Critical Infrastructure, Industrial Control Systems and Cyber Warfare: Ethical and Anticipated Ethical Issues

Richard Wilson[1] and Noah Donnelly[2]
[1]Department of Philosophy/Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA
[2]Computer Science and Information Sciences, Towson University, Baltimore, Maryland, USA

wilson@towson.edu
ndonnel1@students.towson.edu

Abstract: Cyber-attacks on Critical Infrastructure and Industrial Control Systems within nation states are very dangerous. They can damage the services and systems that a country needs to maintain safety and stability. There are reasons why these attacks are so problematic. First, Critical Infrastructure and Industrial Control Systems are very important. They regulate the operation of services that are vital to the public such as power grids, water services, roads, hospitals, and banks. Industrial Control Systems also control how things are made in industries like energy and manufacturing. Critical Infrastructure and Industrial Control Systems play a role in keeping a country running. When these systems are disrupted, the economic paralysis, civilian risks, and military vulnerabilities are very similar to what happens in a war. The effects of the disruption of Critical Infrastructure and Industrial Control Systems have large consequences. The way these attacks occur shows that they can cause a lot of problems and help aggressors achieve their goals. These attacks are analogous to bombings. Instead of using physical weapons, belligerents use computers. Because these attacks on infrastructure systems like power and water can cause real physical damage, stop production, or make water undrinkable, they fail to differentiate between military targets and civilians. The economic paralysis, civilian risks, and military vulnerabilities caused by these attacks on Critical Infrastructure and Industrial Control Systems are a problem. These attacks are like acts of war. We are going to examine IC and ICS attacks from two sides, the technical side and the ethical side. We will use examples like Stuxnet, the Ukraine Power Grid compromises the Colonial Pipeline ransomware event, Triton/Trisis safety breaches the Oldsmar water facility incursion, and the JBS meat processing interference. These examples will show what aggressors are trying to accomplish by attacking industrial control systems, how the attacks affect ICS, and how large these operations are, that that these cyber-attacks are really like warfare against the nation states where industrial control systems are located. The attacks upon Industrial control systems are like acts of war. Moreover, this discussion will explore both the ethical dilemmas and anticipated ethical issues with cyber-attacks on CI and ICS. Furthermore, it addresses the morality of categorizing these cyber-attacks as cyber warfare. As a result, examining these cases will help clarify the greater implications of cyber-attacks on nation state CI and ICS systems for national and global security as well as the ethical frameworks governing cyber engagements.

Keywords: Industrial control systems (ICS), SCADA, Programmable logic controllers (PLC), Safety instrumented systems (SIS), Critical infrastructure, Cyber warfare, Modbus, Firmware analysis

1. Introduction

Modern nations rely on a complicated and invisible network of automated systems called Critical Infrastructure (CI). Laying below the surface of everyday life, behind the light switches, tap water, and gas pumps is a large network of Industrial Control Systems (ICS) and Operational Technology (OT). OT is different than Information Technology (IT) that manages data, OT manages physical systems based on laws of physics. OT spins turbines, mixes chemicals, regulates pressure, and opens valves. These systems operated for decades in isolation with proprietary controls, and they were protected due to their running on a closed system (Stouffer et al., 2015). OT was physically separated from the outside world. The drive for efficiency and the move towards remote monitoring has caused OT and IT to merge, which in effect connects legacy industrial systems to the public internet system. This merger has created a new, paralyzing mode of conflict where lines of code can cause physical destruction.

The inherent vulnerability of these systems' inherent vulnerability now represents a fundamental change in how war can be conducted. Previously to destroy infrastructure, the barrier to entry was higher, requiring explosives and an effective way to deliver and detonate them. Moving to today, and state-sponsored hackers can now achieve the same results by manipulating the logic of a Programmable Logic Controller (PLC) from the comfort of their own home (Perlroth, 2021). This capability creates serious ethical questions with regards to the Principles of Distinction and Proportionality. If a cyber-attack were to target a power grid that is used for both civilian and military purposes, not only would it shut off a radar, but it could also eliminate the power to incubators in hospitals, traffic lights in cities, and produce in stores. This now creates a potential for "Cascading Failure", where a localized attack can spread to sectors connected to a power grid. This means that what may have been intended as a limited strike is now effectively a cyber-attack that affects an entire population.

This paper argues that cyber-attacks on ICS are not just criminal acts or espionage, they are acts of war via digital means that violate International Humanitarian Law (Rid, 2012). Through an analysis of the low-level mechanics, we see that these attacks compromise the established "Purdue Model" of industrial control (Williams, 1992). By examining the range of cyber-attacks including the Enterprise Zone down to the Process zone, we identify the fragility of modern infrastructure. Through forensic analysis of case studies including the molecular level sabotage of Stuxnet, the brute-force method used on the Ukraine power grid, and the supply chain stoppage of Colonial Pipeline and JBS. Through those case studies we can demonstrate that the weaponization of critical infrastructure through digital means and cyber-attacks is the greatest ethical challenge of the 21st century.

2. Technical Issues

Understanding the ethical issues related to the severity of ICS warfare, one needs to understand the low-level systems that make these systems so vulnerable. In ICS the priorities are Safety (physically of employees), Reliability and Availability. The priorities of ICS come at the cost of systems security (Stouffer et al., 2015).

2.1 The Purdue Model and Protocol Vulnerabilities

The architecture of ICS can typically be described by the Purdue Enterprise Reference Architecture (PERA) in which the network is segmented into different levels (Williams, 1992). Level 4 is the enterprise business network, that being IT, levels 0-3 are the OT environment. The OT environment ranges Supervisory Control and Data Acquisition systems at Level 2, all the way to the sensors and actuators at level 0. The vulnerabilities of the system lay in the communication protocols between levels. Since OT includes a variety of legacy systems, driven by the mindset which states if it works, don't replace it, this is where vulnerabilities are found. Legacy protocols such as Modbus, Distributed Network Protocol (DNP3), and Profibus are designed for a technical ecosystem of trust. They lack the basics of cyber security such as authentication and encryption (Morris & Gao, 2013). A Modbus TCP packet is comprised of a transaction identifier, protocol identifier, length field, unit identifier, function code, and the data itself. What is concerning is that there is no field for a password or any sort of user authentication. If a bad actor can access the network segment at Level 1 where the packet transactions take place, they can inject a "Function Code 5" (Write Single Coil) command to control the valves or turn pumps off in a system. The PLC obeys these orders with no questions. The machines have no way to distinguish between a legitimate command that comes from a Human-Machine Interface (HMI) and a command from a hacker's laptop in St. Petersburg. The entire system of global infrastructure lacks any sort of "Origin Integrity" (Stouffer et al., 2015).

2.2 PLC Logic and Firmware Manipulation

At the center of every industrial process is the Programmable Logic Controller (PLC). These computers execute something known as "Ladder Logic," a symbolic programming language meant to represent electrical relay circuits. Advanced cyber warfare attacks like Stuxnet do not only send bad commands, but they can also infect the PLC itself. This strategy of "Logic Injection" attacks involve an attacker rewriting the bytecode that is compiled and ran on the PLC's microprocessor (Langner, 2011). Firmware Modification is a more insidious technique. Firmware is low level code that interfaces with the PLC's hardware by connecting to its operating logic. By overwriting firmware, a "Rootkit" can be created at the hardware level. This allows the PLC to be issued malicious commands (spinning a turbine too fast) while reporting a normal status to the SCADA monitoring screens. This attack is occurring on the sensor itself. The operator can be looking at a screen that reports 0 RPM while the machine is disintegrating at 5,000 RPM. This is Epistemological Warfare, which involves manipulating the operator's perception of reality (Langner, 2011).

2.3 Safety Instrumented Systems (SIS)

Critical infrastructure has a last line of defense known as Safety Instrumented Systems (SIS). SISs are autonomous control loops, they are physically separated from the main process control, designed for monitoring critical thresholds like pressure and temperature, if those reach alarming levels it initiates a emergency shutdown (ESD). The SIS is supposed to operate on a closed loop within control systems. Modern "Smart" SIS controllers like the Schneider Electric Triconex controllers like remote diagnostics. The Triton/Trisis malware specifically targeted the firmware of the safety controllers (Sobczak, 2019). The malware interacted with the TriStation protocol which is a UDP-based protocol that configures controllers. Reverse engineering checksum algorithms and command codes of the TriStation protocol enabled the attackers to inject a Remote Access Trojan (RAT) into the memory of the safety controller. This malware had a conditional logic bomb, if the main attack fails, it disabled the SIS. Disabling the SIS prevents the failsafe from activating, allowing the plant to explode.

3. Ethical Issues

Weaponizing ICS presents a challenge to Just War Theory by creating new categories of moral responsibility and liability for state actors and engineers.

3.1 Erosion of Distinction in Multi-use Grids

The Principle of Distinction found in International Humanitarian Law (IHL) states that belligerents must distinguish between military objectives and civilian activities (Schmitt, 2017). The Principle of Distinction is impossible to uphold if a nation state engages in cyberwarfare against critical infrastructure. A powerplant is considered "Dual-Use" due to a single turbine that can power a local hospital and a military radar at the same time. Electrons do not carry designation tags, therefore, a cyber attack cutting power with the intention of degrading military capabilities will also result in civilian suffering. This shifts the burden of Proportionality onto the attackers. The Foreseeable Harm of cutting off power in a region can cause traffic accidents due to shut off lights, food spoiling causing economic loss, and the failure of medical equipment which could result in causing death. In traditional kinetic warfare, a kinetic strike upon a specific electrical substation knowing it feeds a base can also affect a civilian population. A cyber-attack upon power grids could cause a "Cascading Failure" which can cause blackouts that reach across entire regions. The effects of attacks on ICS's are inherently indiscriminate, which in turn makes them unethical.

3.2 Sociotechnical Imperative and Negligence

Anticipatory Ethics would place upon the operators and designers of the Critical Infrastructure a large moral responsibility. The Sociotechnical Imperative states that systems must be designed for the environments they operate in instead of idealized ones (Miller et al., 2011). ICS vendors prioritized "Availability" over "Confidentiality" thinking their systems would never connect to the internet. If you connected a Windows-XP based HMI to the internet in the modern era through TeamViewer, seen in the Oldsmar hack (CISA, 2021), it would count as Criminal Negligence. Failing to segment networks or implement Unidirectional Gateways is an ethical failure of failing to foresee the misuses of technology (Brey, 2012). The engineers and administrators can be complicit in the attacks that target critical life-safety systems by deploying an inherently faulty design. The state bears moral responsibility for stockpiling "Zero-Day" exploits meant for offensive use targeting ICS systems, which prioritizes offensive military operations over the safety of its own populus.

4. Case Studies

The following case studies illuminate the evolution of ICS warfare which causes indiscriminate destruction, and which highlight specific technical mechanisms used to bridge the gap between code that exists only in digital space and the physical realities that are the targets of these attacks.

4.1 Stuxnet (2010)

Stuxnet used four Zero-Day exploits to spread through Windows networks until it found the specific workstations that ran Siemens Step7 software. Once Stuxnet was inside the software it replaced a DLL (s7otbxdx.dll) with its own harmful version**.** A DLL is a dynamic link library, a shared code file that is used by Windows systems (Microsoft, 2021). This allowed the malware to replace incoming commands sent by an engineer to the PLC. Malicious Statement List (STL) was injected into the Siemens S7-315 PLCs which controlled the centrifuges. The logic changed the output frequency of the variable frequency drives (VFDs) from 1,064 Hz to 1,410 Hz which caused the rotors to spin at supersonic speeds and shatter, then dropped to 2 Hz, and then moved back up again (Zetter, 2014). It recorded 21 seconds of normal sensor data and looped it to play on the monitoring screens (Level 2 SCADA), making sure the attack went under the noses of the operators (Karnouskos, 2011). Stuxnet not only met the threshold of an "Armed Attack" due to its physical destruction, but it was also arguably just under Utilitarian outcomes-based ethics as it delayed Iranian nuclear proliferation. It demonstrated the ability for precise distinction, targeting only the PLCs with specific Profibus network cards.

4.2 Ukraine Power Grid (2015 & 2016)

The attack on Ukraine's power grid (Kyivoblenergo, Prykarpattyaoblenergo) was conducted by the Russian "Sandworm" group (Greenberg, 2019). This attack represents a shift from a precision cyber-attack to a brute-force attack. The attackers gained entry to the system through spear-phishing with the "BlackEnergy 3" malware. They targeted the OT networks and stole VPN credentials. On December 23, 2015, they accessed SCADA Operator Workstations. A synchronized attack where they virtually moved the mouse on operator screens, opening the circuit breakers at 30 substations, effectively cutting power to 230,00 customers (Lee et al., 2016).

Normally someone can simply turn the braker back on, but the Sandworm group inserted KillDisk wiper malware to overwrite the Master Boot Record (MBR) of the operator workstations, making it so operators could no longer boot them. Not only did they effectively kill the MBR, but they also targeted Serial-to-Ethernet converters which are devices that translate IP packets to commands for legacy breakers and overwrote their firmware with garbage data "bricking" the hardware (Assante, 2016). This forced Ukrainian operators to drive to the substations and close the breakers manually in the middle of winter. This attack targeted civilian heating and light sources during winter, it was a direct violation of the prohibition on attacking objects that are required for the survival of a civilian population. Russia wanted to freeze the Ukrainian population into submission, which counts as psychological warfare.

4.3 Triton/Trisis (2017)

Perhaps the darkest chapter in ICS warfare was the targeting of the Petro Rabigh petrochemical plants in Saudi Arabia by targeting the Safety Instrumented System (SIS). Attackers reverse-engineered the TriStation protocol used on UDP port 1502 by targeting the Schneider Electric Triconex safety controller. A payload was injected into the firmware of the controllers. The malware logic monitored the system's memory for a "trigger" condition, that being if there was an emergency, the failsafe would be disabled (Sobczak, 2019). The only reason this attack failed was due to the malware containing a bug that made the Triconex controller crash into a "Failsafe" mode (stopping the plant) as opposed to running malicious code. Stuxnet represented sabotage, Ukrainian power grid shutdowns represented disruption, Triton had the intent to kill people. Disabling the safety system serves one purpose, catastrophe. First a catastrophic explosion, then toxic gas releases, finally, the toxic gas causes mass casualties in the surrounding area. This technically fits the definition of being a War Crime, targeting noncombatant workers and innocent civilian populations with kinetic explosion and chemical warfare.

4.4 Colonial Pipeline (2021) and JBS Meat Packing

These intrusions effectively attacked the supply chain. They demonstrate the vulnerabilities that arise when IT and OT connect, and the rise of Ransomware-as-a-Service (RaaS). In the case of the Colonial Pipeline, the professional DarkSide ransomware group managed to compromise the corporate IT network by stealing a VPN password for an inactive account, which was leaked on the dark web. The ransomware technically only infected the IT billing and administrative systems, Colonial proactively shut down the OT pipeline because they can not bill customers for the fuel (Sanger & Perlroth, 2021). This is best viewed with the Interdependency Vulnerability in mind; OT was stopped because of the finances relating to IT. Similarly, JBS was attacked by Revil by using data exfiltration and encryption to halt meat processing plants across three continents (Turton & Mehrotra, 2021). Economic entities are now proxy battlefields. Criminal groups (often state-tolerated or sponsored) are willing to hold national food and fuel supplies hostage for economic gain through extortion. This obscured the line that separated cybercrime from economic warfare. The state must now consider whether a ransomware attack is an existential threat that justifies a military response.

4.5 Oldsmar Water Plant (2021)

In February 2021 there was a near miss when with a cyber-attack a hacker accessed the SCADA system of a water treatment plant located in Oldsmar, Florida (Perlroth, 2021). The plant used the outdated Windows 7 operating system, which a year earlier stopped receiving security updates. The plant was running TeamViewer which is a commercial remote desktop software which was installed directly on the SCADA workstations, and running on outdated software (CISA, 2021). The attacker managed to take control of the mouse and went to the HMI screen which controls chemical dosing. They changed the dosing of Sodium Hydroxide (Lye) from 100 parts per million (ppm) to 11,100 ppm, which at these levels can cause severe chemical burns or even death. Luckily, an operator noticed the mouse moving on the screen and immediately reversed the changes. This demonstrates how low the barrier to entry is for ICS warfare. This was not a sophisticated attack by a state; it was likely a hacker using a shared password. Yet the kinetic effect being mass poisoning would have caused a catastrophe.

5. Anticipatory Ethics

Failing to prevent Critical Infrastructure from being weaponized is a severe ethical failure of foresight. By applying "Moral Responsibility for Computing Artifacts" framework developed by Miller et al. (2011), specific lapses in engineering and administrative decisions can be identified.

5.1 Rule 4: The Sociotechnical Imperative

The Sociotechnical Imperative states, "People who design... can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded" (Miller et

al., 2011). This rule was ignored in the Oldsmar water plant incident, The designers of the SCADA workstation created a system where it was possible to remotely mix lethal chemicals into water. Their system prioritized remote convenience and budget constraints over safety. The installation of TeamViewer, a remote desktop tool meant for consumers to use which was placed directly onto machines and which then controlled life-safety actuators is an immense oversight. Ease of access was placed higher than the people's safety. They did not anticipate that within a sociotechnical environment filled with credential stuffing and shared passwords, that their tool would be compromised. A responsible implementation of this rule would require an" Out of band" access method or a hardware-based VPN with multi factor authentication. They failed to recognize the weakest link in the security chain is the user. This decision allowed a random hacker to attain admin level control of chemical dosing within the system.

5.2 Rule 2: The Foreseeability of Effect

Rule 1 states "The people who design... are morally responsible for that artifact, and for the foreseeable effects of that artifact" (Miller et al., 2011). This can be applied directly to the state actors who hoard Zero-Day vulnerabilities for ICS attacks. The creators of the "EternalBlue" exploit that was used in NotPetya and the Triton framework saw these tools designed to interface with industrial protocols (Greenberg, 2019). It was foreseeable that once these weapons were deployed, they could be reverse-engineered or leaked which would allow for them to be used by criminal gangs and hostile state actors. The foreseeable effect of developing malware that targets Schneider Electric safety controllers is eventually a negative outcome since all safety controllers become vulnerable to the same exploit (Brey, 2012). The state decided to prioritize offensive capabilities for destructive purposes over the defensive duty to update the safety of its own infrastructure, violating the social contract between a nation and its citizens. When a government finds flaws in a SIS, they are ethically obligated to disclose these shortcomings and patch them.

5.3 The Post-Deployment Mandate

Rule 2 declares "Responsibility includes being answerable for the behaviors of the artifact... after deployment" (Miller et al., 2011). ICS's have lifecycles measured by decades. The "BlackEnergy" malware that was used in Ukraine to exploit legacy protocols was developed over 20 years ago. While those developing the protocols 20 years ago may not have been able to foresee these consequences, modern operators should have, they bear the post-deployment responsibility where one must maintain their systems in a hostile environment. The system being secure when you bought it is not valid under Anticipatory Ethics. Critical Infrastructure operators have a continuous moral duty to examine their systems to harden them against emerging threats. The Colonial Pipeline operators failed to update their primitive VPN profiles, outdated IT software, and this is a failure to uphold the Post-Deployment Mandate. They allowed an account no longer in use to exist, which creates a vulnerability that paralyzed the entire East Coast fuel supply. Liability does not end at the time of installation; it persists until the artifact is no longer used.

6. Recommendations

To effectively halt easy unsophisticated cyber-attacks in ICS warfare, the reactive patching methodology must be replaced. Instead, a secure-by-design policy must be adopted that enforces security at the physical, network and device levels. This requires the re-engineering of the OT systems, using deterministic hardware constraints and physical validation to eliminate cyber threats.

6.1 Hardware-Enforced Unidirectional Security Gateways

The most resilient defense for critical network segments involves the replacement of software level firewalls with hardware-enforced Unidirectional Gateways, commonly called data diodes. Firewalls rely on software rules that can be bypassed with zero-day exploits or a misconfiguration, data diodes enforce security at OSI Layer 1 (Physical Layer) (Stouffer et al., 2015). The device contains a fiber-optic transmitter on the OT side and a receiver on the IT side, but they lack the physical hardware capabilities to transmit light in the opposite direction. This is a physics-based air gap that allows the monitoring of data to flow out of the enterprise network for analysis while rendering it impossible for any packet, command, or malware to enter the OT network. This breaks the TCP/IP protocol which requires a bi-directional three-way handshake (SYN, SYN-ACK, ACK). To overcome this the diode uses proxy servers. The source proxy on the OT side mimics a TCP endpoint terminating the connection and getting rid of the payload. It converts the payload into a one-way UDP stream or serial frame across the optical link. The IT side receives this stream and reconstructs a valid TCP session for the application. Implementing this at Level 3.5 DMZ makes sure that even if the entire corporate network is compromised by a ransomware, adversaries cannot send the packets that are needed to exploit PLCs on the plant floor.

6.2 Deep Packet Inspection (DPI) and Industrial Protocol Sanity Checking

Passive network monitoring is currently a simple flow analysis, which needs to be switched to a Deep Packet Inspection (DPI). Current intrusion detection systems (IDS) typically ignore ICS packet payloads, only scanning the IP headers. A comprehensive DPI solution must parse the structures of the Modbus, DNP3, and Ethernet/IP packets to validate the legitimacy of the commands (Stouffer et al., 2011). A Modbus TCP packet that contains "Function Code 5" (Write Single Coil) is a real, legitimate command structure, but if it targets a register that is associated with a safety mechanism important to turbine overspeed valves, it will represent a hostile act. WE recommend deploying Context-Aware firewalls that enforce Stateful Logic. These systems would maintain a digital model of a plant's operational state. If a plant is undergoing maintenance, a command to update firmware may be permitted, if the plant is running, the DPI engine would cryptographically sign and drop any packet that attempts to write to firmware or critical memory blocks.

6.3 Physics Based Anomaly Detection (P-BAD)

We recommend the installation of a Physics-Based Anomaly Detection (P-BAD) system as an additional validation layer for SCADA data. Current Intrusion Detection Systems (IDS) search for the signatures of known malware. Stuxnet worked by looking like a real driver update. Stuxnet can not defeat the laws of physics. A P-BAD system would use a mathematical model of the physical processes (utilizing differential equations that represent fluid dynamics, thermodynamics and electrical loads) (Giraldo et al., 2018). The system compares the incoming data from PLCs against the expected physical reality that would be derived from the model. As an example, if a PLC reports that a valve has been closed, the laws of physics would state the pressure in the pipe must then increase. If the valve is closed and pressure remains unchanged, the P-BAD system would flag it as a Discrepancy. This would indicate a sensor is broken or an attack like Stuxnet is spoofing the sensor values. By evaluating the physics involved in the situation and not just the code, zero-day attacks can be defeated even if they bypass all digital security layers.

6.4 Firmware Integrity and Root of Trust

Manufacturers and operators of IC and ICS systems must enforce a hardware-based Root of Trust (RoT) by using Trusted Platform Modules (TPM). The Triton attack was successful due to Triconex accepting a firmware update without a comprehensive evaluation of the update. We recommend a Secure Boot protocol where PLC bootloaders calculate SHA-256 hashes of operating firmware, then compares it against a value burned into the chip's One-Time Programmable (OTP) memory during its manufacturing (Stouffer et al., 2015). If the hashes do not match, this indicates a rootkit or some sort of modification, the processor must refuse to boot and trip a Safe State relay at the physical level. We advocate for operators to regularly dump the memory of their PLC's and compare the Ladder Logic bytecode against a perfect image stored on a closed system. A change in the bytecode would indicate a Logic Injection attack. This level of forensic analysis is the only way to detect a resident malware that does not leave a file but lives inside the controller's volatile memory.

6.5 Out-of-Band Analog Safety Loops

Recognizing the fragility of all software, we recommend the re-introduction of Out-of-Band analog safety loops for life-safety functions. The Sociotechnical Imperative reminds us that efficiency should not come at the cost of survivability. In the Oldsmar water plant attack, digital controls allowed the lye levels to be increased to possibly lethal amounts. Digital safety limits in software can be overwritten by attackers. A physical defense or analog limit switch that operates on a closed system would prevent this. A centrifugal controller on a turbine that cuts the steam supply if RPMs exceed a certain physical threshold, or a chemical feed pump that is physically incapable through the limitation of the size of its impeller disallowing pumping more than a safe maximum flow rate would solve this problem (CISA, 2021). Designing physical constraints for machines leaving them with no choice but to operate at safe limits ensures that if the adversary attains system level privileges over digital controls, kinetic consequences are physically impossible to achieve, preventing catastrophe.

7. Future Work

Continuing research must address the integration of Artificial Intelligence into ICS. We anticipate the existence of Self-Healing Grids where AI monitors the physics of the plant and isolates compromised segments instantly (Active Defense). However, this introduces the risk of "Adversarial AI," where malware is designed to trick defense AI into shutting down the grid by intentionally feeding it faulty data. Researching "Physics-Informed Machine Learning," which allows for commands to be validated against the laws of thermodynamics before execution is the next frontier of ICS security.

8. Conclusion

The mixing of IT and OT has militarized the infrastructure civilians use in their daily life. The case studies detailed in this paper demonstrate that the "Air Gap" is dead. These are not just technical glitches; they are acts of aggression that weaponize critical infrastructure against us. Looking at it from a technical perspective, relying on insecure design protocols like Modbus and a lack of firmware integrity checks in PLC, allow for a wide array of attacks. Ethically, targeting multi-purpose infrastructure is a violation of the principles of Distinction and Proportionality in Just War Theory. Cyber conflict now operating in a "Gray Zone" allows states to attack heating, water, and the fuel supplies of adversaries with impunity that would not be tolerated in traditional warfare. We conclude that the security of Critical Infrastructure is a moral imperative. The Sociotechnical Imperative demands systems designed to prioritize safety over the convenience of remote administration. Until the protection of SCADA systems are treated with the same seriousness as the protection of a nuclear missile silo, we remain at risk of a catastrophe designed by ourselves.

Ethics Declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI Tools Declaration: ChatGPT 5.1 for drafting and refinement. Human authors verified all content. Gemini 3.0 pro used for aiding in sourcing.

References

Assante, M. J. (2016). *Confirmation of a coordinated attack on the Ukrainian power grid*. SANS Industrial Control Systems Security Blog.

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

Brey, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. *NanoEthics*, 6(1), 1–13.

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Compromise of U.S. Water Treatment Facility*. Alert (AA21-042A). https://www.cisa.gov/uscert/ncas/alerts/aa21-042a

Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N. O., Sandberg, H., & Candell, R. (2018). A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Computing Surveys*, 51(4), 1–36.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494.

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

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS Institute.

Microsoft. (2021, September 21). *What is a DLL?* Microsoft Learn. https://learn.microsoft.com/en-us/troubleshoot/windows-client/setup-upgrade-and-drivers/dynamic-link-library

Miller, K.W., et al. (2011). Moral Responsibility for Computing Artifacts: 'The Rules'. *IT Professional*, 13(3), 57–59.

Morris, T., & Gao, W. (2013). Industrial control system traffic data sets for intrusion detection research. *International Conference on Critical Infrastructure Protection*, 65–78. Springer.

Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32.

Sanger, D. E., & Perlroth, N. (2021, May 8). Cyberattack Forces a Shutdown of a Top U.S. Pipeline. *The New York Times*.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Sobczak, B. (2019). *The Inside Story of the World's Most Dangerous Cyberattack*. E&E News. https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-cyberattack/

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. NIST. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Tavani, H.T. (2009). *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Wiley.

Turton, W., & Mehrotra, K. (2021, June 2). JBS Cyberattack: Hackers Demand Ransom in Bitcoin. *Bloomberg*.

Williams, T. J. (1992). *The Purdue Enterprise Reference Architecture: A Technical Guide for CIM Planning and Implementation*. Instrument Society of America.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.