within equipment on Levels 0 to 3 of the Purdue Model for ICS security. This equipment includes engineering workstations, programmable logic controllers, sensors, and industrial controllers. This is important because much of the hardware and software that exists within levels 0 to 3 of the Purdue model is used to control industrial processes.[43]

These vulnerabilities residing within levels 0 to 3 of the Purdue Model are important as they are deep within the OT topology, however, they require access to a control system network to be exploited. To be effectively targeted, the adversary must have access to the ICS network. This is positive if industrial facilities make the effort to implement proper network segmentation and enforce certain network security protocols that prevent an adversary's access to the ICS network. However, on the negative side, with the increasing connectivity of organizations, industrial organizations included, properly conducted network segmentation is diminishing.[44]



[43] "Year in Review." *Dragos*, 1 Jan. 2021.
[44] "Year in Review." *Dragos*, 1 Jan. 2021

Image 3: the Purdue model [45]

The 2020 "Year in Review" report also states that the percentage of disclosed flaws which could be used to cause a loss of view and loss of control in ICS systems decreased from 50 percent in 2019 to 36 percent in 2020. However, the report notes that this apparently improved percentage decrease is most likely due to a relative increase in the identified vulnerabilities bordering enterprises that do not have direct operational impacts and can be more easily patched. On the negative side, it demonstrates that most of the vulnerabilities that allow for command and control and cause operator loss of view still exist and are unpatched but have become outnumbered by the amount of less detrimental vulnerabilities that have been identified and are easier to patch.[46]

Multiple third-party vulnerabilities in the software supply chain that impacted ICS systems were identified in the 2020 "Year in Review" report. Some of the more notable of these third-party vulnerabilities were Ripple20 and Amnesia:33, both being vulnerabilities in third-party provided Internet Protocol (IP) stacks. What is important about these third-party stacks is that many of them are embedded in products within the ICS network including PLCs, Serial to Ethernet Converters, Protocol Converters, Remote Terminal Units (RTUs), digital protective relays, and some managed network switches and routers. Although these vulnerabilities are embedded within the ICS network, which is dangerous, the mass exploitation of these vulnerabilities is rare because of how deeply they are embedded in the ICS network and the layers of protection surrounding them. Exploiting these vulnerabilities in third-party stacks embedded within the ICS requires a significant understanding of the stack and the hardware of the Central Processing Unit (CPU) architecture, memory layout, and connections of the vulnerable device in which it is embedded.[47]

The COVID-19 pandemic strongly changed the work environment and forced many people to work from home. Although many industrial systems operators had to remain in the office, other employees at industrial facilities began to work remotely. This is important because Dragos in their 2020 Year in Review Report identified vulnerabilities in virtual private network VPN appliances that facilitate remote work in the industrial sector. Dragos tracked advisories regarding vulnerabilities in the ICS-specific VPN services Ewon, Cosy, and Flexy. Most enterprise VPNs are used by industrial operators to access corporate and operations networks, but some even provide VPN access specifically to ICS equipment. Dragos highly recommended that

[45] "The Third Network." *I²oT Solutions*.
[46] "Year in Review." *Dragos*, 1 Jan. 2021
[47] "Year in Review." *Dragos*, 1 Jan. 2021.

vulnerabilities in VPN appliances be remediated as quickly as possible as some allow for lateral movement. Those that allow for access to ICS are specifically dangerous.[48]

The OT and ICS-specific vulnerabilities listed above can be addressed and fixed. CISA Dragos, Waterfall Solutions and other cybersecurity firms and government agencies have published recommendations for securing ICS and OT. However, what leaves ICS and OT vulnerable is that none of these recommendations are binding or enforced by a regulatory body or agency. This leaves ICS and OT security largely in the hands of the industrial organizations. In the past, the relationship between private industry and the government has been one of "advisement;" the Colonial Pipeline attack has fostered new developments as the Department of Homeland Security is working to promulgate new pipeline security regulations which will likely be mandatory.[49] Once they have completed their focus on pipelines, they would be well-advised to move on to other, equally vulnerable critical infrastructures.

"

In the past, the relationship between private industry and the government has been one of "advisement;" the Colonial Pipeline attack has fostered new developments as the Department of Homeland Security is working to promulgate new pipeline security regulations which will likely be mandatory.[50] Once they have completed their focus on pipelines, they would be well-advised to move on to other, equally vulnerable critical infrastructures.

"

[48] "Year in Review." *Dragos*, 1 Jan. 2021.
[49] "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators." *Department of Homeland Security*, 27 May 2021.
[50] "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators." *Department of Homeland Security*, 27 May 2021.

CITATIONS

Williamson, Graham. “OT, ICS, SCADA – What's the Difference?” KuppingerCole, 2015, www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

Broad, William J., et al. “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.” The New York Times, The New York Times, 15 Jan. 2011, www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Albright, David, et al. “Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report.” Institute for Science and International Security, Feb. 2011, isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2 Feb. 2017. Kindle Edition. Instance

Sanger, David E. “Iran Fights Malware Attacking Computers.” The New York Times, The New York Times, 25 Sept. 2010, www.nytimes.com/2010/09/26/world/middleeast/26iran.html

“ICS Threat Predictions for 2021.” Kaspersky ICS CERT, 2 Dec. 2020, ics-cert.kaspersky.com/reports/2020/12/02/ics-threat-predictions-for-2021/.

“Dragos 2019 YEAR IN REVIEW: LESSONS LEARNED FROM THE FRONT LINES OF ICS CYBERSECURITY.” *Dragos.com*, Dragos, 2020, www.dragos.com/wp-content/uploads/Lessons_Learned_from_the_Front_Lines_of_ICS_Cybersecurity.pdf?hsCtaTracking=ea40a828-084b-4ee9-a0fc-0908864d3f8e|4eafb14d-2e38-44e0-9e6d-08c2aea4a480.

3:42

Ginter, Andrew. “Top 20 cyber-attacks on Industrial Control System: Waterfall.” | *Waterfall Security*, Waterfall, 30 Nov. 2020, waterfall-security.com/20-attacks/.

Qiao, Liang . Unrestricted Warfare: China's Master Plan to Destroy America (pp. 148-149). Shadow Lawn Press. Kindle Edition.

Volz, Dustin. “U.S. Government Concludes cyber-attack Caused Ukraine Power Outage.” Reuters, Thomson Reuters, 25 Feb. 2016, www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K.

“Experts Suspect Russia Is Using Ukraine As A Cyberwar Testing Ground.” NPR, NPR, 22 June 2017, www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground. .

Clarke, Richard A. cyber-war. HarperCollins, 2011.

Evans, Jack. "Someone Tried to Poison Oldsmar's Water Supply during Hack, Sheriff Says." Tampa Bay Times, Tampa Bay Times, 10 Feb. 2021, www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.

Hemsley, Kevin E., and Dr. Ronald E. Fisher. "History of Industrial Control System Cyber Incidents." History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV, 31 Dec. 2018, www.osti.gov/servlets/purl/1505628.

Nicole Ng, Eugene Rumer. "The West Fears Russia's Hybrid Warfare. They're Missing the Bigger Picture." Carnegie Endowment for International Peace, 03 July. 2019.

carnegieendowment.org/2019/07/03/west-fears-russia-s-hybrid-warfare.-they-re-missing-bigger-picture-pub-79412.

"Russian Malware Used by 'Privateer' Hackers against Ukrainian Government." The Guardian, Guardian News and Media, 25 Sept. 2014, www.theguardian.com/technology/2014/sep/25/russian-malware-privateer-hackers-ukraine.

Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'." Wired, Conde Nast, 4 June 2017, www.wired.com/2013/03/stuxnet-act-of-force/.

"Chapter VII." *United Nations*, United Nations, 2020, www.un.org/en/sections/un-charter/chapter-vii/index.html.

"Chapter I." *United Nations*, United Nations, 2020, www.un.org/en/sections/un-charter/chapter-i/index.html.

"Critical Infrastructure Sectors." *Cybersecurity and Infrastructure Security Agency CISA*, October 21, 2020, www.cisa.gov/critical-infrastructure-sectors.

CRS. "Critical Infrastructures: Background, Policy, and Implementation." *EveryCRSReport.com*, Congressional Research Service, 10 June 2015, www.everycrsreport.com/reports/RL30153.html.

Clarke, Richard A., and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, 2019.

"Backgrounder on Cyber Security." *United States Nuclear Regulatory Commission*, 2019, www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html#require.

Clarke, Richard A., and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, 2019.

Daniel Shea, Gretchenn DuBois. "Cybersecurity and the Electric Grid: The State Role in Protecting Critical Infrastructure." *Cybersecurity and the Electric Grid | The State Role in Protecting Critical Infrastructure*, www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx.

"Silent Cyber Scenario: Opening the Flood Gates." *AON*, Oct. 2018, success.guidewire.com/rs/140-LHX-683/images/Long_form_final.pdf.

"Connect the Dots on State-Sponsored Cyber Incidents - Attack on Israeli Water Utilities." *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/cyber-operations/attack-israeli-water-utilities.

Sanger, David E., and Emily Schmall. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out." *The New York Times*, The New York Times, 28 Feb. 2021, www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

Hemsley, Kevin E., and Dr. Ronald E. Fisher. "History of Industrial Control System Cyber Incidents." History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV, 31 Dec. 2018, www.osti.gov/servlets/purl/1505628.

J. Assante, Michael, et al. "Analysis of the cyber-attack on the Ukrainian Power Grid." *E-ISAC and SANS*, Kaspersky Labs, Mar. 2016, media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Team, Securicon. "What's the Difference Between OT, ICS, SCADA and DCS? - Insight from Securicon." Securicon, 18 Feb. 2020, www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/.

"What Are the Differences Between DCS and SCADA?" RealPars, 29 July 2020, realpars.com/dcs-vs-scada/.
"Year in Review." *Dragos*, 1 Jan. 2021, www.dragos.com/year-in-review/.
"Dragos 2020 Year In Review Lesson Learned Webinar." YouTube, YouTube, 2 Apr. 2021, www.youtube.com/watch?v=WDVmbmj3FwY.

Tiga. "What Is The Difference Between PLC And SCADA?" *TIGA*, Feb. 2019, www.tiga.us/blog/what-is-the-difference-between-plc-and-scada.

Team, Waterfall. "Ransomware Targets Largest Gasoline Pipeline in USA." *Waterfall Security*, 13 May 2021, waterfall-security.com/ransomware-targets-largest-gasoline-pipeline-usa/?utm_campaign=WD%2B-%2BGas%2BPipeline&utm_source=google&utm_medium=ppc&utm_term=colonial+pipeline+attack&utm_content=11-05-2021&utm_feeditemid=&utm_device=c&hsa_cam=13048509797&hsa_grp=123818460604&hsa_mt=p&hsa_src=g&hsa_ad=520578676275&hsa_acc=7472163176&hsa_net=adwords&hsa_kw=colonial+pipeline+attack&hsa_tgt=kwd-1256392521536&hsa_ver=3&gclid=Cj0KCQjwkZiFBhD9ARIsAGxFX8ADXDd3zotsPTEG-VfoQb_1KqmYP0YX8TIZJRs3_wHaBaUAJIKqufwaAtoBEALw_wcB.

"DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators." *Department of Homeland Security*, 27 May 2021, www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

"Stuxnet Analysis by Langner, Based on Reverse Engineering of the Payload." *Langner*, 23 July 2020, www.langner.com/stuxnet/.

"The Third Network." *I²oT Solutions*, www.i2otsolutions.com/the-third-network.

ABOUT THE AUTHOR

Daniel Simonds

Daniel Simonds is a Researcher at the Global TechnoPolitics Forum and a senior at the University of Southern California, majoring in International Relations and minoring in Geospatial Analysis and Human Security.

His research interests include foreign affairs, diplomacy and public policy.

GLOBAL TECHNOPOLITICS FORUM LEADERSHIP

CHAIRMAN

Gregory F. Treverton

PRESIDENT

Pari Esfandiari

SENIOR DIRECTOR

Maura Godines

BOARD OF ADVISORS

Philip Chase Bobbitt

David Bray

Thomas A. Campbell

Shelby Coffey

Shanta Devarajan

C. Bryan Gabbard

Nancy K. Hayden

Jim Herriot

Molly Jahn

Spencer Kim

Robert Klitgaard

Ronald Marks

Kevin M O'Connell

Barry A. Sanders

Rod Schoonover

Davide Strusani

Peter Vale

John Walcott

James F. Warren

David K. Young

Global TechnoPolitics Forum

The Global TechnoPolitics Forum is a 501(C)(3) nonprofit educational organization with a mission to shape the public debate and facilitate global coordination at the intersection of technology and geopolitics. It achieves this mission through: convenings, research, and community building.

www.TechnoPolitics.org
info@technopolitics.org
Tel: +1.202.735.1415