Tech & AI Systems | Aug 4, 2026 | 8 min read | By Bryan White

# Two Decades of Cyber Conflict: The Journey from Web Disruption to ICS Exploitation

Ethics * Computing * Urban Environment

## Introduction: The Shifting Paradigm of Infrastructural Conflict

The virtualization of critical civilian infrastructure has fundamentally altered the calculus of international conflict, allowing adversarial states and proxy groups to disrupt the foundational operations of a society without firing a kinetic shot[1]. Over the past two decades, the evolution of state-sponsored cyber operations has progressed from volumetric Distributed Denial of Service (DDoS) floods targeting public web portals -- pioneered during the 2007 cyberattacks against Estonia -- to architecturally aware intrusions targeting the Programmable Logic Controllers (PLCs) that govern physical water, hydrological distribution, and energy infrastructure[2][3][4].

This report examines that two-decade trajectory, analyzing the network mechanics of the 2007 Estonian campaign, the legal thresholds of armed force established in the Tallinn Manual, the forensic anatomy of recent Iranian-linked intrusions into Unitronics PCOM industrial controllers, and the structural remediation frameworks required to restore defense-in-depth across the Purdue Enterprise Reference Architecture.

## The 2007 Estonian Precedent and the Tallinn Manual

In April and May 2007, following a diplomatic dispute over the relocation of the Soviet-era Bronze Soldier of Tallinn memorial, Estonia endured a 22-day digital siege widely recognized as the first major state-aligned cyber campaign[2]. Initial waves beginning April 27 relied on ICMP ping floods, malformed HTTP queries, and UDP packet floods, rapidly escalating into coordinated global botnet assaults mobilizing 1 to 2 million compromised machines across 175 jurisdictions[1][2][5]. Traffic analysis by Arbor Networks' Security Engineering and Response Team (ASERT) recorded sustained attack streams reaching 90 Mbps for up to ten hours per wave -- sufficient in 2007 to saturate parliamentary email servers, overload Domain Name System (DNS) resolvers, and force Estonia's largest commercial bank, Hansabank, offline on May 10[2][5].

To preserve domestic banking and government communications, the Estonian Computer Emergency Response Team (CERT-EE) implemented Border Gateway Protocol (BGP) blackholing to sever external international IP routes[1][2]. Although the attacks synchronized with Russian political dates (such as May 9 Victory Day) and adapted dynamically to countermeasures, decentralized botnet routing preserved plausible deniability and prevented definitive legal attribution[2][1].

In response, NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008, convening legal scholars to draft the Tallinn Manual on how international law governs cyber warfare[2]. Under Rules 80 and 82 of Tallinn

Manual 2.0, cyber operations during armed conflict are bound by International Humanitarian Law prohibitions against targeting civilian survival infrastructure, and an independent cyber operation constitutes a "use of force" or "armed attack" under UN Charter Article 51 when its scale and effects match kinetic force[6][7]. Under the "loss of functionality" doctrine endorsed by states such as Germany, disabling an Industrial Control System (ICS) such that physical component replacement or manual system reinstallation is required crosses the threshold of physical destruction, alongside territorial "due diligence" obligations[6][8]. Consequently, modern threat actors deliberately calibrate gray-zone OT disruptions to inflict economic and psychological costs just below the threshold of kinetic military retaliation[1][4].

## Asymmetric OT Doctrine and the PCOM Protocol Vulnerability

Following heightened Middle Eastern geopolitical tensions beginning in late 2023 and persisting into 2026, Iranian-affiliated threat actors expanded from long-term espionage toward direct disruption of Western operational technology across water and energy utilities[3][4][9].

| Threat Group Designation | | Affiliation | | Primary Targets | | Typical Operational Tactics |

| CyberAv3ngers | | Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC) | | Water/Wastewater, Energy, Manufacturing, specifically targeting Israeli-manufactured equipment | | Exploitation of default credentials on exposed PLCs, HMIs defacement, process disruption |

| MuddyWater | | Ministry of Intelligence and Security (MOIS) | | Government, Defense, Telecommunications, Energy | | Living-off-the-land techniques (PowerShell, WMI), lateral movement, long-term persistence |

Operating under the IRGC-CEC, CyberAv3ngers systematically compromised municipal water and wastewater utilities -- including the Aliquippa Municipal Water Authority in Pennsylvania and regional pumping stations in County Mayo, Ireland -- causing simultaneous loss of view and loss of control that forced operators onto manual bypass[4]. Rather than deploying zero-day malware against public health or wastewater monitoring systems, the attackers exploited Unitronics Vision series PLCs exposed directly to the public internet on TCP port 20256[4][10][11].

Unitronics silicon controllers communicate with engineering workstations via the proprietary PCOM (Programmable Controller Communication) protocol encapsulated over TCP/IP[4][11][12]. PCOM operates in two request-response modes: PCOM ASCII (delimited by / request and /a response magic bytes for homogeneous data) and PCOM Binary (prefixed by /_OPLC for heterogeneous memory operations)[11]. Once connected, hexadecimal opcodes grant complete read/write authority over PLC memory and ladder logic[11].

| Function Code (Hexadecimal) | | Protocol Action Description |

| 0x01 / 0x81 | | Read Memory |

| 0x02 / 0x82 | | Check Password |

| 0x0C / 0x8C | | Get PLC Name |

| 0x10 / 0x90 | | Find Resource |

| 0x41 / 0xC1 | | Write Memory |

| 0x42 / 0xC2 | | Reset Upload Password |

| 0x4D / 0xCD | | Read Operand |

Because legacy industrial protocols lack high-entropy cryptographic session authentication, Unitronics PLCs relied on an optional application-level password initialized by default to "1111" (CWE-1188)[4][10][13]. Using Shodan and Censys queries accelerated by large language models, actors scanned industrial ports, authenticated with "1111", overwrote pump logic, and defaced Human-Machine Interfaces (HMIs)[4].

| Associated TCP/UDP Port | | Industrial Protocol | | Target Device/Function |

| TCP 20256 | | Unitronics PCOM | | Unitronics Vision/Samba PLCs |

| TCP 502 | | Modbus | | Generic ICS process control |

| TCP 44818 | | EtherNet/IP | | Rockwell Automation / Allen-Bradley PLCs |

| TCP 4840 | | OPC UA | | Cross-vendor ICS communication |

| UDP 47808 | | BACnet | | Building and facility automation |

| TCP 20000 | | DNP3 | | Electric utility SCADA protocol |

## Architectural Atrophy in the Purdue Model and CISA Remediations

The exposure of Level 1 PLCs directly to the internet reflects the widespread erosion of the Purdue Enterprise Reference Architecture (PERA), which segments industrial networks into hierarchical trust zones separated by a Level 3.5 Industrial Demilitarized Zone (DMZ)[14][15].

| Purdue Model Level | | Zone Designation | | Description of Components and Functions |

| Level 5 | | Enterprise Network | | Corporate IT functions, internet connectivity, email servers, and broad enterprise resource planning (ERP) systems. |

| Level 4 | | Business Logistics | | Site-specific business systems, production scheduling, and local IT operations. |

| Level 3.5 | | Industrial DMZ | | The Demilitarized Zone. A secure buffer housing firewalls, jump servers, and proxies to prevent direct communication between IT and OT. |

| Level 3 | | Site Operations | | Manufacturing execution systems (MES), data historians, and site-wide OT management. The highest level of the OT network. |

| Level 2 | | Supervisory Control | | Human-Machine Interfaces (HMIs) and distributed control systems monitoring specific local processes. |

| Level 1 | | Basic Control | | Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) executing automated process logic. |

| Level 0 | | Physical Process | | The physical equipment: sensors, actuators,

pumps, and valves interacting with the real world. |

Rapid IT/OT convergence, cloud-connected IIoT telemetry bypassing Level 3.5, and unmonitored vendor remote-maintenance links have collapsed this segmentation across municipal utilities[4][10][15]. To restore resilience in alignment with CISA's updated Cross-Sector Cybersecurity Performance Goals (CPGs 2.0, released December 2025) and Joint Advisory AA23-335A, critical infrastructure operators must implement five core engineering controls[4][16][17]:

* Eliminate Internet-Facing OT Assets: Remove all PLCs and HMIs from public IP space and require multi-factor VPN authentication terminating inside a Level 3.5 jump host[4][9].

* Eradicate Default Credentials: Mandate unique, high-entropy passwords prior to commissioning any controller[4].

* Enforce Bidirectional Boundary Filtering: Apply default-deny firewall rules blocking inbound and outbound traffic on industrial ports (TCP 20256, 502, 44818, 4840, 20000; UDP 47808) to prevent C2 beaconing[4][15].

* Deploy Behavioral Anomaly Detection: Use statistical network baselining to detect living-off-the-land lateral movement (PowerShell, WMI) by threat actors in OT environments[15][17].

* Install Unidirectional Data Diodes: Enforce hardware-level one-way optical replication from Level 3 historians to Level 4 enterprise analytics, physically preventing remote command injection[18].

## Conclusion: Defending the Cyber-Physical Frontier

From the 90 Mbps botnet floods against Estonia in 2007 to the manipulation of municipal water PLCs via exposed PCOM opcodes, cyber conflict has matured into a persistent instrument of gray-zone coercion. Because legacy industrial controllers operate for decades without native cryptographic authentication, securing civilian lifelines requires combining strict Purdue Model network segmentation, hardware data diodes, and CISA CPG baseline hygiene with enforceable international legal norms under the Tallinn framework -- principles tested continuously across 2022-2026 Eurasian and Middle Eastern cyber-OT campaigns.[19]

Updates... (Nov 21, 2026): Replaced commercial cybersecurity vendor glossaries and third-party CVE mirrors with foundational peer-reviewed and federal standards -- including Williams (1994) on the Purdue Enterprise Reference Architecture, NIST SP 800-82 Rev. 3 (Sep 28, 2023), NVD CVE-2023-6448, and Nardone et al. (2025) -- added specific publication dates across all 19 references, and aligned inline citations 1-to-1.

## References & Primary Sources

* [1] NATO Strategic Communications Centre of Excellence (2019). Hybrid Threats: 2007 Cyber Attacks on Estonia. -- https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

* [2] Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. NATO Cooperative Cyber Defence Centre of Excellence

(CCDCOE). -- https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

* [3] Cybersecurity Dive (Jul 23, 2026). CISA, FBI warn that Iran-linked hackers are expanding target set for water, energy sectors. -- https://www.cybersecuritydive.com/news/cisa-fbi-iran-hackers-target-water-energy/826025/

* [4] CISA, FBI, NSA, EPA, & Israel National Cyber Directorate (Dec 1, 2023; updated Dec 18, 2024). IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (Advisory AA23-335A). -- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

* [5] Laasme, H. (2011). Estonia: Cyber Window into the Future of NATO. Joint Force Quarterly, (63), NDU Press. -- https://www.cicerofoundation.org/wp-content/uploads/Laasme_-Estonia_NATO_Cyber_-Strategy.pdf

* [6] NATO CCDCOE (Jun 2026). International Legal Perspectives on Cyber Operations: A Common Understanding. -- https://ccdcoe.org/uploads/2026/06/International_Legal_Perspectives_on_Cyber_Operations.pdf

* [7] Schmitt, M. N. (Ed.) (Feb 2, 2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. -- https://doi.org/10.1017/9781316822524

* [8] Just Security (Mar 10, 2021). Germany's Positions on International Law in Cyberspace Part II. -- https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/

* [9] CloudSEK Threat Intelligence (Mar 6, 2026). AI, the Iran-US Conflict, and the Threat to US Critical Infrastructure. -- https://www.cloudsek.com/blog/ai-the-iran-us-conflict-and-the-threat-to-us-critical-infrastructure

* [10] Net Sec Group (Dec 1, 2023). The County Mayo Water Hack: How a Default Password Took 180 Homes Offline. -- https://netsecgroup.io/guides/county-mayo-water-hack-unitronics

* [11] Claroty Team82 (Aug 7, 2024). From Exploits to Forensics: Unraveling the Unitronics Attack. -- https://claroty.com/team82/research/from-exploits-to-forensics-unraveling-the-unitronics-attack

* [12] Nardone, R., et al. (2025). Challenges and Cybersecurity Attacks in Operational Technology (OT) and Industrial Control Systems (ICS). Apress Pocket Guides. -- https://doi.org/10.1007/979-8-8688-2016-8_3

* [13] NIST National Vulnerability Database (Dec 11, 2023). CVE-2023-6448 Detail: Unitronics Vision PLC and HMI Insecure Default Password Vulnerability. -- https://nvd.nist.gov/vuln/detail/CVE-2023-6448

* [14] Williams, T. J. (Sep 1994). The Purdue Enterprise Reference Architecture. Computers in Industry, 24(2-3), 141-158. -- https://doi.org/10.1016/0166-3615(94)90017-5

* [15] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (Sep 28, 2023). Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. --

https://doi.org/10.6028/NIST.SP.800-82r3

* [16] CISA (Nov 29, 2023). Cross-Sector Cybersecurity Performance Goals (CPGs) & Water and Wastewater Sector Guidance. -- https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

* [17] CISA (Dec 2025). Cross-Sector Cybersecurity Performance Goals (CPGs) 2.0. -- https://www.cisa.gov/sites/default/files/2025-12/CPG_Report_2.0_508c.pdf

* [18] U.S. Cybersecurity Magazine (Jun 25, 2026). The Evolving Threat: Iranian and Nation-State APT Cyber Operations -- Present and Future. -- https://www.uscybersecurity.net/csmag/the-evolving-threat-iranian-and-nation-state-apt-cyber-operations-present-and-future/

* [19] Krasznay, C. (Sep 1, 2026). Cyber Resilience Under Fire: OT Systems and Critical Infrastructure in the Russia-Ukraine War. Land Forces Academy Review. -- https://doi.org/10.2478/raft-2026-0028