waterfall

South Asia Clean Energy Forum (SACEF) 2024

Trends in the ICS/OT threat landscape & relevancy for the clean energy transition

LinkedIn

Rees Machtemes, P.Eng.
Director of Industrial Security

About Waterfall Security

2007
Founded

>1000
Sites

>20
Verticals

6
Global Sales & Ops Hubs

14
Published Patents

Leading the world's OT unidirectional gateway market with superior solutions, worldwide presence, and proven track record of success

Key Sectors:

Power | Oil & Gas | Rails | Facilities | Water | Manufacturing | Government

waterfall

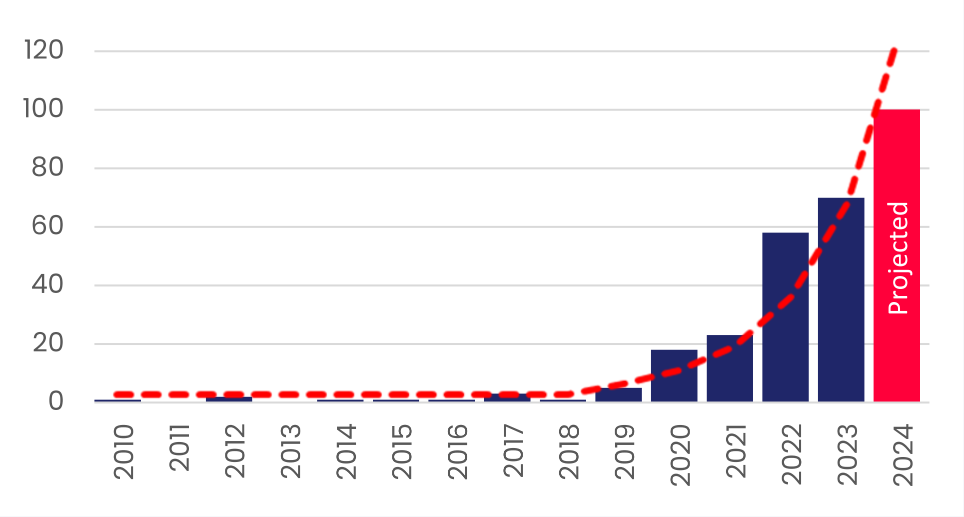
Threat Report – OT Cyber Attacks with Physical Impacts

Deliberate Attacks –
not equipment failures, nor errors or omissions

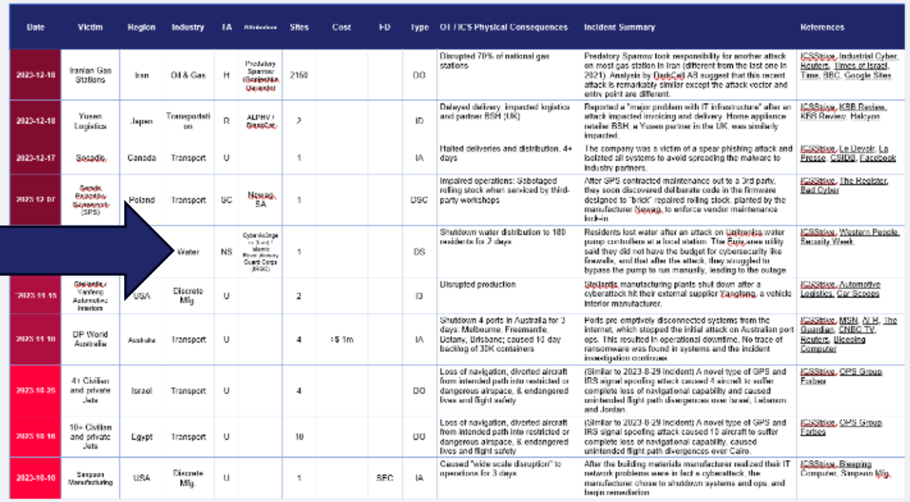
With Physical Consequences –
not near misses, not data theft only, not crippled IT but OT kept working

In the Focus Industries –
building automation, manufacturing, heavy industry and critical industrial infrastructure

In the Public Record –
no confidential disclosures



Attacks with physical consequences



Date	Victim	Region	Industry	IA	[illegible]	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-12-18	Iranian Gas Stations	Iran	Oil & Gas	H	Predatory Sparrow (Gonjeshke Darande)	2150			DO	Disrupted 70% of national gas stations	Predatory Sparrow took responsibility for another attack on most gas station in Iran (different from the last one in 2021). Analysis by DarkCell AB suggest that this recent attack is remarkably similar except the attack vector and entry point are different.	ICSStrive, Industrial Cyber, Reuters, Times of Israel, Time, BBC, Google Sites
2023-12-18	Yusen Logistics	Japan	Transportation	R	ALPHV / BlackCat	2			ID	Delayed delivery, impacted logistics and partner BSH (UK)	Reported a "major problem with IT infrastructure" after an attack impacted invoicing and delivery. Home appliance retailer BSH, a Yusen partner in the UK, was similarly impacted.	ICSStrive, KBB Review, KBB Review, Halcyon
2023-12-17	Sosadis	Canada	Transport	U		1			IA	Halted deliveries and distribution, 4+ days	The company was a victim of a spear phishing attack and isolated all systems to avoid spreading the malware to industry partners.	ICSStrive, Le Devoir, La Presse, CSIDB, Facebook
2023-12-07	[illegible] (SPS)	Poland	Transport	SC	Newag SA	1			DSC	Impaired operations: Sabotaged rolling stock when serviced by third-party workshops	After SPS contracted maintenance out to a 3rd party, they soon discovered deliberate code in the firmware designed to "brick" repaired rolling stock, planted by the manufacturer Newag, to enforce vendor maintenance lock-in	ICSStrive, The Register, Bad Cyber
			Water	NS	CyberAv3ngers / Iranian Islamic Revolutionary Guard Corps (IRGC)	1			DS	Shutdown water distribution to 180 residents for 2 days	Residents lost water after an attack on Unitronics water pump controllers at a local station. The Erie-area utility said they did not have the budget for cybersecurity like firewalls, and that after the attack, they struggled to bypass the pump to run manually, leading to the outage	ICSStrive, Western People, Security Week
2023-11-15	Stellantis / Yanfeng Automotive Interiors	USA	Discrete Mfg	U		2			ID	Disrupted production	Stellantis manufacturing plants shut down after a cyberattack hit their external supplier Yanfeng, a vehicle interior manufacturer.	ICSStrive, Automotive Logistics, Car Scoops
2023-11-10	DP World Australia	Australia	Transport	U		4	>$ 1m		IA	Shutdown 4 ports in Australia for 3 days: Melbourne, Freemantle, Botany, Brisbane; caused 10 day backlog of 30K containers	Ports pre-emptively disconnected systems from the internet, which stopped the initial attack on Australian port ops. This resulted in operational downtime. No trace of ransomware was found in systems and the incident investigation continues	ICSStrive, MSN, AFR, The Guardian, CNBC TV, Reuters, Bleeping Computer
2023-10-25	4+ Civilian and private Jets	Israel	Transport	U		4			DO	Loss of navigation, diverted aircraft from intended path into restricted or dangerous airspace, & endangered lives and flight safety	(Similar to 2023-8-29 incident) A novel type of GPS and IRS signal spoofing attack caused 4 aircraft to suffer complete loss of navigational capability and caused unintended flight path divergences over Israel, Lebanon and Jordan.	ICSStrive, OPS Group, Forbes
2023-10-16	10+ Civilian and private Jets	Egypt	Transport	U		10			DO	Loss of navigation, diverted aircraft from intended path into restricted or dangerous airspace, & endangered lives and flight safety	(Similar to 2023-8-29 incident) A novel type of GPS and IRS signal spoofing attack caused 10 aircraft to suffer complete loss of navigational capability, caused unintended flight path divergences over Cairo.	ICSStrive, OPS Group, Forbes
2023-10-10	Simpson Manufacturing	USA	Discrete Mfg.	U		1		SEC	IA	Caused "wide scale disruption" to operations for 3 days	After the building materials manufacturer realized their IT network problems were in fact a cyberattack, the manufacturer chose to shutdown systems and ops, and begin remediation	ICSStrive, Bleeping Computer, Simpson Mfg.

The complete data set is included in Appendix A, with links you can follow to read the original reports yourself.

waterfall

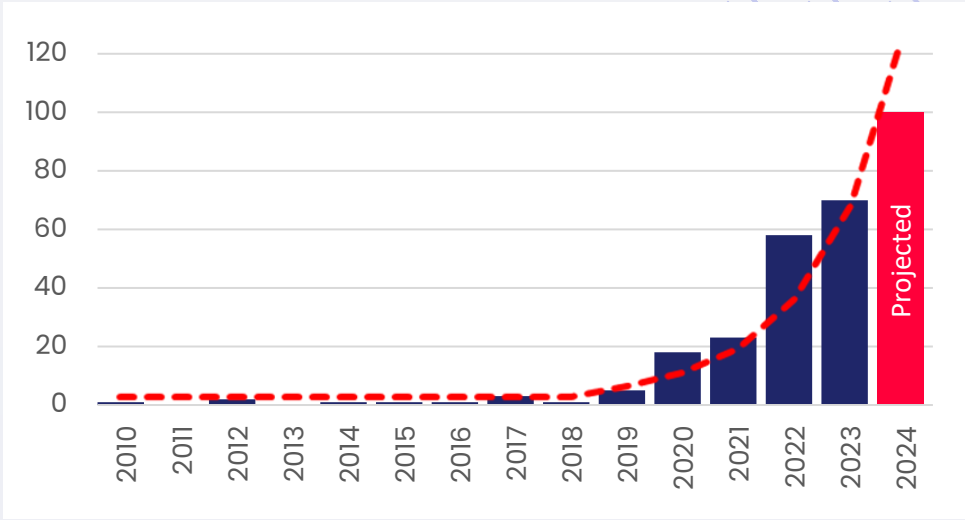
Threat Report – OT Cyber Attacks with Physical Impacts

Exponential Growth –
nearly doubling every year – 68 attacks in 2023 impacting more than 500 sites

Ransomware – most attacks
most sophisticated use nation-state-grade TTPs

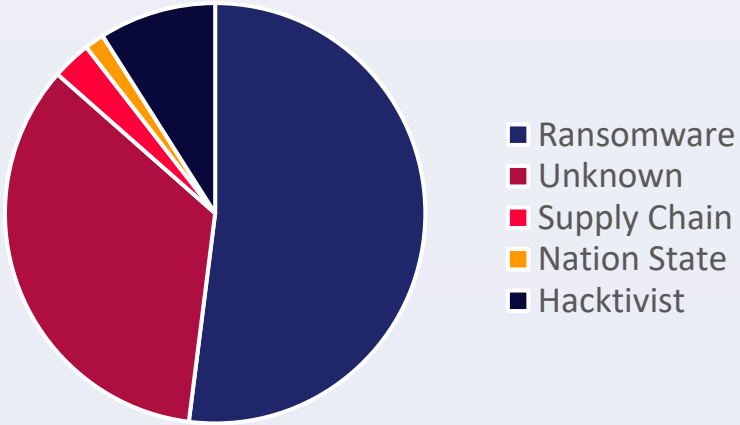
Nation-States – E.g. Volt Typhoon, Sandworm, etc.

Hacktivists – target critical infrastructures



Attacks with physical consequences

Threat Actor Mix (2010 – 2023 YE):



waterfall-security.com/2024-threat-report

waterfall

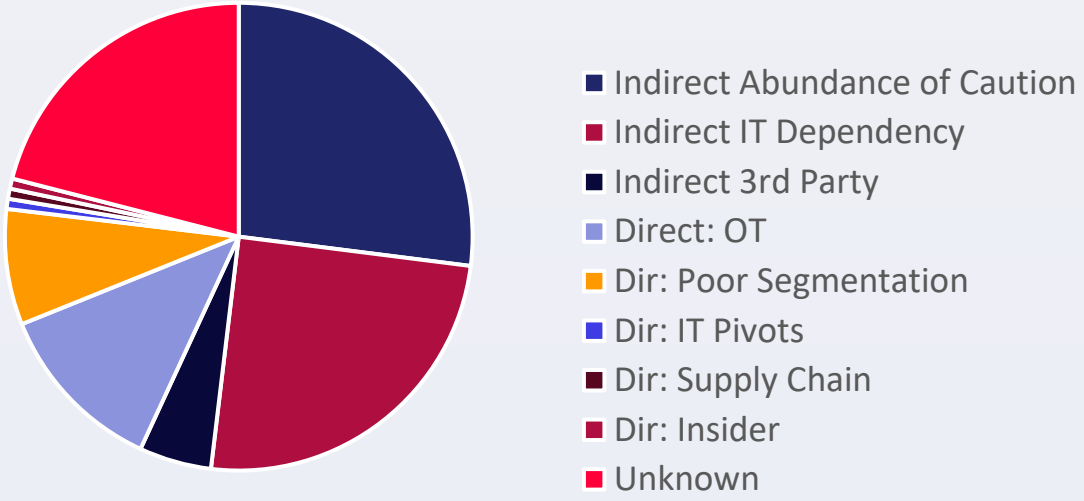
Known Attack Types, from 2010 to present

Key Takeaway: Two-thirds (2/3) of known attacks *indirectly* impact OT

"Abundance of Caution" – 35% shut down pre-emptively to protect OT

Dependencies – 31% shut down as IT systems & 3rd parties are essential to operations

Target OT Directly – *Remaining* 28% manipulate, encrypt or impair OT (various ways)



The data shows: Almost all attributable attacks directly targeting OT are perpetrated by hacktivists & nation states

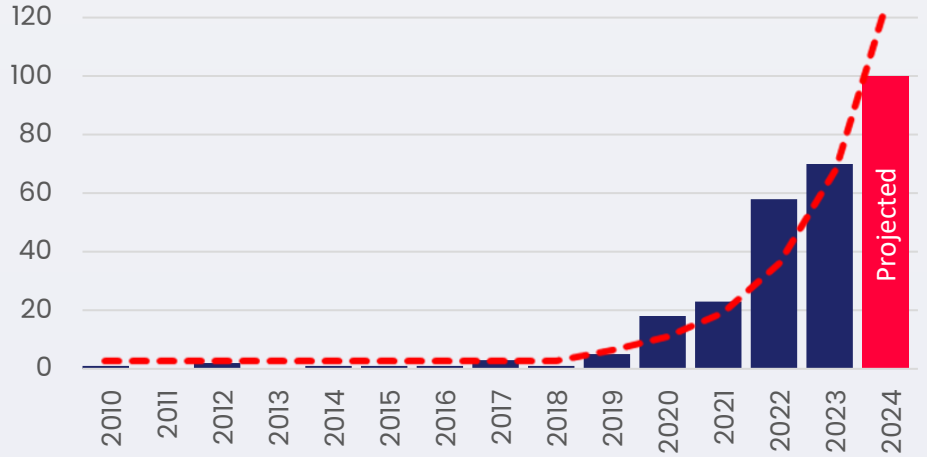
Relevancy to South Asia & Clean Energy Transition

Cyber Attacks – Now A Global, Pervasive Problem
physical consequences continue to increase, as do the number of affected sites and costs of compromise

Nation States and Ransomware – like Volt Typhoon
target critical infrastructures and cannot be ignored

Modern ICS/OT design for the clean energy transition–
Can not afford to spend the bulk of precious financial resources in cyber incident response and recovery, or suffer costly shutdowns, safety & environ. impacts

CIE and Engineering Grade Protections –
powerful new ways of looking at OT security design with strong solutions that were previously overlooked



rees.machtemes@waterfall-security.com
https://www.linkedin.com/in/reeskm/

LinkedIn

waterfall-security.com/2024-threat-report

waterfall