2026

2028+

DRAGOS

Office for
Nuclear Regulation

EMERGING CYBERSECURITY AND INFORMATION ASSURANCE THREATS & RISKS FOR THE CIVIL NUCLEAR SECTOR

Abstract

Dutyholders in the civil nuclear sector conduct complex operations that carry potentially catastrophic consequences. As they become increasingly attractive targets for adversaries, it is essential for them to continue to strategically implement controls to ensure safe and secure operations. Effective leadership and independent assurance are key to managing the sector's current and emerging risks.

Executives and decision-makers in industry, government, and academia can use this executive summary and the accompanying whitepaper to guide their risk management. Whereas already present threats and risks will mainly remain relevant, technology and societal changes will introduce new challenges for dutyholders in the UK and worldwide.

Dragos examined emerging threats and risks to the civil nuclear sector over a three-year timeline and beyond. This report characterises each threat or risk by its ability to impact industrial operations significantly. Depending on the dutyholder and use of technology, some risks might be more relevant than others.

The Office for Nuclear Regulation and Dragos collaborated on this whitepaper to provide unique insight into emerging cybersecurity threats and risks.

Office for
Nuclear Regulation

DRAGOS

Today’s Threats & Risks to Civil Nuclear

2025

Conflict-Driven Cyberattacks

Geopolitical conflicts affect the cybersecurity landscape. Adversaries target critical infrastructure in support of hybrid warfare. This includes attacking strategic targets and maintaining a foothold.

Espionage

Espionage can occur from economic and geopolitical interests. Dutyholders have access to sensitive nuclear information and other information of economic or political value. Adversaries will use cyberattacks to perform espionage.

Hacktivism and Vandalism

As a consequence of geopolitical conflicts hacktivism has seen a rise in 2024. Organisations in critical sectors or easy targets have seen defacements and disruption.

Defence Evasion Techniques

Cybercriminals have developed new techniques for gaining and maintaining access to target environments. Detecting adversaries using tools and technology already present on target systems continues to be difficult.

Ransomware Economy

Ransomware has moved beyond single cybercrime operations. Ransomware-as-a-service professionalisation and business cases make these a credible threat to any dutyholder.

Data Leaks and Unprotected Data

Adversaries gather data from data leaks and unprotected data storage endpoints for use in subsequent attacks or as part of extortion. Dutyholders need to ensure appropriate data governance.

Threats & Risks to Civil Nuclear

2026

2026-A
Convergence & Connectivity

2026-B
Espionage

2026-C
Ransomware

2026-D
Deepfake & Initial Compromise

2026-E
Artificial Intelligence

2027

2027-A
Skills & Workforce

2027-B
Misinformation

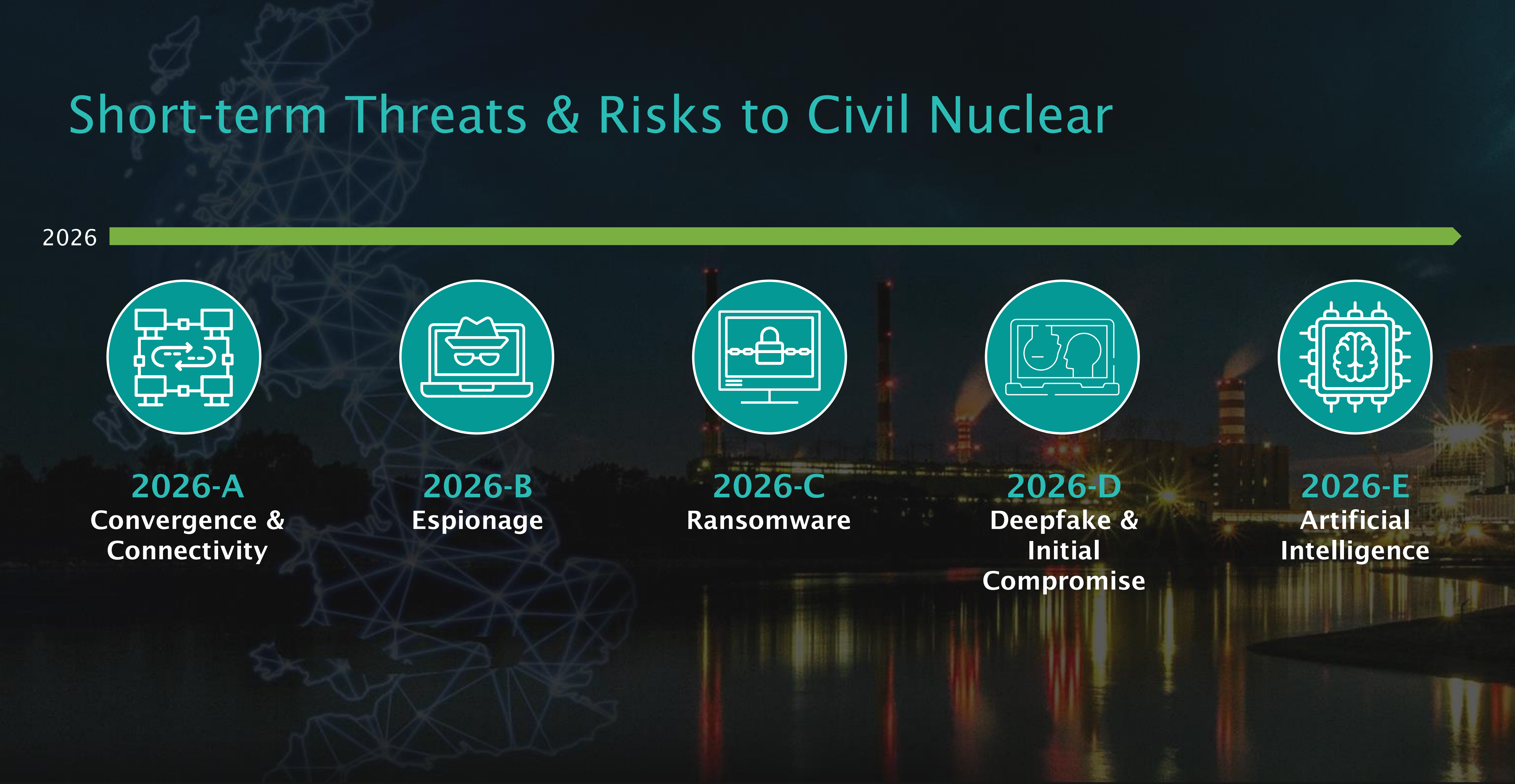
2027-C
Universal OT Malware

2028

2028-A
Quantum Cryptography

2028-B
Integrity & Sourcing

Short-term Threats & Risks to Civil Nuclear



2026

2026-A
Convergence & Connectivity

2026-B
Espionage

2026-C
Ransomware

2026-D
Deepfake & Initial Compromise

2026-E
Artificial Intelligence

2026

Threats and Risks

2026-A
Convergence and Connectivity

The advantages of cloud, virtualisation, Internet-of-Things (IoT), and similar technologies will increase the demand for wider adoption in civil nuclear. Greater connectivity means more cyber-attack entry points, supply chain breach opportunities, and easier malware propagation or lateral movement. The further convergence of technology, shifting OT environments to single-solution architectures will enable adversaries to codify their knowledge and scale attacks with cross-industry OT malware, such as PIPEDREAM.

2026-B
Espionage

State-sponsored adversaries are interested in exfiltrating advanced leading-edge research, such as the work on Advanced and Small Modular Reactors and fusion energy development in the UK. Nuclear is an increasingly strategic target for state-sponsored research, reconnaissance, and pre-positioning activity by threat groups. Operational data exfiltrated from OT networks may provide the adversary with crucial intelligence to aid in follow-up offensive tool development or attacks against OT networks. Modern internet-enabled devices, like wearables, provide adversaries with additional techniques.

Recommendations

2026

- **Identify and classify** vital information, such as sensitive nuclear information, research, and operational data, likely to be targeted for theft or exfiltration. This also applies to the supply chain.
- Employ **stringent access controls and encryption** on data, including any backups or drafts.

- **Monitor cross-zone communications** between IT and OT networks and utilise behavioural detections engineered to identify the latest applicable tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs).
- **Establish choke points** for access and data flow.

- **Operationalise a technical community** as a visibility and collective defence programme centred on the capability of **sharing OT threat intelligence** through recognised partnerships (e.g., CISP).
- **Anonymisation** protects the individual but allows community defenders to provide trusted insights and prioritise alerts.

2026

Threats and Risks

2026-C Ransomware

Cybercriminals will continue to refine their tactics, techniques, and procedures (TTPs) to remain lucrative. Ransomware-as-a-Service (RaaS) has become the dominant operating business model, with almost all the top ransomware strains operating this way. Integrating AI features can amplify RaaS capabilities, making attacks more targeted, efficient, and harder to detect.

2026-D Initial Compromise & Deepfake

Initial Access is a prerequisite to any cyber-attack. Adversaries use phishing, social engineering, supply chain, and similar techniques to gain an initial foothold within a network as they strive to escalate privileges, expand access, and gain persistence. AI chatbots and deepfake technology can enhance the effectiveness of phishing and social engineering. Supply-chain attacks have affected the civil nuclear industry in the past and will continue to provide a vector into otherwise heavily secured environments.

Recommendations

2026

- Organisations need to have a **defence-in-depth** approach to counter evolving ransomware.
- Effective implementations of **security fundamentals** paired with the ability to detect and recover from ransomware will become increasingly important.
- Organisations need a **defensible architecture** that includes controls against ransomware and cybercriminals.

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

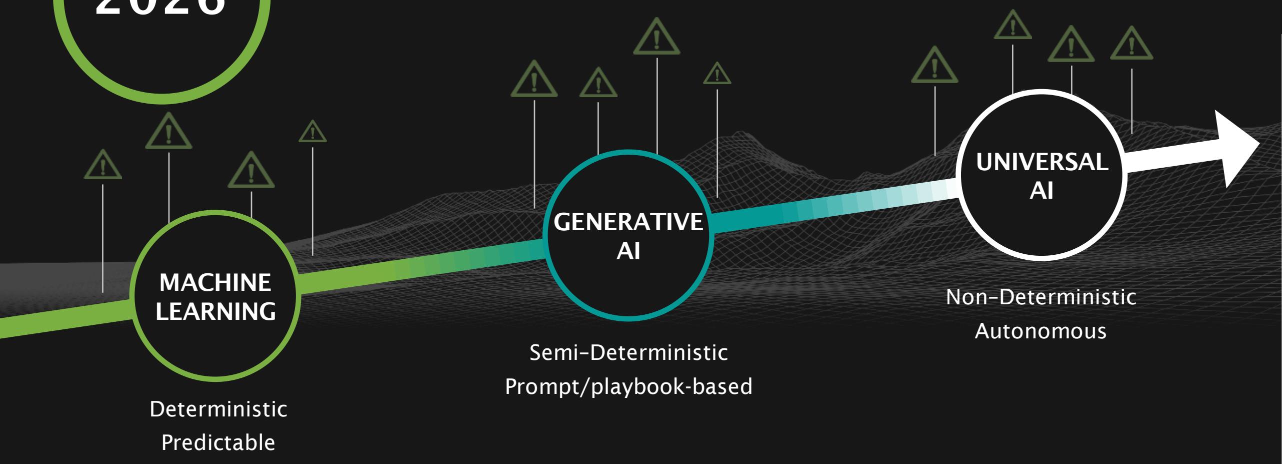
SANS 5

01	ICS Incident Response Plan
02	Defensible Architecture
03	ICS Network Monitoring Visibility
04	Secure Remote Access
05	Risk-based Vulnerability Management

- Initial compromise often uses human weaknesses. **Awareness** is one of the most effective countermeasures.
- Develop and document processes for **confirming identities**, as video and voice calls may no longer be trusted for confirmation.
- New phishing methods, like QR or multifactor bombing, need **continuous control adjustment**.

2026

Threats and Risks



2026-E – Artificial Intelligence

The term AI is ambiguous. It is not just one technology but a collection of technologies. Machine Learning has direct applicability in today's civil nuclear sector solving problems, designed to excel at specific tasks such as classification or predictive modeling. Generative AI can create new content, including pictures, texts, and potentially training and operations documents relevant to dutyholders. However, AI enabled cyber security solutions and tools are expected to increase the opportunities for adversaries to compromise assets within the sector.

Many AI models have intermediate layers that process input data before producing an output. These layers are "hidden" because how they transform and extract patterns from data is not directly visible or interpretable to users. Hidden layers are a technical challenge to be solved before the adoption of AI for making critical decisions. Dependency on third-party AI models and platforms makes supply chains increasingly attractive targets.

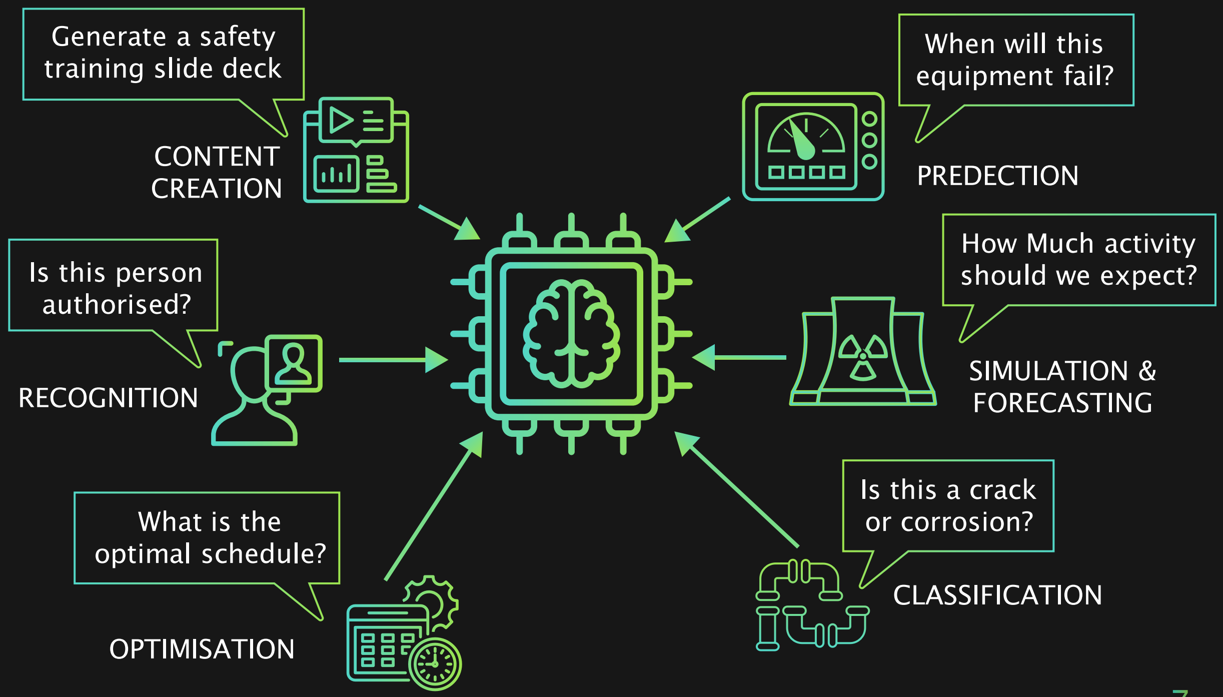
The final stage of universal AI is too far in the future to influence dutyholders. The lack of transparency and reasoning, in combination with increased data processing associated with generative AI, introduces new risks. Universal AI or Artificial General Intelligence (AGI) is beyond the 3-year timeline.

Recommendations

2026

- Organisations planning to use AI should conduct a careful trade-off analysis of the risk and benefits.
- Tailor training programs to all levels of organisations, emphasising AI's impact on nuclear security.
- Enhance trust/confidence in AI decisions by establishing clear chains of responsibility.

AI Use Cases in Nuclear


Generate a safety training slide deck
CONTENT CREATION
When will this equipment fail?
PREDECTION
Is this person authorised?
RECOGNITION
How Much activity should we expect?
SIMULATION & FORECASTING
What is the optimal schedule?
OPTIMISATION
Is this a crack or corrosion?
CLASSIFICATION

Mid-/Long-term Threats & Risks to Civil Nuclear

2027

2027-A
Skills & Workforce

2027-B
Misinformation

2027-C
Universal OT Malware

2028

2028-A
Quantum Cryptography

2028-B
Integrity & Sourcing

2026

Threats and Risks

2027-A
Skills and Workforce

The civil nuclear industry will encounter a shortage of qualified workforce that can implement, operate, and manage systems and components. Industry veterans retire, and the new workforce lacks knowledge of legacy systems. This likely leads to a higher reliance on third parties, consultants, and vendors. Vetting third parties is already a challenge today. Relying on third parties due to a lack of workforce can introduce critical dependencies and risks of an uncontrolled insider. Increased use of automation and AI can also impact the effectiveness and knowledge of the workforce.

2027-B
Misinformation

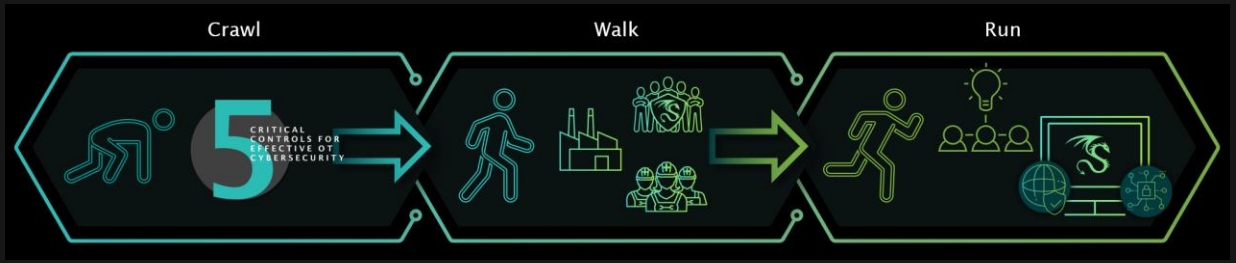
A misinformation campaign could severely impact the civil nuclear industry's reputation, workforce, and morale. False narratives, AI-generated deepfakes, or manipulated data could amplify fears, erode public trust, and fuel anti-nuclear sentiment. This could delay projects, disrupt operations, and undermine confidence in the civil nuclear industry and its operators, hindering progress toward energy goals.

FAKE

Recommendations

2026

- **Identify** the **required cybersecurity skills** within the nuclear industry while considering recognised professional bodies and certification.
- **Encourage existing experts** to share and document their knowledge.
- **Cross-skill new workforce** for the intricacies of civil nuclear and capability to handle legacy systems.
- Take a **crawl-walk-run approach** and start training today.



- Organisations should continuously **monitor the media** to react to information spread maliciously quickly.
- The civil nuclear industry should encourage **information sharing**, especially if misinformation applies to a larger audience.
- Organisations should **educate the workforce** about the potential impact of misinformation and the impact on their operations.

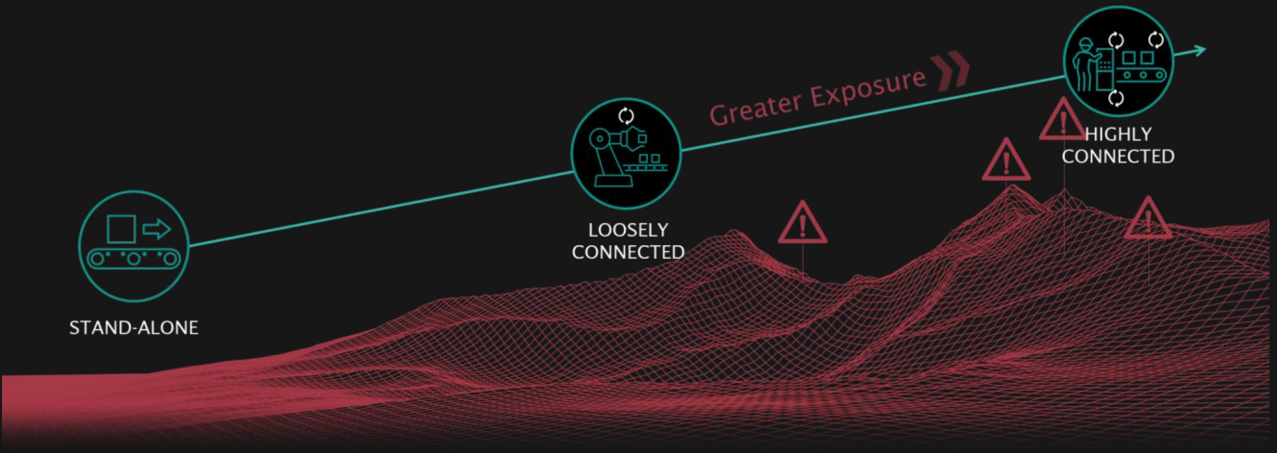
Threats and Risks

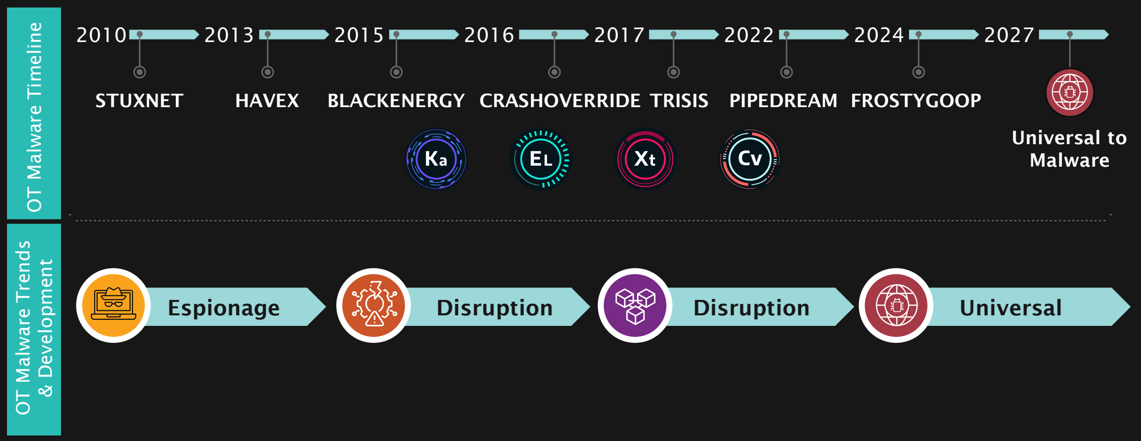
Recommendations

2027-C
Universal OT Malware

Execution of malicious code in industrial environments will continue to pose a threat to organisations. While such malware was highly specific in the past, adversaries have moved to modular and universal code that can impact many control components and industries. Scalability and repeatability have become themes that will enable new, faster compromises. Analysis reveals that adversaries seek to achieve impacts far greater than immediate disruption by undermining fundamental aspects of process integrity. Loss of integrity or availability in the control domain poses a significant risk, especially in the nuclear sector.

- Organisations need to establish a **defensible architecture** hindering malware use and lateral movement.
- Industrial environments need to **monitor network traffic** with OT-protocol-aware technologies.
- Establish signature and **heuristic antimalware scanning** on components supporting such tools.
- **OT-specific threat intelligence** can provide early information on emerging threats.
- Leverage behaviour-based detections instead of signatures
- Consider application allowlisting to **prevent unauthorised code execution**. Anomalies are rare, especially in nuclear environments, and they provide a good detection approach.
- Establish a code-vetting program for new or unknown code. **Enforce digital signatures** for code.




OT Malware Timeline

2010 STUXNET

2013 HAVEX

2015 BLACKENERGY

2016 CRASHOVERRIDE

2017 TRISIS

2022 PIPEDREAM

2024 FROSTYGOOP

2027 Universal to Malware

OT Malware Trends & Development

Espionage → Disruption → Disruption → Universal

2026

Threats and Risks

2028-A
Quantum Cryptography

Progress in Quantum Cryptography leads to conventional asymmetric algorithms losing their security. Adversaries could eavesdrop or tamper with encrypted data or communications secured by those algorithms. The civil nuclear industry has long data retention and long system lifespans and is thus more susceptible to using impacted algorithms.

Quantum risks are still theoretical today, but once they are proven practical, they will immediately impact various applications and systems.

2028-B
Integrity and Sourcing

Hardware- and firmware-based supply chain attacks involve compromising components during manufacturing or distribution. The industry will complete upgrades and changes to components in the coming years. This could lead to the insertion of malicious chips, altered firmware, or backdoors to be exploited later.

With an increased dependency on third parties for hard- and software implementation, validating the origin of every chip and software is difficult.

Once a supply chain or a hardware component has a backdoor or an intentional flaw, organisations using this component might lose integrity, confidentiality, and availability.

Recommendations

2026

- Organisations should **assess and classify existing algorithms and data**. They should consider external channels secured by broken algorithms.
- Components and data using insecure algorithms should receive an **upgrade to post-quantum** cryptography (PQC). This might take a long time.
- Organisations should **enforce PQC by vendors**.

Threat and Risk Origins

Misconfigurations and Accidental Incidents

Non-targeted Cybercrime

Targeted Intrusions

- The existing **supply chain programme** within the civil nuclear sector is effective. Organisations should continue using elements like **audits, inspections, supplier vetting, and collaborative efforts** among regulators, operators, and suppliers.
- **Software- and Hardware Bill of Materials** (SBOM/BOM) help to trace individual components to their origin and allow analysis.

About the Whitepaper

This paper has been created and published by ONR working in partnership with Dragos and is provided for guidance and information purposes. It does not constitute official ONR guidance or regulatory requirements. Further information can be found at www.onr.org.uk

Office for Nuclear Regulation

ONR Office for Nuclear Regulation

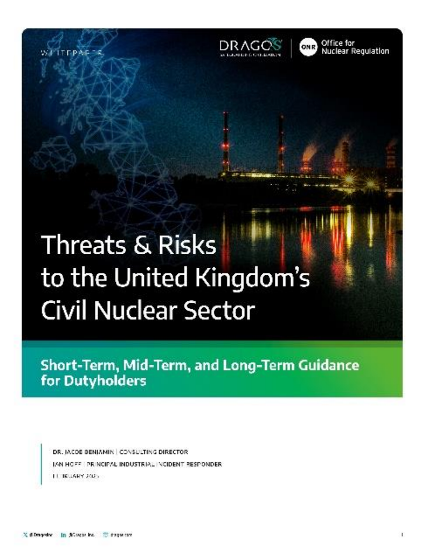
The Office for Nuclear Regulation is the UK's independent nuclear regulator and competent authority for nuclear security. ONR regulates security arrangements to ensure that the civil nuclear sector adequately protects sensitive nuclear information and industrial systems against cyber-attack and remains resilient to emerging threats as part of their broader mission to protect society by securing safe nuclear operations.

DRAGOS Safeguarding Civilization

Dragos is an industrial cybersecurity company founded to investigate and respond to the most significant OT cyberattacks in history. It combines a leading technology platform, OT services, and cyber threat intelligence to protect critical infrastructure from increasingly capable adversaries.

Get the Whitepaper

www.PlaceHolderLinkToPaper.Dragos.com



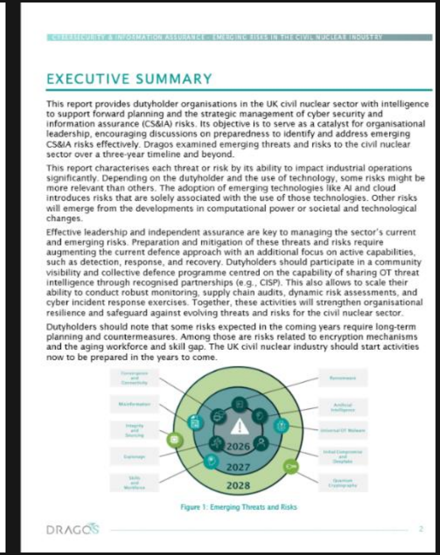
WHITEPAPER

DRAGOS | ONR Office for Nuclear Regulation

Threats & Risks
to the United Kingdom's
Civil Nuclear Sector

Short-Term, Mid-Term, and Long-Term Guidance for Dutyholders

DR. JACOB BENJAMIN | CONSULTING DIRECTOR
IAN HOFF | PRINCIPAL INDUSTRIAL INCIDENT RESPONDER
FEBRUARY 2025



CYBERSECURITY & INFORMATION ASSURANCE - EMERGING RISKS IN THE CIVIL NUCLEAR INDUSTRY

EXECUTIVE SUMMARY

This report provides dutyholder organisations in the UK civil nuclear sector with intelligence to support forward planning and the strategic management of cyber security and information assurance (CS&IA) risks. Its objective is to serve as a catalyst for organisational leadership, encouraging discussions on preparedness to identify and address emerging CS&IA risks effectively. Dragos examined emerging threats and risks to the civil nuclear sector over a three-year timeline and beyond.

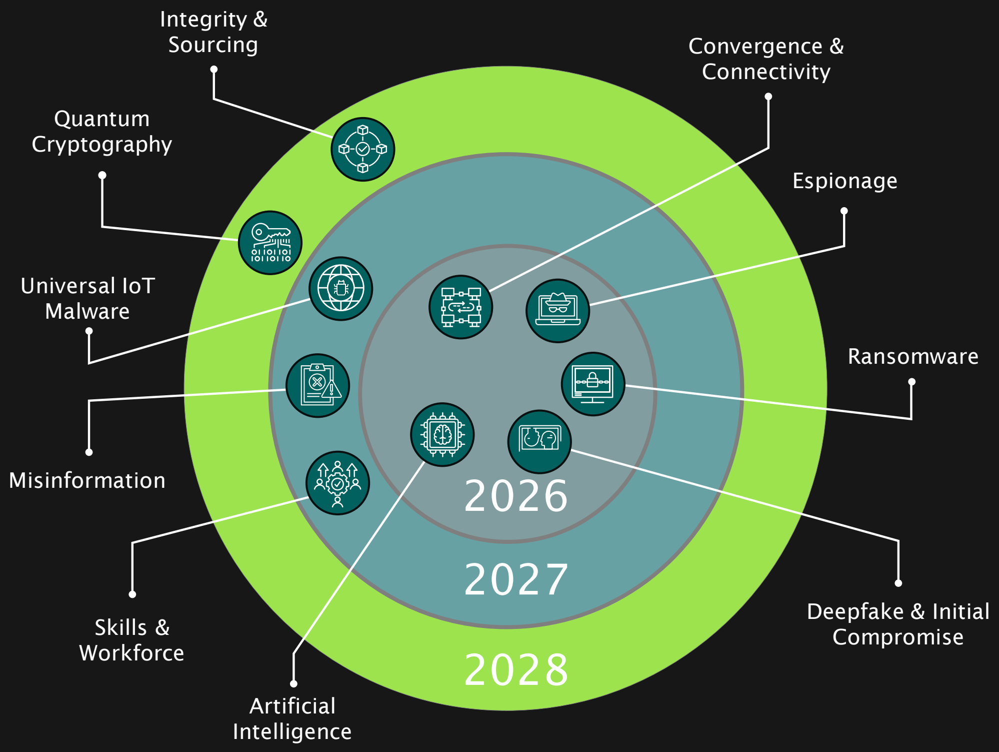
This report characterises each threat or risk by its ability to impact industrial operations significantly. Depending on the dutyholder and the use of technology, some risks might be more relevant than others. The adoption of emerging technologies like AI and cloud introduces risks that are solely associated with the use of those technologies. Other risks will emerge from the developments in computational power or societal and technological changes.

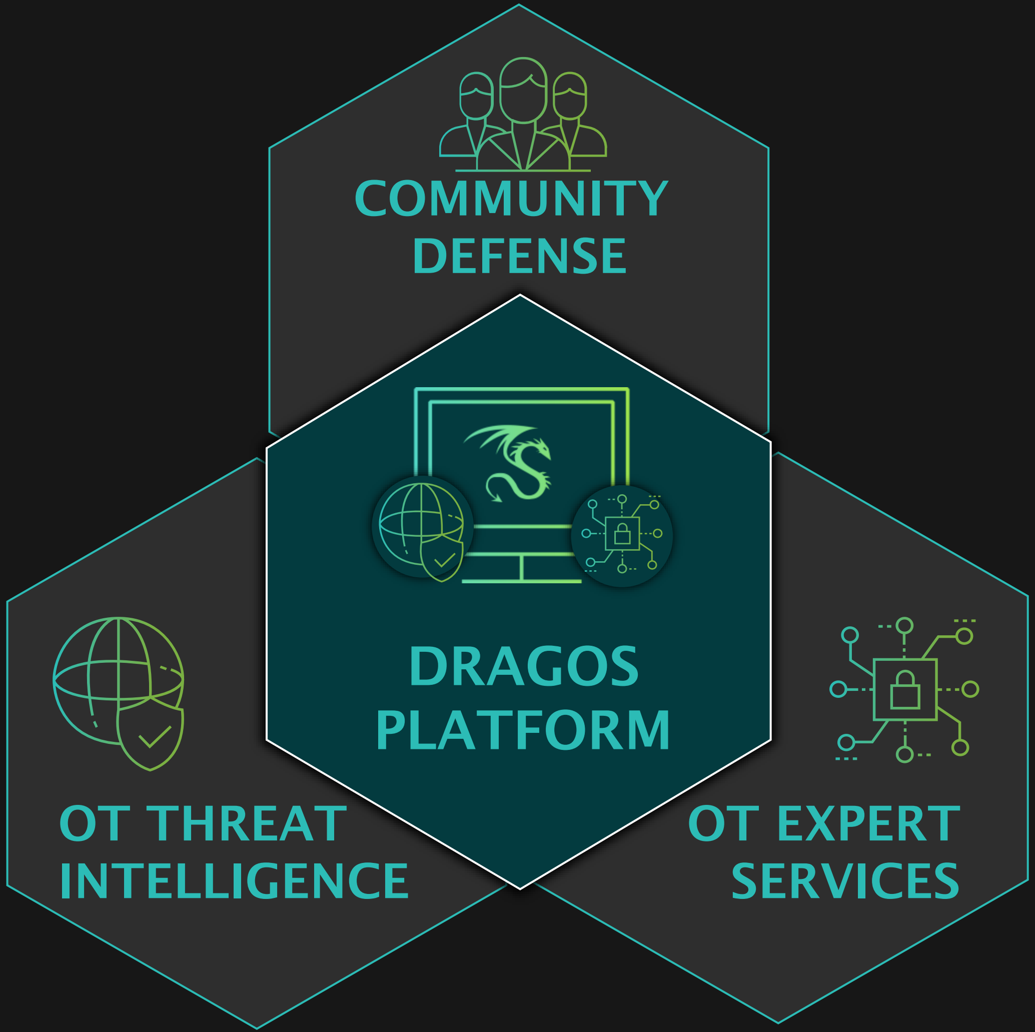
Effective leadership and independent assurance are key to managing the sector's current and emerging risks. Preparation and mitigation of these threats and risks require augmenting the current defence approach with an additional focus on active capabilities, such as detection, response, and recovery. Dutyholders should participate in a community visibility and collective defence programme centred on the capability of sharing OT threat intelligence through recognised partnerships (e.g., CISP). This also allows to scale their ability to conduct robust monitoring, supply chain audits, dynamic risk assessments, and cyber incident response exercises. Together, these activities will strengthen organisational resilience and safeguard against evolving threats and risks for the civil nuclear sector.

Dutyholders should note that some risks expected in the coming years require long-term planning and countermeasures. Among those are risks related to encryption mechanisms and the aging workforce and skill gap. The UK civil nuclear industry should start activities now to be prepared in the years to come.

Figure 1: Emerging Threats and Risks

DRAGOS





DRAGOS

Safeguarding Civilization

The Most Effective OT Security Tech Platform
Visibility into OT assets, vulnerabilities, traffic, and threats to reduce OT risk.

A Community-Focused Mission
Skills, communications, & resources to strengthen the collective defense

Expert OT Intelligence & Service Resources
OT expert analysts, threat hunters, & responders to help you win the fight.