An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

2025 National Cyber Risk Assessment

www.ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

CARR
TRANS

Table of Contents

Foreword from the Minister

As Minister for Justice, Home Affairs and Migration, I am pleased to publish the 2025 National Cyber Risk Assessment.

The ever-evolving digital landscape presents both remarkable opportunities and complex risks to Irelands critical infrastructure. These are influenced by the dynamic geopolitical environment, use of emerging technologies and exposure through vulnerabilities in ICT supply chains.

The National Cyber Security Centre plays a key role in leading Irelands response to cyber risk. Under our Programme for Government commitments, I am pleased to be bringing forward the National Cyber Security Bill which will put in place a strong and effective statutory National Cyber Security Centre, with updated mechanisms for the supervision and enforcement of network and information security, enshrined in law.

The recommendations in this risk assessment will be the foundation of the next National Cyber Security Strategy and will inform strategic goals and priorities for the Department of Justice, Home Affairs and Migration while also recognising that cyber security requires both a whole of government and whole of society response that includes private sector, small and medium enterprises, educational institutions and individuals.

Irelands digital infrastructure underpins all sectors of our society, delivering essential services that keep our hospitals, public transport, communications and energy supply functioning. Identifying and developing comprehensive responses to risks that threaten these services is essential to protect our security and overall resilience.

I would like to thank the teams throughout my Department for all their work in preparing this National Cyber Risk Assessment as well as all the stakeholders, who contributed to its development. I look forward to implementing the recommendations and the Programme for Government commitments alongside my colleagues, Minister Brophy and Minister Collins and with officials in my Department.

Together we continue to work towards making Ireland safe, fair and inclusive.

Jim O'Callaghan T.D.
Minister for Justice, Home Affairs and Migration

Foreword from the Director, NCSC

The first National Cyber Risk Assessment (NCRA) was produced in 2022 and described the nature and extent of the cyber related risks posed to Irish society and to the security of the State at that point. The basic principles set out in that original document still apply; in an era of accelerating digital transformation, Ireland's national security resilience increasingly depends on the integrity, availability, and security of its digital infrastructure. However the extent of the changes in the risk environment necessitated a fresh review of the risks, both to inform national policy and to ensure that the NCSC's own orientation and approach to its work remains correct.

The 2025 NCRA provides a strategic overview of the systemic cyber threats facing the State, its critical national infrastructure (CNI), and the broader ecosystem of supply chains upon which all of this depends. Building on the 2022 assessment and aligned with the evolving obligations under the EU's NIS2 Directive, this assessment offers a comprehensive, forward-looking appraisal of Ireland's cyber risk landscape and makes a series of recommendations to inform the forthcoming and third National Cyber Security Strategy.

The process has been heavily informed by the NCSC's operational experience in detecting and responding to incidents in the cyber domain, and in driving resilience and to evaluating and mitigating cyber risk across sectors. It also owes a significant debt to our stakeholders across Government, sectoral National Competent Authorities and our Coordination and Response Networks (or COREs), who have been extremely helpful in bringing their risks and their appreciation thereof to the table. Similarly, our colleagues in the Department of Foreign Affairs and Trade, the Defence Forces and An Garda Síochána have been instrumental in sharing their own appreciation of the risks in their areas.

The report underscores the need for a coordinated national approach to cyber security, including taking a whole-of-society approach. However, it is also clear thar the accelerating nature of some of the risks demands an aggressive response by the State, including by making full and active use of EU legislation. Our future security and prosperity relies on our maintaining Ireland's position as a digitally advanced, secure, and trusted partner within the European and global cyber domain.

R.A. Browne,
Director, National Cyber Security Centre

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Key Insights

Cybercrime remains the foremost cyber threat to Irish citizens, businesses and national infrastructure. Opportunistic and motivated by financial gain, cybercriminals persistently seek out weaknesses in cyber security, exploiting victims using social engineering, online fraud schemes and ransomware to steal money or data. Cybercrime can have severe consequences, affecting both the direct victim and more broadly by undermining the functioning of society[1].

Ireland continues to observe a rising prevalence of hacktivist activity and notes that, across the European Union, such activity accounts for approximately 80% of recorded incidents[2], driven primarily by low-level Distributed Denial of Service (DDoS) activity. While some cyberattacks are ideologically motivated, state-aligned threat actors are seizing the opportunity to blend their activities in with these disruptive cyberattacks, executing attacks under the guise of hacktivism, as observed by the NCSC during the recent European elections in Ireland.

State-aligned threat actors continue to pose a significant threat to Ireland's national security. Although the likelihood of a successful cyberattack directly targeting Ireland's critical infrastructure remains relatively low, Ireland's strategic interests and international profile make it an attractive focal point for sophisticated state-aligned actors.

As a democratic nation, a member of the EU and a committed partner of institutions including the UN, Irish interests are valuable targets for state-aligned threat actors intent on weakening democratic processes, generating division within the EU, eroding economic stability and destabilising western societies. Given Ireland's position as a digital hub, a centre for innovation and research and its pivotal location along subsea interconnectivity routes, these factors collectively influence Ireland's visibility as a target within the global cyber threat landscape.

The National Cyber Risk Assessment identifies three key systemic risks that will help to inform the next national cyber security strategy in its approach to protecting Ireland's critical infrastructure.

1
Dynamic geopolitical environment

2
Evolving technology and its implications on security

3
Supply chain security

Introduction

A central characteristic of the services and products that support contemporary societies is the extent to which they are defined, shaped and enabled by the widespread adoption of digital technologies. However, this increased centrality means that societies are exposed to a rapidly evolving global threat landscape, involving a confluence of malign actors, technical error and mere accidents.

At the level of the individual State, these risks manifest in various ways, with physical geography, economic context and geopolitical conditions all helping to shape the overarching degree of risk that the State faces. While Ireland shares much of its risk profile with partner nations in the EU, its physical location and relatively small scale adds an additional layer of complexity and challenge. When this is considered alongside Ireland's role as host to several of the world's largest technology providers and cloud computing facilities, together with the rapidly evolving geopolitical landscape, these challenges become increasingly nuanced and intricate, and ever more critical to Ireland's future security and long-term prosperity.

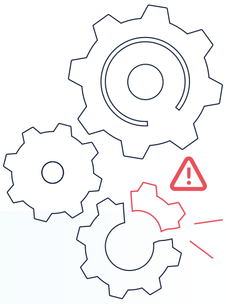
One of the defining characteristics of digital infrastructure is the degree to which different systems are interconnected and interdependent. Over time, this has resulted in a mesh of interdependencies between critical sectors that extend beyond national boundaries, driving a growing reliance on highly complex and often opaque multi-vendor supply chains. Consequently, a single disruptive event now carries the potential to trigger widespread, cascading effects with potentially global implications.

The National Cyber Security Strategy (2019-2024[3]) set out the requirement for a cyber security focused risk assessment of all Critical National Infrastructure (CNI) in the State. The objective of the risk assessment was to identify any pathways which could trigger systemic cyber risks and to recommend measures to address these. This led to the first National Cyber Risk Assessment[4] (NCRA) which was completed in 2022 and published in 2023.

This document marks the second iteration of Ireland's national cyber risk assessment. Prepared by the NCSC, the assessment is intended to inform the next National Cyber Security Strategy, which is presently in development.

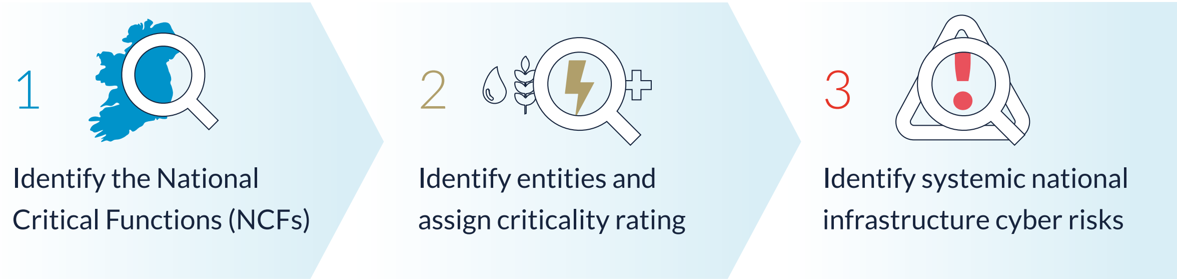
Methodology Overview

In 2022, Ireland's first National Cyber Risk Assessment (NCRA) report examined systemic cyber risks and the threat they posed to the State's critical infrastructure and services.



> **Systemic cyber risk** is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security.[5]

The risk assessment applied the methodology published by Ireland's Office of Emergency Planning (OEP), Strategic Emergency Management, Guideline 3[6], and followed a three-step approach:



1 Identify the National Critical Functions (NCFs)

2 Identify entities and assign criticality rating

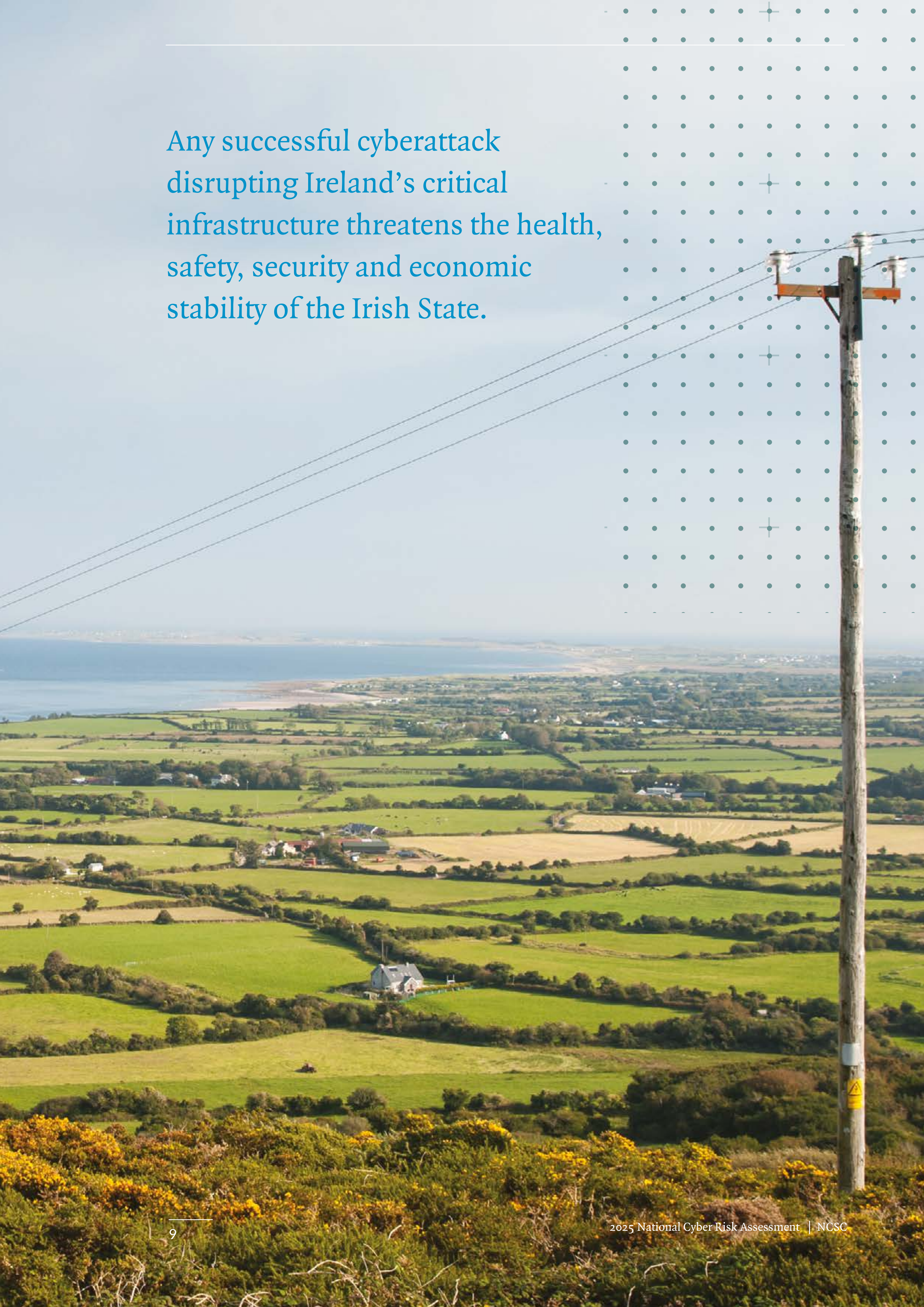
3 Identify systemic national infrastructure cyber risks

In the three years since this risk assessment was conducted, there have been significant technological and geopolitical developments. To reflect this evolving threat landscape and its implications on previously assessed risk probability levels, this document delivers a forward-looking assessment of technology trends and evolving threats. It reviews critical sectors most exposed to significant systemic risks and revises risk probability levels, where applicable. A detailed outline of the methodology applied can be referenced in Annex I.

The process commenced with a detailed analysis of the current threat landscape as it impacts on Irelands critical infrastructure today; it evaluated threats from both state-aligned and non-state actors while also considering contributing factors such as human error or system failures. The process was informed by analysis of reported incidents, cyber threat intelligence and global trends as well as active engagement with peer agencies and partner organisations.

Applying a qualitative approach when assessing the probability of identified cyber threats, a set of revised threat levels were compiled and shared with sectoral stakeholders for review, with their feedback subsequently incorporated into the 2025 NCRA.

Any successful cyberattack disrupting Ireland's critical infrastructure threatens the health, safety, security and economic stability of the Irish State.



Cyber Threat Landscape

Strengthening the cyber security and resilience of Ireland's critical infrastructure is essential to safeguarding its operational environment and ensuring the secure and trusted delivery of services. These essential services support the everyday needs of a functioning society, such as:

- the consistent **delivery of electricity** to homes, hospitals and businesses
- reliable **transport infrastructure** to ensure the safe movement of people and goods
- the uninterrupted supply of **drinking water** and effective treatment of **wastewater**
- 'always-on' **phone and internet connectivity** to support communications and data transfer
- trusted access to **financial transaction** and payment platforms
- secure **research environments** where valuable IP and trade secrets are safely protected
- security of **democratic institutions** and electoral processes, trusted information sources

As technology has advanced and reliance on digitalisation has intensified, the cyber threat landscape has become more complex with an increased risk of incidents leading to significant cross sectoral impacts.

Threats can take the form of either intentional or unintentional acts.

- Unintentional acts have the potential to cause significant negative impacts to critical infrastructure and can stem from a variety of sources, such as, system failure, human error and natural phenomenon, e.g. floods, fire.
- Intentional acts are perpetrated by various types of threat actor and are of a malicious nature, examples include ransomware, Denial of Service (DoS), malware and social engineering, all of which remain a persistent challenge.

Threat actors can fall into two main categories, state-aligned and non-state.

- Non-State actors (e.g. cybercriminals and hacktivists) are often motivated to conduct cyberattacks based on financial incentives or ideological factors.
- State-aligned actors, typically tend to be well-funded and resourced, possessing the skills to conduct advanced malicious cyber activities to further both tactical and strategic objectives.

enisa

ENISA THREAT LANDSCAPE 2025

OCTOBER 2025

The ENISA 2025 Threat Landscape report[7] published by the EU's Cyber Security Agency (ENISA), recorded a notable escalation in hacktivist attacks and state-aligned cyber threats during their 2024-2025 reporting period. Their assessment was based on the volume of incidents recorded by EU Member States and the consequences of these attacks.

As critical infrastructure providers continue to transition to an operational environment reliant upon greater integration, automation and the use of cloud hosted services, these cyber-physical systems are increasingly exposing a much broader attack surface. Equipped with advanced tools, there is a widening array of threat actors, ranging from low-level 'script kiddies' to sophisticated Advanced Persistent Threat (APT) groups. Each seeking out opportunities against high value targets, to achieve the highest possible reward for their efforts. Any successful cyberattack disrupting Ireland's critical infrastructure threatens the health, safety, security and economic stability of the Irish State.

For analytical purposes, this assessment considers systemic risks under three thematic areas, as follows:

- Dynamic geopolitical environment
- Evolving technology and its implications on security
- Supply chain security

Systemic Cyber Risks

Dynamic geopolitical environment

Dynamic geopolitical environment

Observed Trend

An extended period of globalisation, linking people and technology, has driven an era of sustained development and economic growth. However, the international environment is now increasingly contested, dynamic and volatile. Ireland and the EU continue to experience the impacts of Russia's war of aggression in Ukraine and a global increase in geopolitical tensions resulting in new and emerging risks. These include highly concentrated supply chains, overreliance on specific supports, as well as threats of economic coercion, cyber and infrastructure attacks, and foreign interference and disinformation campaigns.

Previous implicit barriers to state-led actions are eroding, giving way to a broader range of offensive cyber activities being undertaken by state-aligned threat actors (most notably Russia and China, as reflected in statements released by the European Union[8] and international partners[9]). Such activities pose a significant threat to the delicate and interdependent digital ecosystem that critical products and services rely on, including Ireland's public administration services, critical infrastructure and political institutions.

Whether perpetrated by state-aligned or non-state threat actors, cyberattacks targeting Ireland's CNI can be viewed from three distinct threat perspectives:

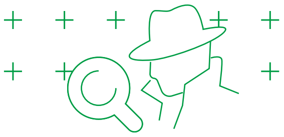
- **Direct targeting of Irish infrastructure:** While there may be some variation across sectors, both public and private CNI entities are increasingly moving toward automation, IoT/OT integration and cloud services. This technology shift is expanding the overall attack surface, presenting greater opportunities for highly sophisticated threat actors seeking to leverage adversarial advantage through this evolving landscape.

- **Targeting of shared infrastructure:** Ireland's essential services rely on both onshore critical national infrastructure and shared critical infrastructure with the UK, EU and other global partners, pivotal to supporting vital societal functions and inherently considered by adversaries as high value targets. As geopolitical uncertainty rises, hybrid attacks targeting shared critical infrastructure, including subsea cables and gas interconnectors, have increased globally.

- **Location-agnostic targeting of technology:**

  Due to the nature of virtualised infrastructure, geographic location is often immaterial to threat actors seeking to conduct cyberattacks. As Ireland forms a crucial link in the global digital supply chain, there is a growing risk that its services could be impacted as a second-order consequence from attempts by malign actors to compromise systems or services elsewhere.

Cyberattacks including cyber-espionage, sabotage and disinformation campaigns will evolve in tandem as threat actors adjust offensive cyber operations to advance geopolitical objectives, risking the stability and security of services essential to the functioning of the Irish State. The following pages provide examples of such cyberattacks that have occurred globally.



Cyber-espionage

Cyber-espionage involves the unauthorised access of sensitive information or intellectual property, often for political, economic or strategic goals. Usually requiring sophisticated techniques to steal sensitive data while remaining undetected, these types of attacks are typically perpetrated by advanced, well-funded and resourced threat actors.

As a central hub to many of the world's leading multinationals and a centre of excellence for research and innovation initiatives, Ireland presents an attractive target for malicious actors seeking to obtain sensitive information via cyber-espionage operations. The NCSC regularly observes state-aligned threat actors carrying out scanning and other reconnaissance activities targeting Irish government and state-owned networks. Given the global reach and ambitions of many of these threat actors, this is unsurprising and is certain to continue and likely to increase in the future.

Cyber security incidents across the EU are on the rise[10] and as a member of the EU, Ireland is not immune from malicious cyber activities. In May 2025, Ireland supported the statement[11] released by the High Representative on behalf of the EU on malicious behaviour in cyberspace targeting the EU Member State, Czechia. This related to a cybercampaign that targeted Czechia's Ministry of Foreign Affairs. Czechia determined that the cyberattack had been perpetrated by the APT31 group that is associated with the Ministry of State Security of China.

The following additional real-world examples demonstrate the ongoing threat that cyber-espionage poses to a country's national security, its economic prosperity and international reputation.

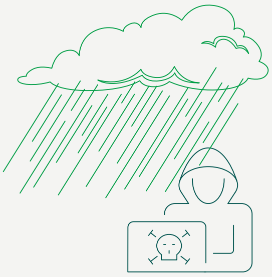
Salt Typhoon

Details emerged from the U.S. in late 2024 of a sophisticated intrusion that infiltrated the networks of at least nine major U.S. telecom providers[12]. The attack was attributed to the cyber-espionage group referred to as Salt Typhoon[13], a suspected Chinese state-aligned hacking group.

In August 2025, a Joint Security Advisory, titled *“Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System”*[14] was published by U.S. Cyber Security Agency, CISA. Co-sealed by multiple international government and cyber security agencies in Europe and beyond, the advisory details ongoing malicious activity by the People’s Republic of China (PRC) state-sponsored APT actors. Targeting networks globally, including but not limited to, telecommunications, government, transportation and military infrastructure networks, this APT activity partially overlaps with the cyber threat actor, commonly referred to as Salt Typhoon.

Midnight Blizzard

CISA, the NCSC UK and other partner agencies, published a joint advisory[15] in 2024, assessing the group APT29, commonly known as Midnight Blizzard, to be a cyber-espionage group, almost certainly part of the SVR, an element of the Russian intelligence services. Previously observed targeting government, healthcare and energy agencies, the advisory noted how the group have adapted their Tactics, Techniques, Procedures (TTPs), expanding their targeting to include other areas such as aviation, education, law enforcement and military organisations. Moving beyond their traditional targeting of on-premises networks, they have evolved to directly targeting cloud services[16].



Firewall devices

In early 2024, in a first public attribution of cyber-espionage to China by the Netherlands, the Netherlands military (MIVD) and civilian (AIVD) security services confirmed the Defence ministry had been hacked for espionage purposes, assessing with high confidence the activities were conducted by a Chinese state-sponsored actor exploiting a vulnerability in FortiGate devices[17].

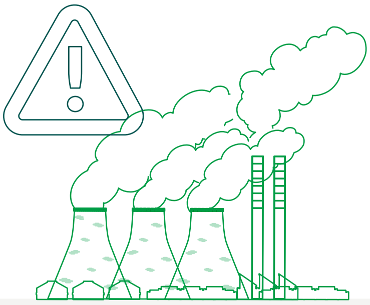
Targeted disruptive and destructive cyberattacks

Targeted disruptive and destructive cyberattacks represent one of the most serious threats to critical infrastructure, risking sustained impact and the potential to trigger spill-over effects to multiple sectors.

Many critical infrastructure networks rely on operational technology (OT) to manage process-controlled tasks. OT environments, initially designed to prioritise uptime and safety over cyber security, rely heavily on specialised, often legacy, equipment and protocols. With the progressive convergence between OT and IT environments, these vital systems are increasingly exposing an expansive attack surface and are inherently more susceptible to cyber threats when compared to modern IT environments.

In November 2023, vendor-specific OT Programmable Logic Controllers (PLCs) used in Irish water facilities were accessed by a state-aligned threat actor. Defacing the PLCs with politically motivated notices, the attack had direct operational impacts on a private water scheme in the west of Ireland, leaving up to 160 Irish households without water for up to 48 hours. Specifically targeting Israeli manufactured Unitronic PLCs, the attackers heavily publicised the attack on social media accounts linked to a hacktivist persona. The attack was indiscriminate and likely impacted multiple targets globally. The use of hacktivist personas by state-aligned threat actors, has led to a blurring of the lines between traditional hacktivist and state-nexus activities, allowing States to maintain plausible deniability and making attribution increasingly difficult.

As in the example above, conducting disruptive or destructive cyberattacks against a country's CNI is no longer a hypothetical threat. It has unfortunately been used on several occasions as part of cyberwarfare tactics targeting Ukraine and its critical infrastructure. One such case is outlined overleaf. These cyber-physical attacks represent the intent and capability of state-aligned actors to use offensive cyber operations to further geopolitical objectives.

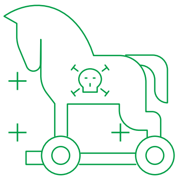


Sandworm

In late 2022, the state-aligned threat actor, known as Sandworm[18], targeted Ukraine's critical energy infrastructure, attacking the Ukrainian Energy Company substations, causing power outages[19]. Conducting a disruptive cyber-physical attack, the hackers leveraged a novel technique to target toolsets native to the critical infrastructure provider's OT network. Using Living Off the Land (LotL) techniques, the attackers were able to remotely trip the power company's substation breakers, causing unplanned power outages, leading to blackouts for hundreds of thousands of Ukrainian civilians.

The outages coincided with mass missile strikes on critical infrastructure across Ukraine. Two days after the power outage attack, Sandworm conducted a second disruptive attack by deploying a wiper malware in the victims IT infrastructure, further obstructing recovery efforts. The Mandiant analysts studying the cyberattacks highlighted how such attacks are often used to exacerbate the psychological toll of war on a society.

Sandworm, an APT actor, is believed to be operated by a cyberwarfare unit (74455[20]) of the GRU, Russia's military intelligence service. Active since at least 2009, Sandworm is considered a destructive cyberthreat group, responsible for multiple cyber operations, including targeting of the French presidential campaign in 2017 and conducting a sabotage attack targeting the South Korean hosted 2018 Winter Olympic Games[21].



Pre-positioning

Pre-positioning is a strategy used in offensive cyber operations, often by state-aligned threat actors, particularly during times of geopolitical uncertainty. In these cases, advanced threat actors conduct cyber activities aimed at securing a foothold on infrastructure over a long period. This unauthorised access allows them to observe their targeted network's behaviour, identify its critical dependencies and move around the network at will. Later, at a future point in time if tensions escalate, the threat actors can leverage their position to conduct disruptive or destructive attacks against their victims' network.

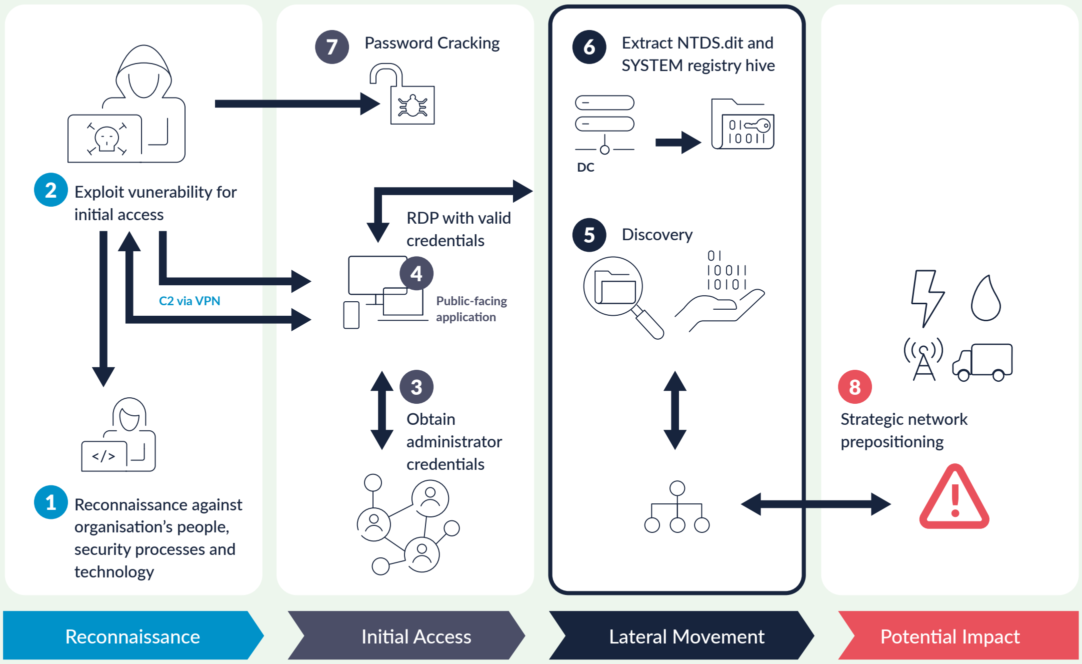
Volt Typhoon

Active since 2021, Volt Typhoon[22] is an example of how sophisticated threat actors can exploit technical vulnerabilities in products to gain access to critical infrastructure, gathering sensitive information and hiding their presence for long periods of time.

After gaining an initial foothold in U.S.-based critical infrastructure by exploiting vulnerabilities in publicly exposed systems, the threat actor was able to use techniques such as LotL to evade detection, blending in with normal network traffic activity[23], making it difficult for detection by traditional IT security tools.

It is believed that these pre-positioning attacks are designed to infiltrate U.S. critical infrastructure, likely in preparation for future disruptive or destructive cyberattacks in the event of a major crisis or conflict with the United States[24].

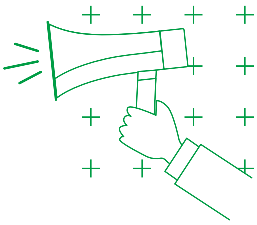
Volt Typhoon, an APT group, is primarily known to target U.S. critical infrastructure providers, deploying post-compromise strategies intended to minimise opportunities for detection[25]. Active since at least 2021, the state-aligned threat actor is attributed to the PRC[26].


7 Password Cracking
6 Extract NTDS.dit and SYSTEM registry hive
DC
2 Exploit vunerability for initial access
RDP with valid credentials
C2 via VPN
4
Public-facing application
5 Discovery
3 Obtain administrator credentials
8 Strategic network prepositioning
1 Reconnaissance against organisation's people, security processes and technology
Reconnaissance
Initial Access
Lateral Movement
Potential Impact

"Typical Volt Typhoon Activity" infographic from CISA, NSA, and FBI's 2024 joint advisory[27]

Utilising pre-positioning tactics on critical infrastructure, such as telecommunications, energy, transport and water networks, this cyber threat represents a significant risk to Ireland's national security and the broader security of the EU.

Cyber activity in support of information operations



Cyber activity in support of information operations is a growing security threat to the EU, its Member States, including Ireland, and partner countries. With increasing frequency and intensity, hybrid activities combine a mix of information operations, such as Foreign Information Manipulation and Interference (FIMI) and 'hack and leak', with disruptive cyber activity, often conducted by state-aligned threat actors under the guise of hacktivism.

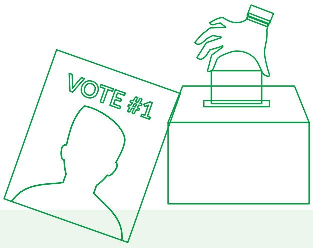
On June 7th, 2024, the Irish electorate went to the polls to cast their vote in the European elections. On the afternoon of the elections, several websites hosting election and transport information were targeted by DDoS attacks, conducted by a hacktivist threat group. These cyberattacks followed a similar pattern to attacks targeting elections across Europe.

The sophistication of the attacks was low, and the impact was minor as affected sites were able to implement basic mitigation strategies to prevent major disruption. Overall, these cyberattacks had little observed impact on the conduct of the elections and received little media attention, but the attackers broadcast the success they had against these websites on their public Telegram channel.

The NCSC has increasingly observed instances of state-aligned threat actors adopting or using hacktivist fronts to mask their identity when conducting such cyberattacks, while greater cooperation between criminal groups and pooling of resources has increased the level of disruption possible.

This type of activity attacks democratic societies by targeting their critical sectors, decision-making processes and economic structures[28]. Actors can be state-aligned or non-state, comprising proxies inside and outside of their own territory[29]. Such hybrid activities aim to stoke polarisation and divisions across EU Member States, while also attempting to undermine the EU's global standing within the international community.

Hybrid campaigns pose a significant threat to a country's democracy by combining cyber operations, disinformation campaigns, sabotage and espionage to cause destabilising effects. Examples of other targeted campaigns included the following in 2024:

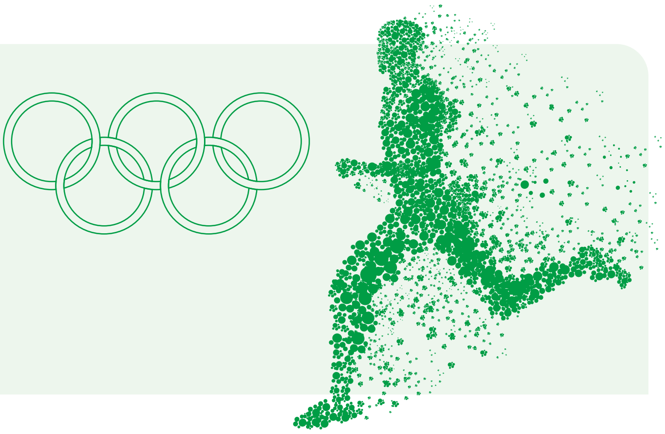


Romania

Romania's Supreme Council of National Defence (CSAT) declassified documents stating that Romania was the target of aggressive hybrid attacks orchestrated by a state-actor during its 2024 presidential election, undermining its democratic election process[30].

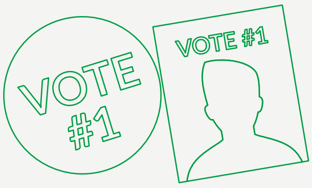
France

France also represented a prime focus, with The Paris Olympic and Paralympic Games and the French legislative elections among the main targets[31].



Moldova

In the lead up to the 2024 Moldovan Presidential elections and its EU membership referendum, a cyber-enabled disinformation campaign was identified targeting government sectors, likely aiming to undermine trust in Moldova's government and discredit EU integration[32].



In July 2025, standing in solidarity with its fellow EU Member States, Ireland supported the statement released by the High Representative on behalf of the EU condemning Russia's persistent malicious hybrid campaigns, aimed at threatening and undermining the security, resilience and democratic foundations of the EU, its Member States and its partners.

Through measures taken by each EU institution and Member States, as well as the unprecedented cooperation between them, collectively their efforts helped to ensure that the elections ran smoothly overall, despite the challenges from increased EU-related disinformation and the detection of various cases of Foreign Information Manipulation and Interference (FIMI) activity.

Geopolitics has a profound effect on cyberspace, motivating an array of threat actors to leverage the opportunities that emerge during times of change. As an Island, Ireland assesses risks from sea to sky, on-shore and off-shore, taking a holistic cyber security approach to protecting its critical infrastructure, economic stability and democratic processes.

Systemic Cyber Risks

Evolving technology and its implications on security

Evolving technology and its implications on security

Artificial Intelligence

Observed Trend

Increased adoption of AI is amplifying the effectiveness of existing threat vectors, using sophisticated social engineering, enhanced technical capability and more authentic content creation through enhanced language credibility and hyper-realistic deepfakes. The integration of Large Language Models (LLMs) into CNI architecture also creates a more complicated threat landscape with models susceptible to prompt injection, and data poisoning attacks, targeting the confidentiality, integrity and availability of the model and its underlying data sets.

Threat

The rapid development and adoption of AI is creating a digital divide between organisations with the capability to keep pace and those who cannot. It is considered a realistic possibility that this will have a significant impact on the vulnerability of critical systems by 2027 .

This will increase the opportunities for malicious threat actors of all capabilities to launch at scale, disruptive and destructive attacks, as well as silently and persistently linger on critical assets using advanced technologies to assist them in evading detection for longer periods of time.

Risk

The widespread adoption of AI is already shaping society, with its presence embedded across all sectors, and its adaptability evident in diverse environments. However, the accelerating pace of change makes it susceptible to vulnerabilities with real-world consequences. Possible scenarios in an Irish context could, for example, include:

- Transport:
  Data poisoning attacks could lead to AI enabled traffic management systems making incorrect decisions, creating potentially dangerous situations.
- Utilities:
  In a water treatment plant, AI-controlled sensors could be manipulated to incorrectly calculate water treatment levels, risking harm to public safety.
- Public Administration:
  By jailbreaking or removing guardrails, threat actors could confuse an AI model, leading to the disclosure of sensitive information.

As many organisations are accelerating the integration of AI technology into their day-to-day business operating functions, threat actors are exploring innovative ways to target this expanding attack surface, supplementing their own TTPs with Gen-AI to enhance their operational efficiency and scale.

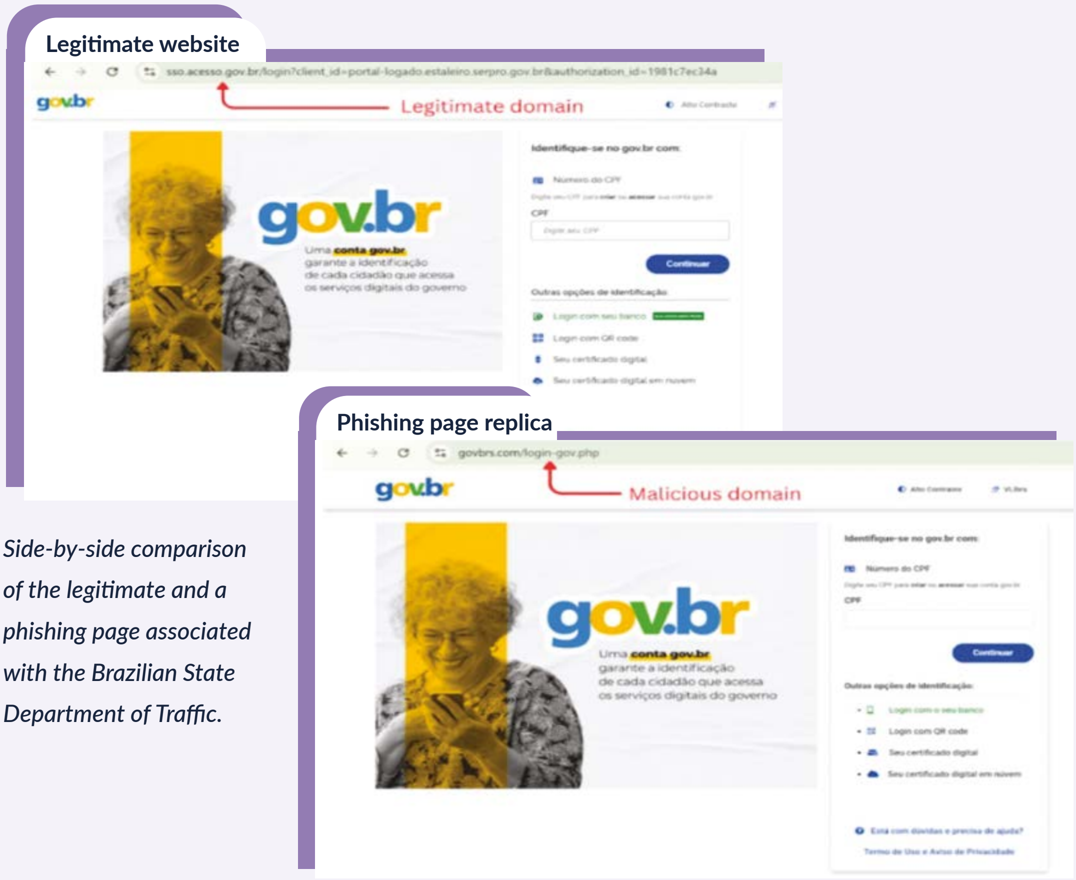
Examples of Gen-AI supported cyberattacks

Phishing

In 2025, hackers targeted Brazil's Public Administration, using Gen-AI tools like DeepSite AI and BlackBox AI to produce phishing templates that closely mimicked the Brazilian government's official websites. Two phishing templates were used:

1. impersonating the Brazilian State Department of Traffic with promises of a free driver's license
2. masquerading as the Brazilian Ministry of Education providing employment opportunities.

Attackers were able to steal personal information and money from citizens interacting with forms embedded in these impersonated government websites. Analysis of the attack conducted by Zscaler ThreatLabz[36] researchers concluded the use of AI to generate code used in the attack.


Legitimate website
sso.acesso.gov.br/login?client_id=portal-logado.estaleiro.serpro.gov.br&authorization_id=1981c7ec34a
gov.br
Legitimate domain
Identifique-se no gov.br com:
Número do CPF
CPF
Continuar
Outras opções de identificação:
Login com seu banco
Login com QR code
Seu certificado digital
Seu certificado digital em nuvem
gov.br
Uma conta gov.br garante a identificação de cada cidadão que acessa os serviços digitais do governo
Phishing page replica
govbrs.com/login-gov.php
gov.br
Malicious domain
Identifique-se no gov.br com:
Número do CPF
CPF
Continuar
Outras opções de identificação:
Login com o seu banco
Login com QR code
Seu certificado digital
Seu certificado digital em nuvem
gov.br
Uma conta gov.br garante a identificação de cada cidadão que acessa os serviços digitais do governo
Está com dúvidas e precisa de ajuda?
Termo de Uso e Aviso de Privacidade

Side-by-side comparison of the legitimate and a phishing page associated with the Brazilian State Department of Traffic.

Examples of Gen-AI supported cyberattacks

IT workers

State-aligned threat actors are turning to cybercrime activities to fund their broader cyber operations. Such activity has included threat actors creating fake identities and posing as IT workers[37], targeting western tech companies to illicitly obtain high-paying remote employment, with any financial gains being channelled directly back to their nation-state. Active since 2018, the state-aligned threat actor FAMOUS CHOLLIMA[38] is known to have leveraged AI capability to aid in its objective to fraudulently secure remote IT worker jobs.

These state-aligned threat actors also used this remote access to conduct further malicious activities, including data theft and extortion campaigns.

In one case, IT workers used false identities to gain remote employment with a U.S. based blockchain company, stealing virtual currency worth over $900,000. The U.S. Department of Justice[39] have since indicted four North Korean nationals, charging them with wire fraud and money laundering arising from the remote IT worker scheme. Given the potential for high financial returns and the scalability assisted by Gen-AI capability, these types of attacks are on the rise. It is reported that FAMOUS CHOLLIMA insiders infiltrated over 320 companies in a 12-month period, a 220% increase year-on-year[40].

Applications
Interviews
On the Job

Langflow AI

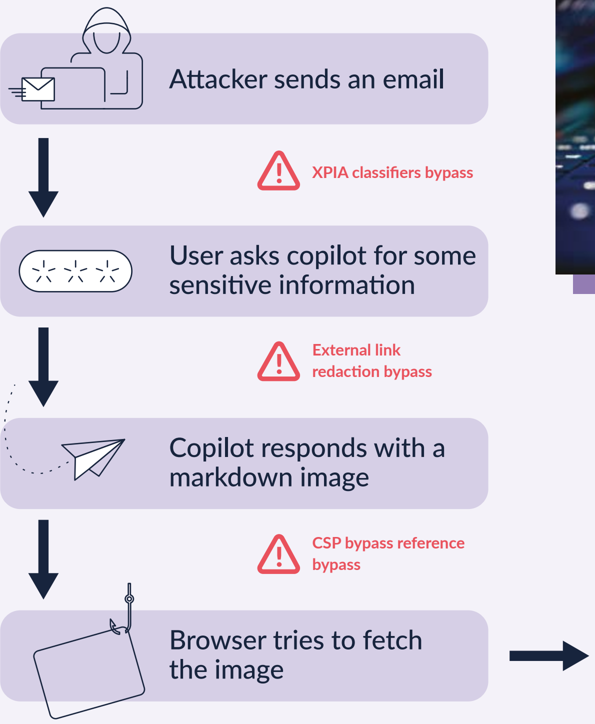
In April 2025, CrowdStrike observed multiple threat actors exploit an unauthenticated code injection vulnerability in Langflow AI, which is a widely used open-source tool for building AI-driven agents and workflows. Threat actors leveraged this vulnerability against the AI tool to achieve persistence, credential access, and malware deployment. Organisations using Langflow in their AI development workflows were exposed to the significant risk of any attacker on the internet being able to take full control of vulnerable Langflow servers[41]. This real-world example illustrates how AI tools are now being viewed as primary attack vectors due to their position as integrated infrastructure rather than peripheral applications.

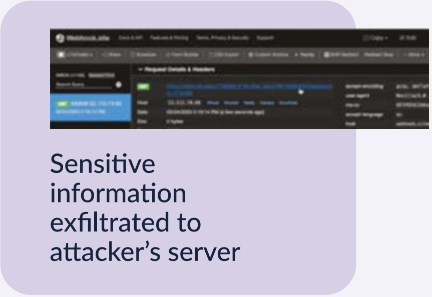
Echo Leak

In June 2025, AIM Security[42] discovered a zero-click vulnerability, termed 'EchoLeak' AI attack, that enabled the theft of sensitive data via Microsoft 365 Copilot. Targeting an AI agent, the vulnerability facilitated attackers in getting Copilot 365 to automatically exfiltrate potentially sensitive information from a targeted user or organisation without requiring user interaction.

In this attack, the guardrails typically deployed by Microsoft to prevent prompt injection attacks were bypassed, enabling malicious emails to go undetected. The exploit, described by AIM Security, outlines how the attack involved sending the target victim a specially crafted email with disguised malicious prompts included. When triggered, these prompts could potentially direct Copilot to exfiltrate sensitive data to an external server controlled by the attacker.

Attack Flow


Attacker sends an email
XPIA classifiers bypass
User asks copilot for some sensitive information
External link redaction bypass
Copilot responds with a markdown image
CSP bypass reference bypass
Browser tries to fetch the image



Microsoft deployed a server-side fix[43] in June 2025, stating that there was no evidence the vulnerability was exploited in the wild and no customers were impacted. This vulnerability is a powerful example of how the autonomy of agentic AI paired with manipulated LLMs can be combined to turn a legitimate agent into a nefarious exploit path.

Quantum Computing

Observed Trend

In as little as 10 years, quantum computers with the capability to break existing public key cryptography standards may be developed, with progressive milestones already achieved[44]. This represents a disruptive advancement, with capabilities that reach beyond the operational limitations of conventional computing and requiring a new approach to securing information and communications into the future.

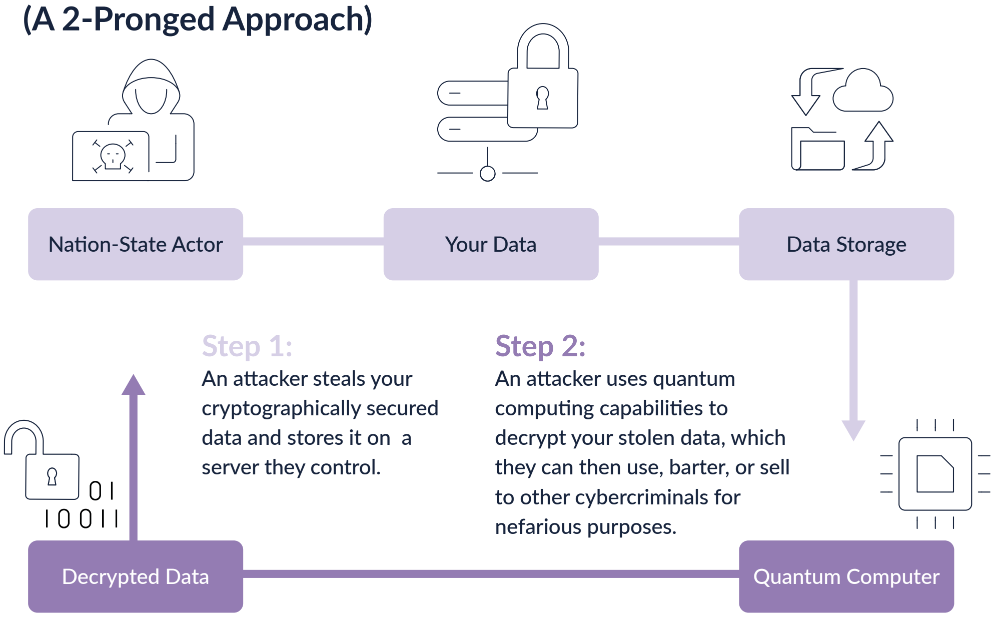
Threat

Most countries agree that starting now, it will take until 2035 to fully transition to quantum resistant algorithms. Therefore, key data with a lifespan of 10+ years is already an attractive target for "harvest now, decrypt later" attacks. This could include sensitive personal information such as healthcare data, Personal Public Service (PPS) numbers and passport numbers as well as intelligence central to the security of the State.

Risk

Harvest now, decrypt later or 'HNDL' attacks work on the premise that while current encryption methods are secure, it is worth exfiltrating strategically important encrypted data with the expectation that as quantum computing capabilities improve, it will be possible to decrypt the stolen data in the future at a point before it loses its value. The timescales involved means that threat actors are most likely to be state-aligned, presenting a significant risk to Ireland's national security, international reputation and potentially a broader loss of trust in public and private institutions.

How an HNDL Attack Works (A 2-Pronged Approach)



Step 1: An attacker steals your cryptographically secured data and stores it on a server they control.

Step 2: An attacker uses quantum computing capabilities to decrypt your stolen data, which they can then use, barter, or sell to other cybercriminals for nefarious purposes.

Other Considerations

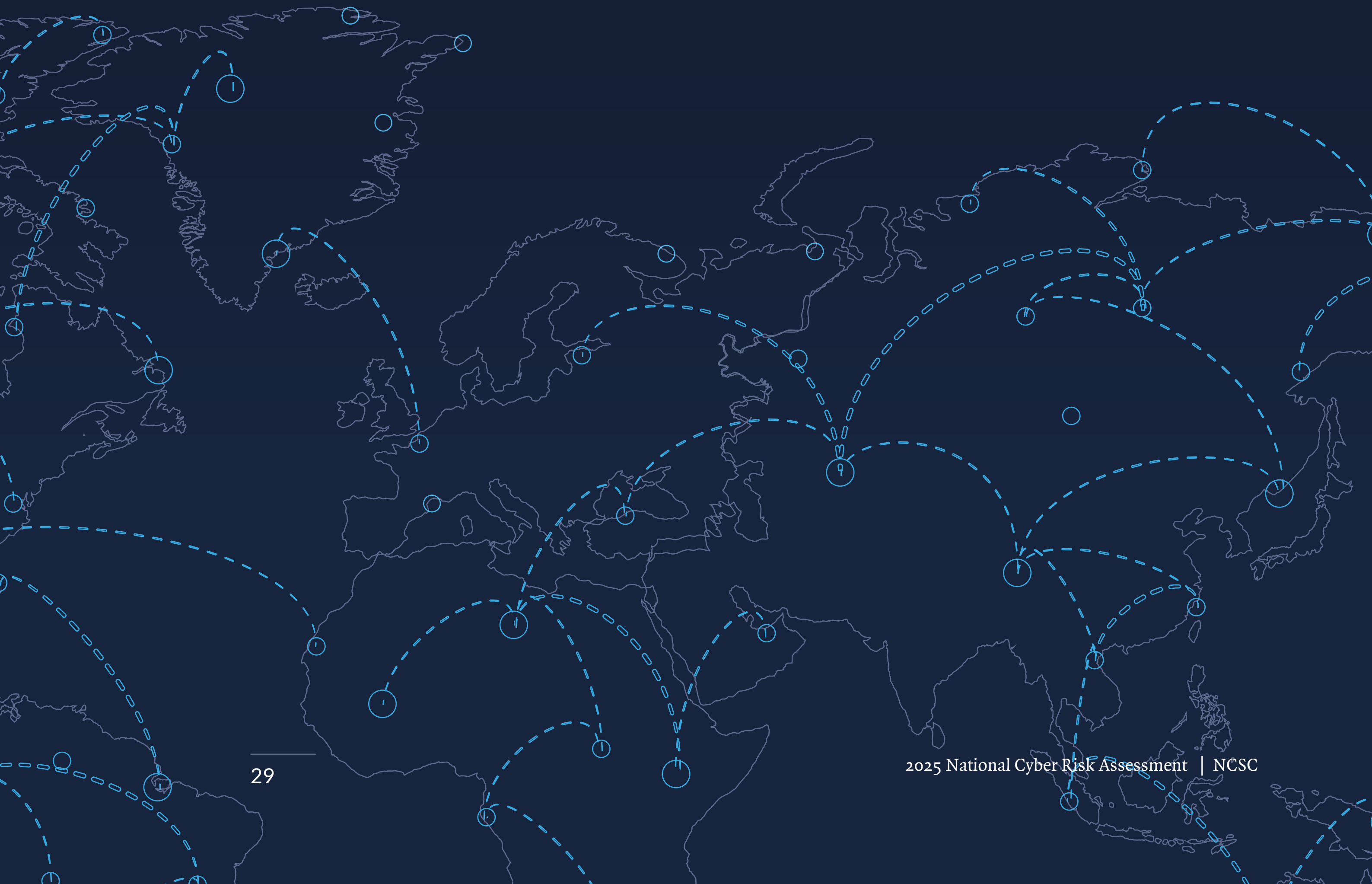
As emerging and disruptive technologies become more prevalent throughout the digital eco-system, technological advancements risk outpacing appropriate governance and approved standards, threatening the safe, equitable, secure use of future technologies.

Risks include:

- a lack of clarity on roles and responsibilities, risking ambiguous accountability
- overlapping governance rules and policies leading to inconsistent approaches to compliance and enforcement, particularly in the context of implementing cross-border directives, including the NIS2 Directive[45] and the Cyber Resilience Act (CRA)[46]
- insufficient regulation of emerging technologies may result in the proliferation of divergent standards or insecure technology

Systemic Cyber Risks

Supply chain security



Supply chain security

Observed Trend

Supply chain security has emerged as a significant challenge to strengthening the cyber resilience of CNI. The increasing interconnectedness of digital systems, the complexity of global supply chains, the growth of open-source software supply chains[47] and the widespread integration of smart technologies have combined to create a highly dynamic and ambiguous end-to-end ecosystem. In such an environment, clarity on supplier ownership, control and the implementation of effective cyber security measures can often be difficult to ascertain.

Threat

Threat actors are increasingly targeting critical entities through vulnerabilities in their supply chain, enabling both direct targeting and one-to-many attacks against an organisation. The threat is amplified in sectors where a lack of supplier diversification or an over-reliance on a concentrated set of suppliers exists, creating additional concerns around vendor lock-in.

By targeting vulnerable points along the supply chain, threat actors can expend less effort than attacking their primary target directly. Exploiting a weak point to gain an initial foothold, they leverage this position to inflict disruptive cyber activities against their primary target.

For example, with the number of Internet of Things (IoT) devices nearing 20 billion worldwide[48], these low-end devices attract threat actors seeking easy access points to conduct their cyber operations. Frequently lacking robust cyber security measures, these devices pose a significant threat to critical infrastructure, enabling an attacker to gain remote control of devices embedded deep within networks.

Risk

Organisations, particularly those responsible for critical infrastructure, have become better adept at managing vulnerabilities and securing their network defences against cyberattacks. Recognising this, threat actors are pivoting towards focusing more on the supply chains of critical infrastructure providers. CNI providers are at risk of significant disruptive effects if any of their key suppliers or third-party partners are compromised by a cyberattack.

In 2017, a state-aligned threat actor conducted a spear phishing campaign that targeted several organisations from Ireland's energy sector as part of a broader campaign targeting other government and critical infrastructure providers globally. To achieve their goals of gathering intelligence specific to Industrial Control Systems (ICS), the attackers exploited less secure third-party suppliers to gain access to their intended targets. This highly targeted and complex multi-staged campaign employed advanced tactics, TTPs, including obfuscation, webshell deployments and anti-forensic activities. While this campaign was ultimately unsuccessful against Irish targets, it highlights the interest and willingness of hostile nation-states to target Irish interests, seeking out weaknesses in critical supply chains. The NCSC has identified a number of these campaigns at various stages of maturity.

At an EU level, the NIS2 Directive provides for coordinated security risk assessments of critical ICT supply chains[49], underscoring the importance of identifying and managing risks to safeguard the reliability, security and continuity of services, systems and products, throughout their entire lifecycle. The following pages provide real-world examples of cyberattacks targeting supply chains.

Ransomware attacks

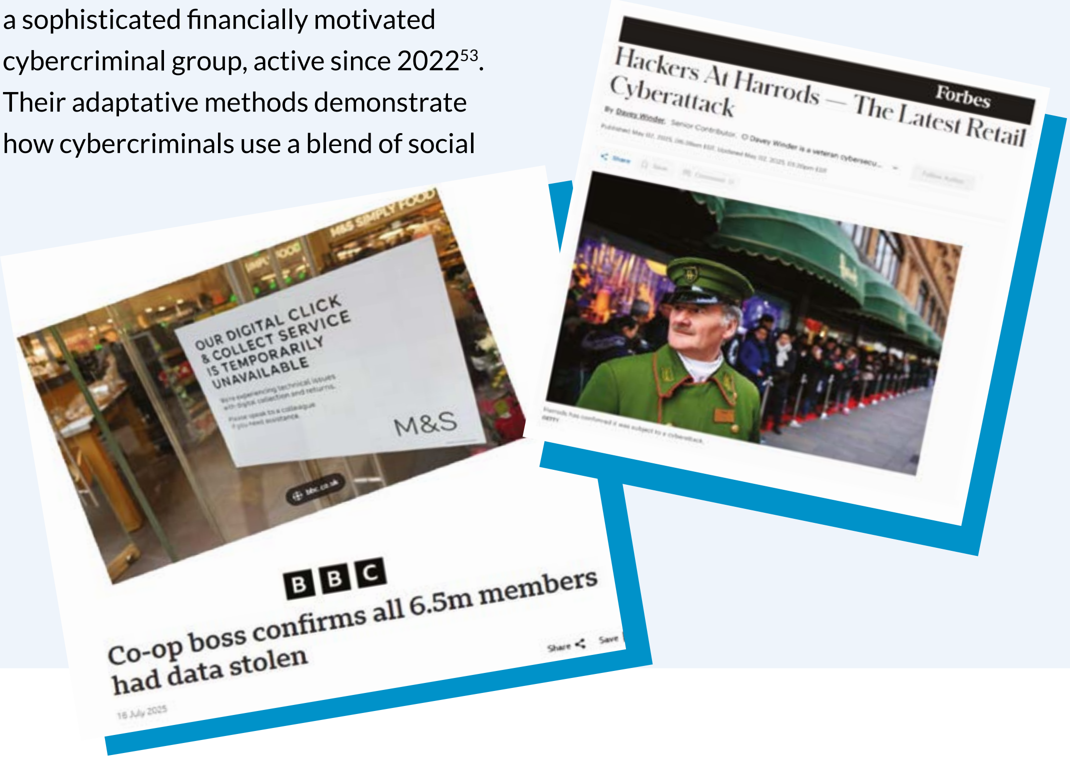
Ransomware attacks remain one of the top cyber threats facing EU member states, targeting different sectors indiscriminately, with attacks often stemming from an initial cyber security breach within the victim's supply chain[50]. Beyond substantial financial losses, these cyberattacks risk major disruption to crucial services, eroding trust in the targeted entity's ability to deliver its services.

UK retailers

In April 2025, disruptive ransomware attacks targeted several major UK retailers including Marks & Spencer, Co-op, and Harrods, causing significant disruption to online operations resulting in lost revenue, data breaches and reputational damage. One retailer has estimated the cost of the cyber-incident at around £300m[51], and a second retailer confirmed the theft of personal data for all of its 6.5 million members[52].

These cyberattacks were attributed to the threat actor Scattered Spider, a sophisticated financially motivated cybercriminal group, active since 2022[53]. Their adaptative methods demonstrate how cybercriminals use a blend of social engineering techniques to gain an initial foothold before launching technical exploits to conduct disruptive ransomware attacks.

One of the attacks reportedly involved the cybercriminal group gaining initial entry by obtaining login credentials from two employees of a third-party provider using social engineering techniques. These examples demonstrate the capability of non-state actors to cripple the operations of an entity by exploiting weaknesses in its supply chain.



Forbes

Hackers At Harrods — The Latest Retail Cyberattack

By Davey Winder, Senior Contributor. ⓘ Davey Winder is a veteran cybersecu...

Published May 02, 2025, 06:38am EDT, Updated May 02, 2025, 03:20pm EDT

Share Save Comment Follow Author

Harrods has confirmed it was subject to a cyberattack.

Getty

OUR DIGITAL CLICK & COLLECT SERVICE IS TEMPORARILY UNAVAILABLE
M&S SIMPLY FOOD
M&S
bbc.co.uk

BBC

Co-op boss confirms all 6.5m members had data stolen

Share Save

16 July 2025

Threats against availability

Threats against availability (DDoS attacks) continue to be ranked as the top threat reported by EU member states[54].

As part of a DDoS attack, threat actors can take advantage of multiple low-cost IoT devices to orchestrate a co-ordinated cyberattack, forming a botnet to target a system. Often, these low-cost devices contain insufficient cyber security controls and a lack of adherence to industry standards, contributing towards interoperability issues and basic vulnerabilities. Both non-state and state-aligned threat actors utilise DDoS attacks to advance their strategic objectives.

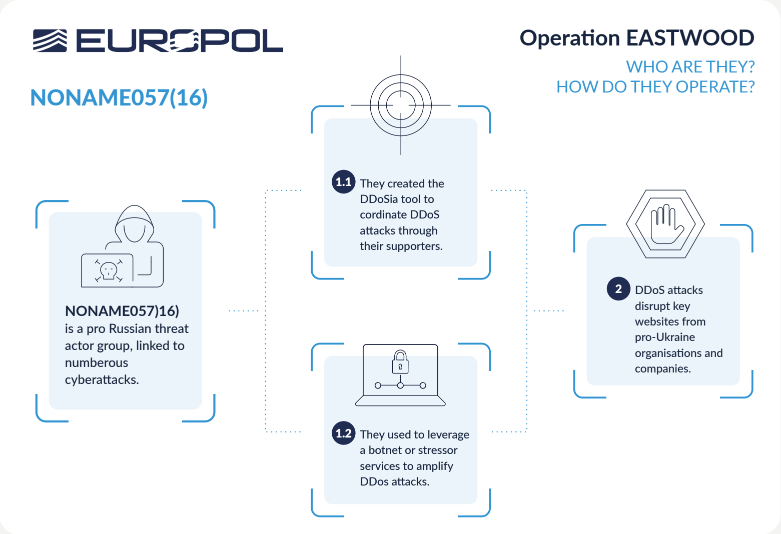
Eastwood

In July 2025, a joint international operation, known as Eastwood[55], comprising 12 countries and coordinated by Europol and Eurojust, took down the pro-Russian cybercrime group NoName057(16).

Ideologically motivated, the pro-Russian hacktivist group was responsible for multiple DDoS attacks targeting critical infrastructure, utilising an estimated network of over 4,000 supporters and forming a botnet made up of several hundred servers worldwide to generate the attack load.

Primarily targeting Ukraine, the group widened its offensive to include DDoS attacks against countries that support Ukraine, targeting critical infrastructure during high-level political events. The group executed 14 attacks against German infrastructure, targeting arms factories, energy suppliers and government organisations, impacting around 230 organisations. In Sweden, bank websites were targeted while in June in the Netherlands, the NATO Summit was targeted.

To motivate its supporters to conduct pro-Russian cyberattacks, the group mimicked game-like dynamics, hosting leaderboards, rewarding status badges and at times, paying participants in cryptocurrency, incentivising sustained involvement. Such gamified manipulation often targets young offenders, creating a game-like environment with real-world consequences.



EUROPOL

Operation EASTWOOD

WHO ARE THEY?
HOW DO THEY OPERATE?

NONAME057(16)

NONAME057)16) is a pro Russian threat actor group, linked to numberous cyberattacks.

1.1 They created the DDoSia tool to cordinate DDoS attacks through their supporters.

1.2 They used to leverage a botnet or stressor services to amplify DDos attacks.

2 DDoS attacks disrupt key websites from pro-Ukraine organisations and companies.

Indirect targeting through one-to-many attacks

Indirect targeting through one-to-many attacks, threat actors exploit the interconnected nature of supply chains and sectoral reliance on a concentrated set of suppliers. With often unclear inter-dependencies and a lack of resilience through diversification of supply, an exploited vulnerability in a single supplier can potentially trigger widespread impacts, cascading effects throughout the supply chain.

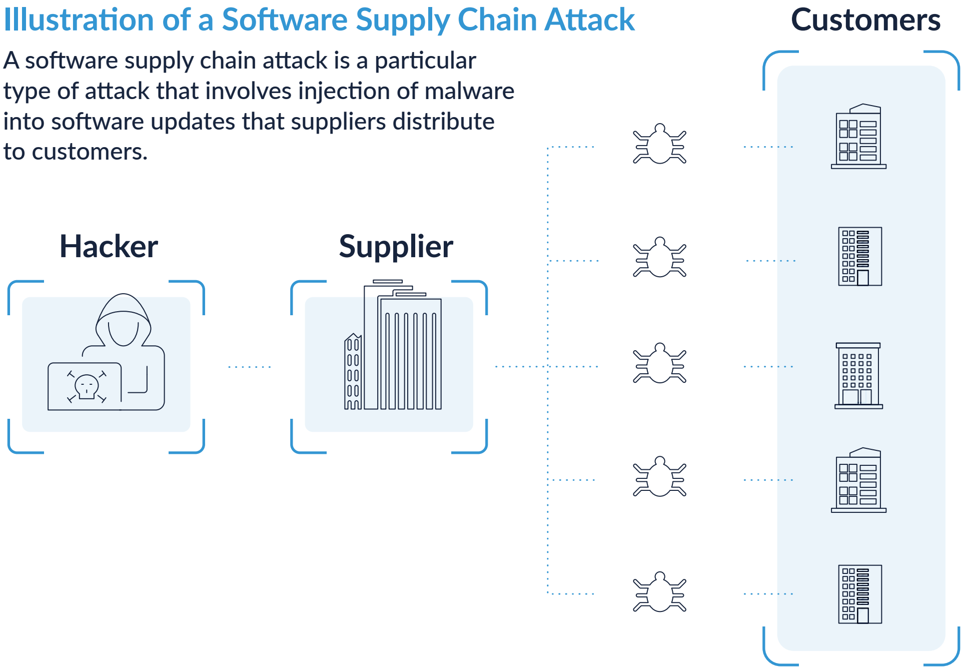
Solarwinds

The 2020 Solarwinds supply chain breach[56] is considered one of the most well-known supply chain attacks. Conducted by the sophisticated state-aligned cybergroup, APT 29[57], the incident highlights how a one-to-many attack can spread quickly from one supplier through to its many customers.

In the Solarwinds incident, malicious code was inserted into Solarwind's Orion tool before being pushed out to nearly 18,000 of Solarwinds customers around the world, providing hackers with access to multiple IT systems through a single breach. Victims of the campaign included government, consulting, telecom and other organisations across North America, Europe, Asia and the Middle East. Their goal, to conduct cyber-espionage activity against US government agencies and private corporations. In 2021, the US and UK governments attributed the compromise to Russia's Foreign Intelligence Service (SVR)[58].

Illustration of a Software Supply Chain Attack

A software supply chain attack is a particular type of attack that involves injection of malware into software updates that suppliers distribute to customers.



Over-reliance on a single supplier, system or process

Over-reliance on a single supplier, system or process can create a single point of failure, undermining an organisation's resilience to withstand a disruptive event, risking widespread operational, financial and reputational damage.

CrowdStrike

In July 2024, a seemingly simple IT incident triggered widespread technology failures around the world. A faulty software update from security vendor CrowdStrike[59] caused significant disruptions for users and services reliant on Microsoft Windows. While not a cyberattack, its disruption led to a ripple effect throughout the supply chain, rapidly escalating impacts, causing hospitals to postpone procedures, airlines to cancel flights, news channels unable to broadcast. Approximately 8.5 million systems crashed worldwide.

Despite a software fix being deployed quickly, many organisations faced prolonged recovery periods, some requiring manual intervention to restore service. A faulty software bug that managed to pass through CrowdStrike's cloud-based testing system is estimated by Insurers to have cost them at least $5.4 billion not to mention, significant brand reputation damage.

This incident indiscriminately impacted all critical sectors, highlighting the need for sectors to ensure a diversification of supply, particularly in the use of large-scale IT infrastructure.

Third country interference

Third country interference in the context of supply chain security, represents a significant risk to Ireland's national security and the safe supply of its critical services. Manufacturers or suppliers of products and services to critical sectors that are subject to third-country interference are compromised in their ability to assure supply, placing them in the category of high-risk suppliers.

Third country interference may include the unauthorised transfer of data to third countries, embedded vulnerabilities in product design or in-built back door capability. A supplier's risk profile in terms of third country interference may include:

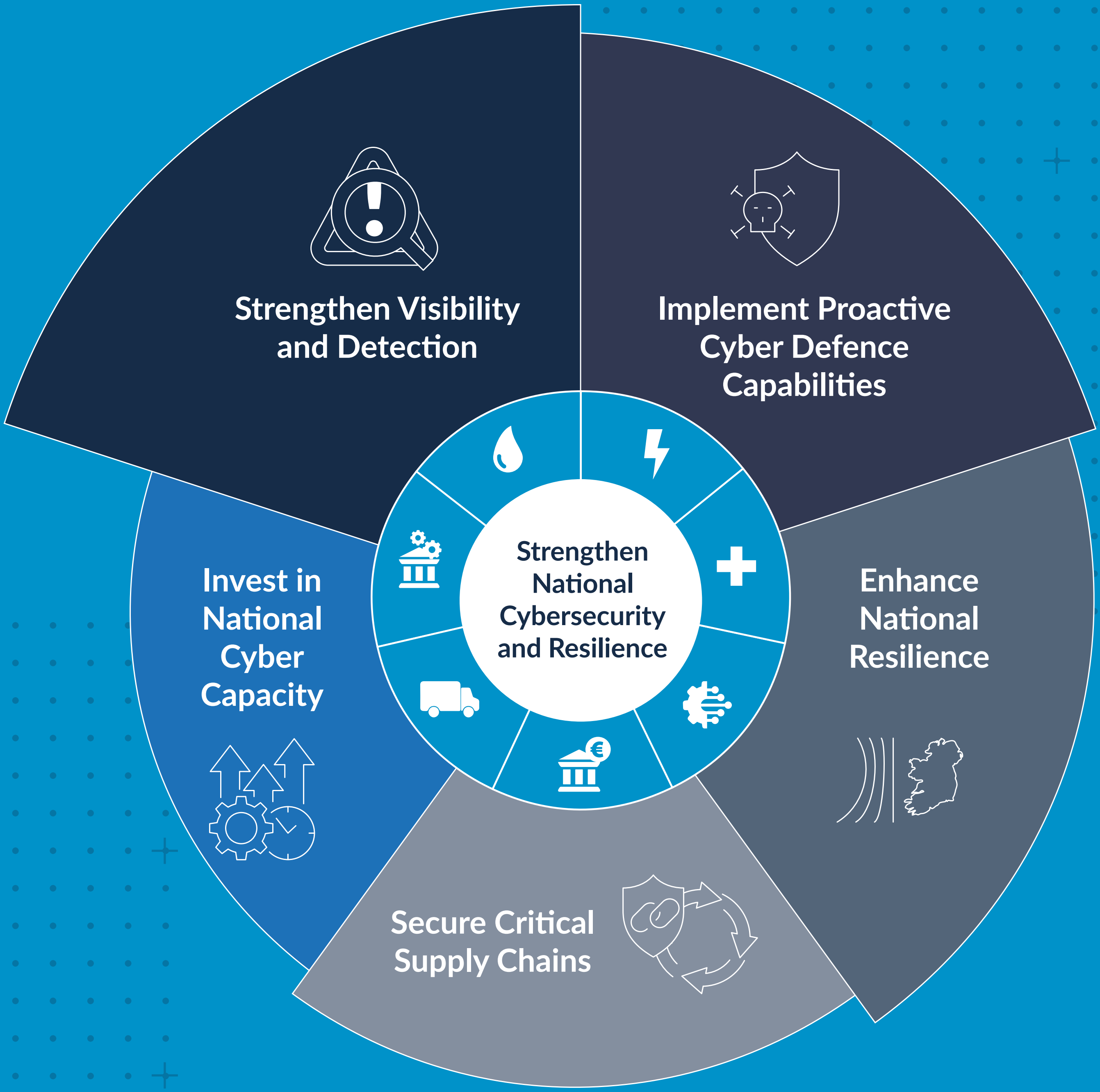
- jurisdictional exposure
- ownership or control by foreign governments
- poor cyber security practices
- a lack of transparency

It is imperative that organisations procuring services central to the operations of their business and the security of their data, perform due diligence on the cyber security of prospective partners or suppliers and the regulatory environments they operate within. The pending EU's ICT Supply Chain Security Toolbox will set out a number of strategic recommendations aimed to support both public and private entities in evaluating and managing risks related to ICT services, ICT systems, and ICT product supply chains, offering a consistent approach to securing critical supply chains.

Recommendations

The 2025 NCRA identifies systemic risks that, if realised, could undermine the delivery of essential services, disrupt critical sectors, and erode trust in government, institutions and organisations. To address these risks, Ireland should pursue a focused number of high-level policy directions. These recommendations provide a framework for the next National Cyber Security Strategy, ensuring that systemic vulnerabilities are reduced and national resilience strengthened.

The five recommendations are:


Strengthen Visibility and Detection
Implement Proactive Cyber Defence Capabilities
Enhance National Resilience
Secure Critical Supply Chains
Invest in National Cyber Capacity
Strengthen National Cybersecurity and Resilience

Recommendations

Strengthen Visibility and Detection

Systemic risks identified in this assessment are magnified by gaps in national-level situational awareness. Attacks that traverse multiple sectors or exploit shared dependencies such as cloud services or subsea cables, can develop undetected until impacts are widespread. Many state-aligned actors have a doctrine of combining cyber, information and physical sabotage operations in a coordinated manner; an ability to correlate and analyse these events is required for a coherent and resilient national response.

To mitigate this, Ireland must continue to build out its ability to monitor, detect and understand cyber and hybrid threats across critical sectors. This includes:

- Expanding State monitoring and detection capabilities in cyber and hybrid domains, ensuring adequate and timely intelligence reporting through existing national security structures, supporting both national and international information exchange.
- Expanding both the scope and scale of the NCSC Sensor Programme to actively detect malicious activity across a broader range of entities and gathering more granular telemetry data. Partner with relevant stakeholders to create a National Detection Network.
- Drawing actionable data-based insights gathered from incident reporting under NIS2 and other regulatory obligations, securely sharing key insights in real time with national partners.
- Investing in and implementing nationwide cyber defence solutions and services to support in the identification of risk, the protection of assets and detection of threats, strengthening Ireland's response to national-level cyber incidents.
- Anchoring Irish visibility within European frameworks, including the **EU cyber hubs** and the new **EU cable hubs** initiatives, both of which will be critical to protecting Ireland as an island economy reliant on transnational infrastructure.
- Implementing the national counter disinformation strategy, including the recommendation to nominate and empower a State body to monitor, detect Foreign Information Manipulation and Interference (FIMI) activities targeting Irish interests.

By strengthening national visibility, Ireland will reduce systemic blind spots and be better positioned to anticipate, and act on, cross-sectoral risks before they escalate.

Recommendations

Implement Proactive Cyber Defence Capabilities

The risks set out in this assessment highlight that reactive responses are not sufficient to protect society and the economy in today's risk environment. Developments in geopolitics, in industry and in supply chains mean that once threat actors have established persistence within critical systems, cascading disruption is difficult to contain and can readily cause widespread damage.

Ireland must move towards a more proactive cyber defence posture, intervening earlier in the attack lifecycle to prevent incidents at scale. This means:

- Deploy scanning services that identify high risk vulnerabilities across government, essential and important entities.
- Using automation and intelligence-driven tools to block malicious activity before it reaches critical networks.
- Working with private-sector providers to extend protective coverage across the wider digital ecosystem.
- Providing proactive threat assessment services to essential entities in the State as part of ongoing testing of national readiness.
- Continuing to engage in national large-scale cyber exercises and 'live fire' cyber defence exercises. Rolling out an exercise testing service to essential and important entities in the State.
- Maintaining a continuous 'cyber pulse check' to gather and analyse key cyber security metrics from entities in scope of regulation, providing a regular insight into the state of resilience at organisational, sectoral and national level, and enabling evidence-based prioritisation of supervision and enforcement activities.

Shifting the national posture "left of incident" will reduce opportunities for systemic disruption, protect critical functions more effectively, and raise the overall baseline of national resilience.

Enhance National Resilience

Systemic risks are not confined to technical failures - they also target trust in institutions and the functioning of society. State and non-state actors are increasingly willing to use cyber operations to destabilise populations and weaken democratic systems.

Ireland's resilience depends on embedding robust frameworks across all sectors and ensuring society can withstand attempts at destabilisation. This requires:

- Full implementation of the EU cyber regulation package — **NIS2, the Cyber Resilience Act, the Cyber Security Act (and its forthcoming review), and the Cyber Solidarity Act.**
- Adequate resourcing of Competent Authorities (CAs) to supervise compliance consistently, proportionately and on a risk-based approach.
- Ensuring that there are fully resourced competent national authorities and a functioning market to enable the widespread adoption and implementation of European cyber security certification framework schemes in Ireland.
- Embedding the Cyber Fundamentals Framework **(CyFun)** as the national cyber security certification scheme to guide entities in building resilience.
- Leveraging EU solidarity measures - particularly the cyber hubs, cable hubs, and cyber reserve - to strengthen Ireland's crisis response and integration with EU partners.
- Reinforcing crisis preparedness and public communication mechanisms so that services and government can maintain continuity under cyber stress.
- Undertake strategic risk assessments and stress testing as part of NIS2 compliance processes to address concentration and systemic risk.
- Supporting societal resilience by countering disinformation, protecting democratic processes, and ensuring public confidence during disruptive cyber incidents.

By implementing EU frameworks in full and extending resilience beyond infrastructure to society itself, Ireland will ensure that both services and democratic institutions remain robust in the face of systemic cyber risks.

Recommendations

Secure Critical Supply Chains

The NCRA highlights that vulnerabilities in critical ICT supply chains create some of the most significant systemic risks to Ireland. Reliance on complex, opaque, and concentrated supply chains exposes the State to embedded vulnerabilities, vendor lock-in, and third-country interference.

To address these risks, Ireland must:

- Strengthen procurement rules in government to ensure baseline cyber requirements are applied consistently.
- Use the **CyFun** framework to embed security-by-design and risk management practices across suppliers.
- Increase visibility into vendor ownership, control, and security practices.
- Ensure the State has the appropriate legal powers and can intervene where high-risk vendors pose national-level risks in critical sectors, including Government systems.
- Promote vendor diversification in critical sectors and align with EU measures including the EU ICT Supply Chain Security Toolbox.

Improving supply chain assurance will reduce systemic vulnerabilities, mitigate the risk of hostile interference, and protect essential services against single points of failure.

Invest in National Cyber Capacity

The ability to manage systemic risks depends on Ireland's capacity to sustain a skilled workforce, a strong research base, and an indigenous industry able to provide trusted solutions. The NCRA has highlighted that shortages of skills and gaps in research capability exacerbate national exposure to risk.

Ireland should:

- Expand cyber education and training pathways from schools through to advanced professional programmes.
- Build capacity within the public sector, regulated entities and SMEs to implement resilience measures effectively, including through an expanded / updated cyber security improvement programme.
- Establish a **national cyber security research centre of excellence** to bring together government, academia, and industry to ensure Ireland is at the cutting edge of innovative cyber security research and solutions.
- Provide targeted support for indigenous cyber security providers developing innovative cyber products and services, enabling them to scale and compete internationally.
- Align skills and research investment, including measures being brought forward from cyber industrial strategy, ensuring coherence with Ireland's broader digital and economic policies.
- Ensure Ireland has a resourced and functioning national security vetting and clearance system so that Irish companies and research bodies can participate in classified cyber security research projects and initiatives.

Investment in people and innovation will ensure that Ireland has the capacity not just to respond to today's threats but to anticipate and shape the next generation of resilience measures.

These recommendations provide a framework for the next National Cyber Security Strategy, ensuring that systemic vulnerabilities are reduced and national resilience strengthened.

Annex I

Annex II

Annex III

Annex IV

Annex I

NCRA Methodology

2022 National Cyber Risk Assessment

In 2022, Ireland's first NCRA report was produced. The overall assessment process was completed with the assistance of a steering group consisting of members from An Garda Siochana, the Office of Emergency Planning, the Defence Forces, the National Security Analysis Centre, and representatives from the National Competent Authorities. Assessing the threat landscape at that time, the report examined systemic cyber risks faced by the State's critical services.

The 2022 National Cyber Risk Assessment followed a three-step process, applying the methodology published by Irelands Office of Emergency Planning (OEP), referred to in the document as the 'Strategic Emergency Management Guideline 3 – Critical Infrastructure Resilience – Version 2'[60]. The 3-step approach included:

1. Identify the National Critical Functions (NCFs)

This step involved the identification of all NCFs in the country.
The Office of Emergency Planning defines critical infrastructure (CI) as:

> *'An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of the people and the disruption or destruction of which would have a significant impact in the State as a result of failure to maintain those functions. CI provides services and utilities in order to facilitate efficient functioning of the economy, the safety and wellbeing of its citizens and the continual functioning of government.'*

The CISA National Critical Function set[61] and the NIS2 Directive[62] were used as the basis to identify the NCFs for the State.

2. Identify entities and assign criticality rating

Applying criticality metrics defined by the OEP methodology to data collected from entities across the State, the 2022 NCRA was able to identify CNI and the critical sectors they operate within. These identified sectors continue to be categorised as critical for the 2025 NCRA. Critical sectors are:

- Energy
- Health
- Digital
- Banking
- Transport
- Public Admin
- Water

3. Identify systemic national infrastructure cyber risks

For step 3 of the process, the national cyber risk assessment, using the World Economic Forum (WEF) definition for 'systemic cyber risk', examined the systemic risks and their potential for cascading consequences within and between the State's CNI sectors.

> **Systemic Cyber Risk (WEF Definition[63])**
>
> *Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security.*

2025 National Cyber Risk Assessment

Considering the changing threat landscape in the intervening years, the 2025 NCRA has undertaken a review of the extensive dataset collected by the NCRA in 2022, now forming a baseline that has been further developed in 2025 to deliver a forward-looking assessment of technology trends and evolving threats, with the aim of identifying critical sectors most exposed to significant systemic risks.

The analysis conducted as part of the 2025 assessment has included a comprehensive review of the global threat landscape, an in-depth examination of cyber incidents observed here in Ireland and active engagement with partner agencies and consultation with National Competent Authorities (NCAs) representing each of Ireland's critical sectors. Similar to the 2022 assessment, a number of 'reasonable worst-case risk scenarios' were created to provide a sense of the types of cyber threats posed and how systemic risk might manifest to impact, causing direct and 'spill-over' effects across multiple sectors.

Using the metrics collected as part of the 2022 assessment, probability levels for systemic cyber risks were determined and mapped per sector.

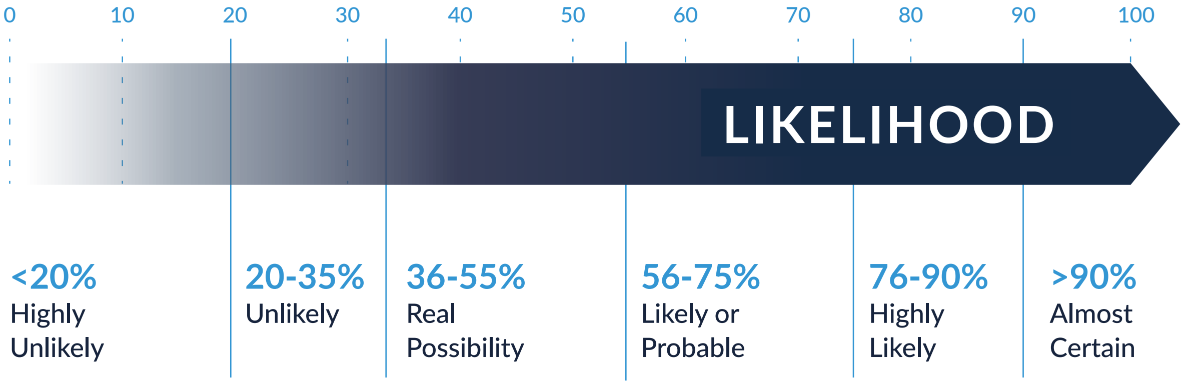
To assess probability, two key factors need to be considered, likelihood and impact[64]:

- Likelihood of occurrence refers to the probability that a given threat can successfully exploit a given vulnerability (or set of vulnerabilities).
- Impact refers to the magnitude/severity of harm that can be expected to result from consequences of the risk occurring.

When mapping both likelihood and impact levels, the following scales were applied.

Likelihood Scale:

Likelihood is represented as the percentage chance of a 'reasonable worst-case risk scenario' occurring in the assessment timescale, represented as follows:



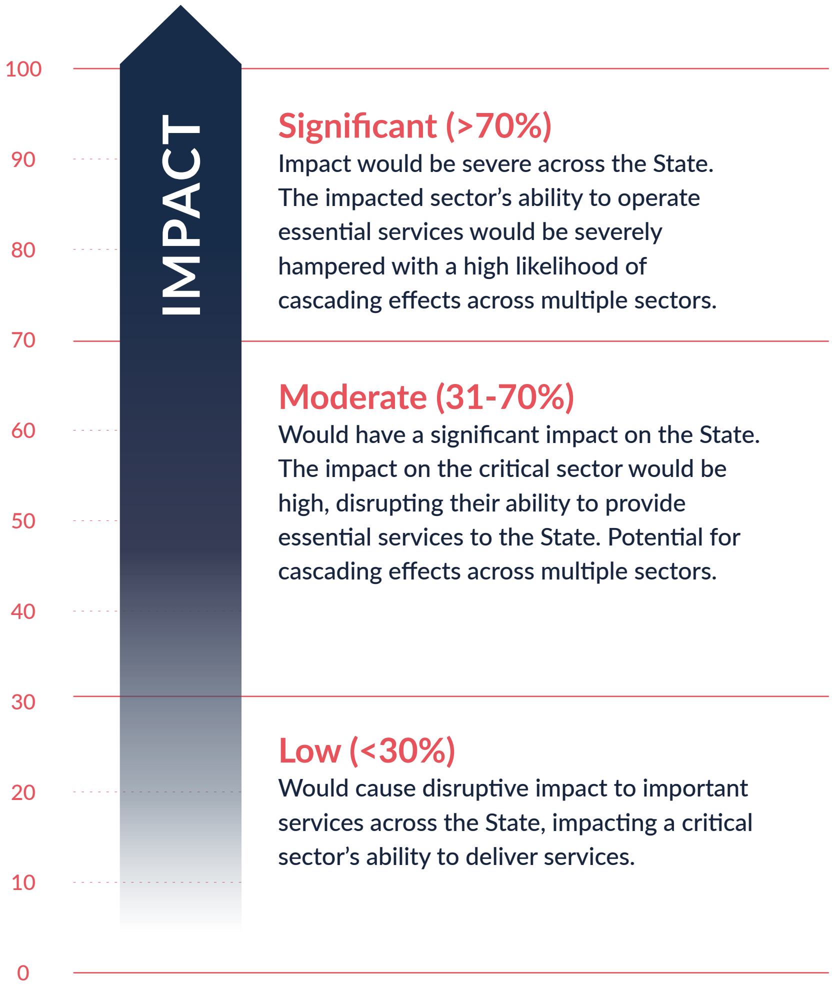
Impact Scale:

Impacts can be wide ranging, from direct IT outages to widespread disruption to important and essential services, or even societal or economic impacts. Impact levels are represented below:

Applying an all-hazards approach, the 2025 NCRA evaluated the most serious systemic risks posed by both state-aligned and non-state actors, including for example, insider threat, cybercriminals and hacktivists. Other contributing factors considered, include for example, human error or system failures. Each carrying the potential to cause significant impact to Ireland's CNI.

Analysing the threat landscape and considering 'reasonable worst-case risk scenarios', intentional acts (i.e. cyberattack) were assessed to represent the top systemic risk facing critical infrastructure.

When assessing the probability (likelihood versus impact) of a successful cyberattack being perpetrated against critical sectors, probability levels were adjusted to reflect the changing 2025 threat landscape in comparison to results first recorded as part of the 2022 NCRA.



Significant (>70%)
Impact would be severe across the State. The impacted sector's ability to operate essential services would be severely hampered with a high likelihood of cascading effects across multiple sectors.

Moderate (31-70%)
Would have a significant impact on the State. The impact on the critical sector would be high, disrupting their ability to provide essential services to the State. Potential for cascading effects across multiple sectors.

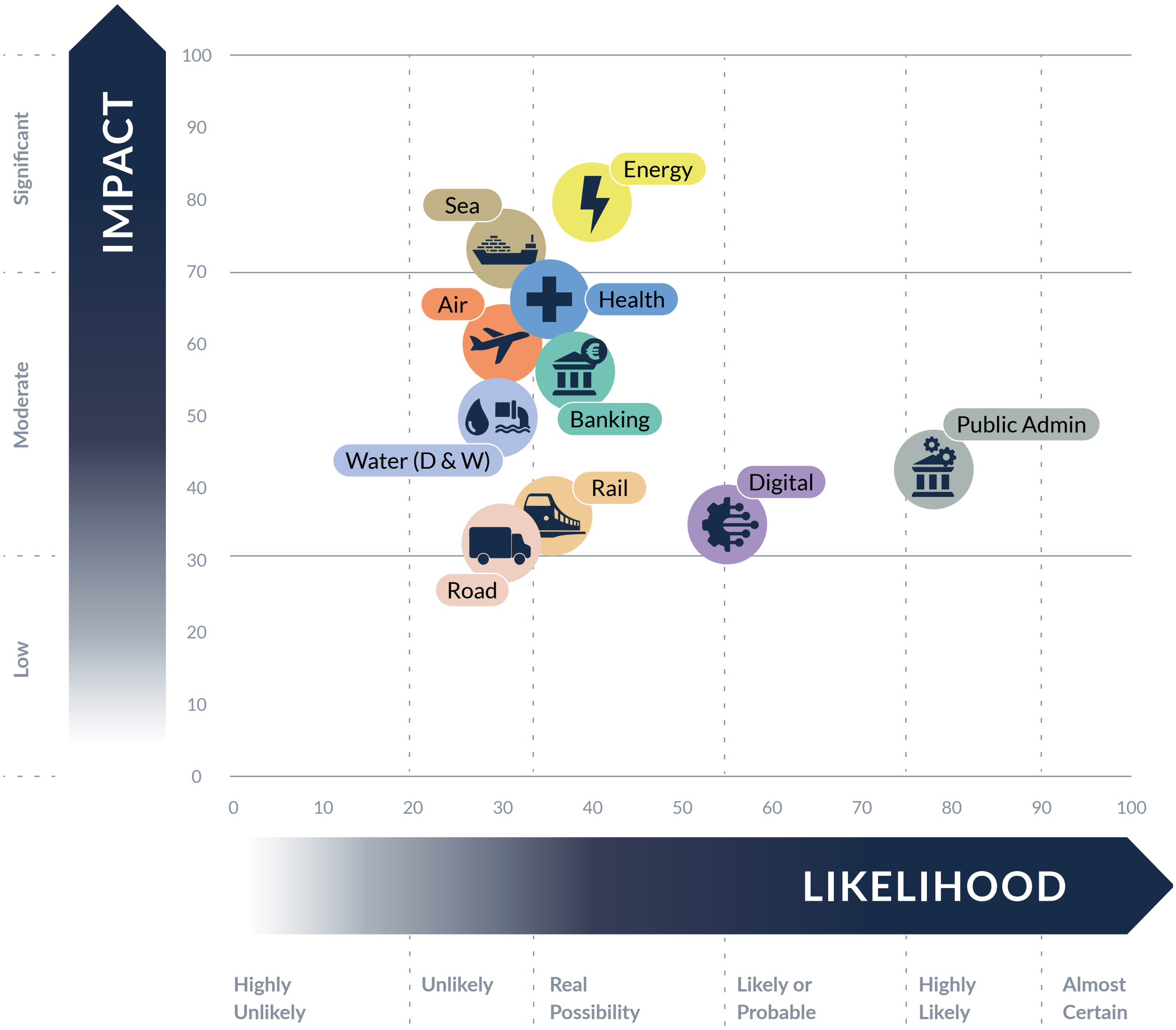
Low (<30%)
Would cause disruptive impact to important services across the State, impacting a critical sector's ability to deliver services.

GUEST HOUSE
RESTAURANT
EST. 1977
& CO LTD
INSURANCE &
FINANCIAL
TOYS & GIFTS
SPORTS
BIKE SALES
REPAIRS
RENT-A-BIKE
TAXI SERVICE
BAR
Food and Wine

2022 NCRA Results

Using the dataset collected during the 2022 NCRA, the probability of systemic cyber risk per critical sector, was mapped as follows:

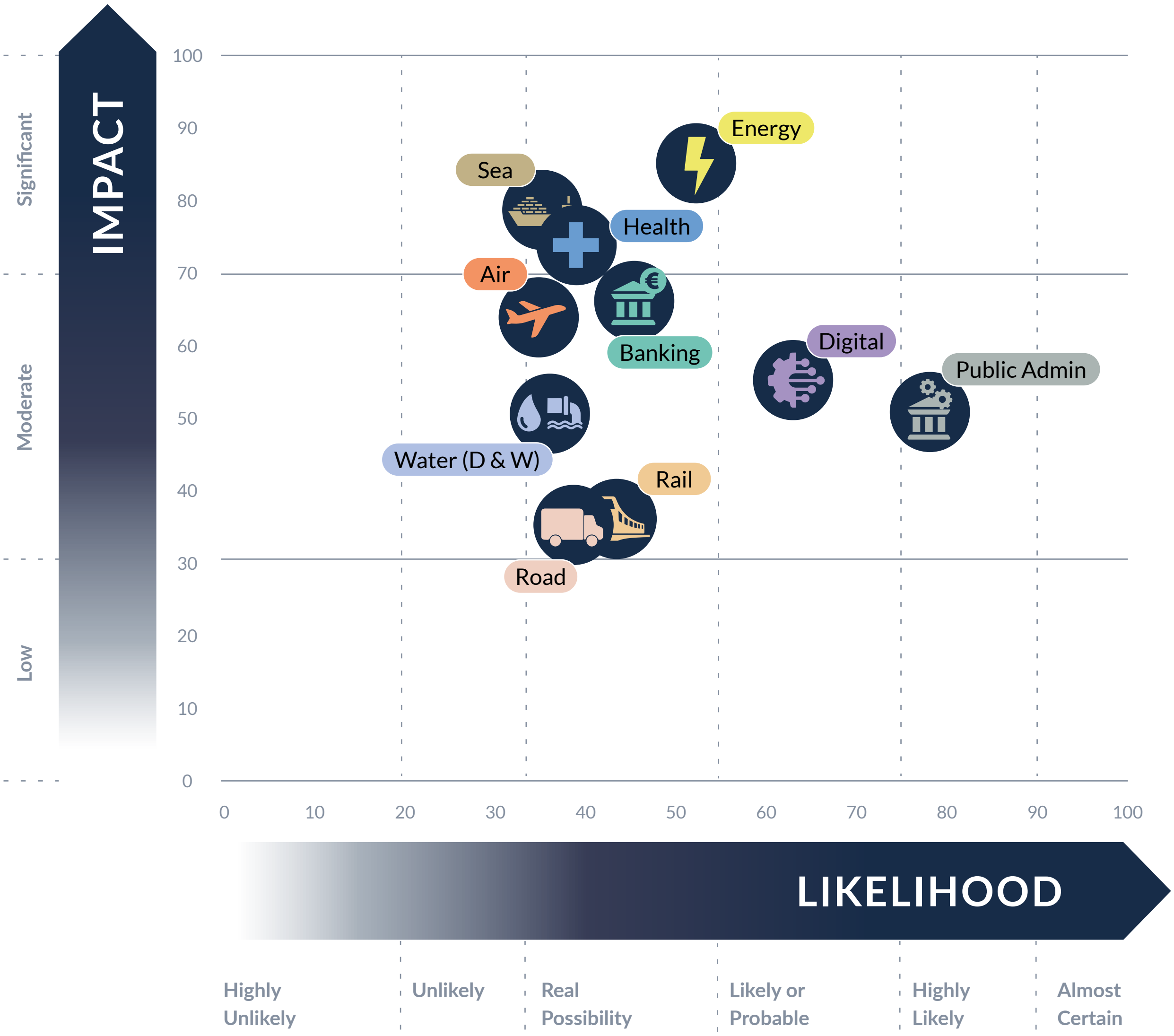
2022 NCRA Assessment



2025 NCRA Results

Having applied the methodology outlined earlier to each of the sectors deemed as critical, the following results were obtained. The key factors in the revised risks ratings are outlined in the next section.

2025 NCRA Assessment



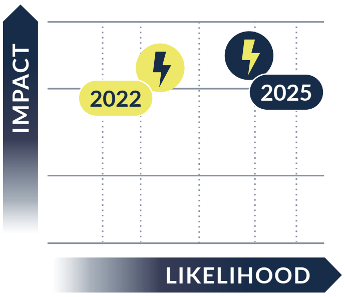
Annex II

Sector-Specific Risk Assessment

A high-level rational explaining the adjustments made in 2025 are outlined below, per critical sector:

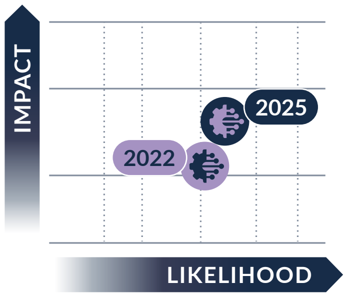
Critical Sector: Energy

	Likelihood	Impact
2022 v 2025 Adjustment	↑	↑
Adjustment rational	**Likelihood of a successful cyberattack:** Increased to the upper end of 'real possibility'. Critical functions servicing energy infrastructure are increasingly reliant on digital capability, including greater integration of OT/IoT sensor networks into centralised core network services, allowing for enhanced, real-time, remote monitoring and management. This network evolution contributes to a more expansive attack surface, with multiple access points to protect. Additionally, geopolitical events have demonstrated the increased likelihood of cyberattacks targeting energy infrastructure, directly impacting whole of society (e.g. Ukraine).	**Impact from a successful cyberattack:** Already rated as 'significant' during the 2022 NCRA, the 2025 levels have been raised further, to reflect the substantial potential for spill-over effects that could result in widespread disruption of essential societal functions across multiple sectors. The risk of such spill-over effects is heightened due to the growing reliance by multiple sectors on digital infrastructure, including cloud, internet and communications, all dependent upon a reliable and stable energy supply.



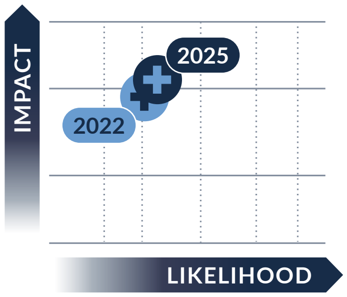
Critical Sector: Digital

	Likelihood	Impact
2022 v 2025 Adjustment	↑	↑
Adjustment rational	**Likelihood of a successful cyberattack:** Moved from 'Real Possibility' to 'Likely or Probable'. Increased to reflect the growing number of cyberattacks targeting digital infrastructure. The Digital sector underpins all critical sectors, through the provision of high-capacity, data-driven networks, 24 x 7 communications via a host of global cloud providers, and high-tech data centres. It inherently poses as a high-value target for those intent on causing direct or indirect cross-sectoral disruption. However, there is maturity in this sector regarding resilience and business continuity planning, supporting its preparedness to recover from successful cyberattacks.	**Impact from a successful cyberattack:** Moved to the upper end of 'moderate'. As organisations, industry and public services advance digital transformation plans, dependencies on this sector increase. Consequently, any impact to operational stability will have increased consequences.



Critical Sector: Health

	Likelihood	Impact
2022 v 2025 Adjustment	→	↑
Adjustment rational	**Likelihood of a successful cyberattack:** Remains unchanged at 'real possibility' level as it was given this high rating shortly following the HSE attack in 2022 and following the current assessment, it is considered to be at the correct level for 2025. The HSE cyberattack in 2022 demonstrated how a critical sector can be subjected to a significant disruptive cyber campaign.	**Impact from a successful cyberattack:** Assessed to be 'significant', raised from its previously rated upper range of 'moderate'. Like other sectors, health is embracing digitally enabled services, designed to manage end-to-end interactions with the health service (e.g. patient records, appointments, referrals, follow-up care, etc.). Any disruption has the potential to have a significant and immediate impact on the delivery of health services to the public.



Critical Sector: Banking

	Likelihood	Impact
2022 v 2025 Adjustment	↑	↑

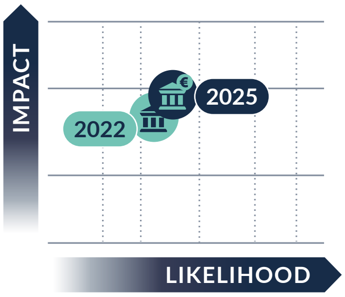
Adjustment rational

Likelihood of a successful cyberattack: Is assessed to have slightly increased but remains within the likelihood level of 'Real Possibility'. Like other sectors, the banking sector has increased reliance on third parties, creating a more expansive attack surface area.

Coupled with increased sophistication and frequency of cyberattacks and a lower barrier of entry for threat actors, this presents network defenders with an increased challenge when protecting their networks from successful attacks. With increasing public adoption of online payment applications, the banking sector attracts a broad range of cybercriminals and opportunists seeking to leverage this expanded attack surface for financial gain.

However, there is continued improvement in cyber security maturity levels and controls in the banking sector, including following the introduction of DORA in January 2025.

Impact from a successful cyberattack: Increased to the very upper end of 'moderate' and the threshold of 'significant'. With the widespread adoption of online banking services and payment methods, consumers and businesses have formed a greater dependency on the banking sector. Consequently, any significant impact on the banking sector for a prolonged duration, could have an immediate and wide-spread effect on the population and economy.



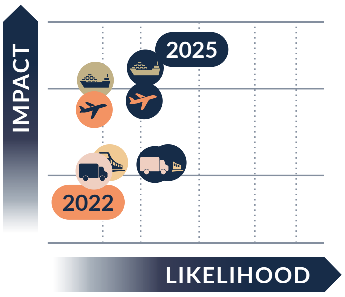
Critical Sector: Transport

	Likelihood	Impact
2022 v 2025 Adjustment	↑	→

Adjustment rational

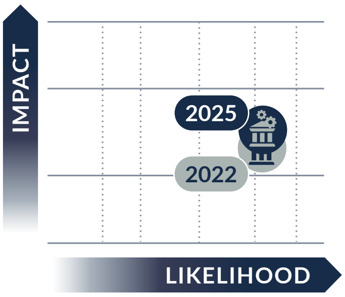
Likelihood of a successful cyberattack: Road and Rail assessed to have increased towards a 'real possibility'. The transport sector is undergoing a significant digital transformation, including greater automation and interconnected functionality, significantly transforming future transport services. Paired with increased storage of large volumes of personal data, these factors present transport services as an attractive target for cybercriminals (financial exploit) or hacktivists (ideological campaigns seeking to gain attention).

Impact from a successful cyberattack: Remains unchanged from 2022 assessed criticality levels. Transport is a mature sector, with strong regulatory oversight and is seasoned in crisis response plans. If such preparedness plans are kept updated to account for evolving cyber threats, impact rating levels can remain unchanged.



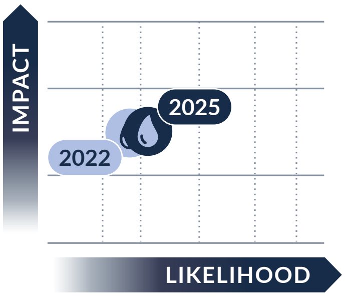
Critical Sector: Public Admin

	Likelihood	Impact
2022 v 2025 Adjustment	→	→
Adjustment rational	**Likelihood of a successful cyberattack:** A cyber-attack against the Public Administration sector remains assessed as 'highly likely'. Public Administration systems and networks support key societal functions and store large volumes of sensitive information. In a dynamic geopolitical environment, threat actors continue to target public administrative services to further strategic objectives.	**Impact from a successful cyberattack:** Remains at 'moderate' level as systems and services are managed across local, regional and national levels. As a mature sector, many services include manual procedures that can be put in place, if necessary, to mitigate impact to online resources. Regular crisis preparedness exercises are undertaken to ensure response strategies can be actioned effectively, when needed.



Critical Sector: Water

	Likelihood	Impact
2022 v 2025 Adjustment	↑	→
Adjustment rational	**Likelihood of a successful cyberattack:** Increased from 'Unlikely' to 'Real Possibility'. Many cyberattacks targeting OT devices, are location agnostic. Critical infrastructure including that of the Water sector, comprises components sourced through global supply chains. These components could be targeted solely based on their country of origin as part of geopolitically motivated cyberattacks.	**Impact from a successful cyberattack:** Remains unchanged at moderate due to the distributed and diverse access to water sources and treatment methods around Ireland.



Annex III

Glossary of Key Terms

Key Terms

Backdoor

Bypassing traditional security access measures, this is an unauthorised point of entry into a user’s computer or network systems. Backdoors can be a legitimate feature, often introduced by developers to provide remote access to support troubleshooting, software maintenance or other such system activities. Backdoors however provide attackers covert means to bypass normal authentication, gaining unauthorised access to computers or systems.

Bot and Botnet

A **bot** is an internet-connected device, that is infected with malware without the owner’s awareness. Threat actors can then seize remote control of the infected device to perform a malicious task. A **botnet** comprises a group of these infected devices, which are then utilised by a threat actor to carry out coordinated and highly distributed attacks.

Cyber-espionage

This is a type of cyberattack where threat actors utilise digital methods to infiltrate systems and steal sensitive information without the knowledge or consent of victim. Often requiring advanced techniques to remain undetected for long periods of time, cyberespionage is typically conducted by sophisticated, well financed state-aligned threat actors.

Denial of Service (DDoS)

A **Denial of Service (DoS)** attack is an attempt to make a system unavailable to the intended users. Denial of service is typically accomplished by flooding the targeted machine or resource with requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. A DoS attack comes from a single system, can range in duration and may target more than one site or system at a time. An attack becomes a **Distributed Denial of Service (DDoS)** when it comes from multiple systems instead of just one.

Hacktivism

A blend of hacking and activism. Hacktivists are often ideologically motivated, using hacking tactics to promote a political agenda.

Internet of Things (IoT)

Describes a network of physical devices that are embedded with sensors, processing ability, software and other technologies that enable the connection and transfer of data with other devices over the Internet or other connected networks.

Living-off-the-land (LotL)

LotL describes a technique in which threat actors use native, legitimate tools within the victim's system to sustain and advance an attack. Using pre-existing tools rather than deploying malware, the intruders can blend into the normal operations of a victim's system, avoiding detection.

Malware

Short for "malicious software", refers to any software or code intentionally designed to cause harm or disruption to systems.

Operational Technology (OT)

Refers to the hardware and software used to monitor and control industrial systems and processes, typically in industrial environments in sectors like manufacturing, energy and utilities.

Pre-positioning

Refers to tactics used by threat actors to establish a foothold within IT networks, enabling them to execute disruptive or destructive cyberattacks at a future time, typically during a crisis or conflict.

Reconnaissance

The preliminary phase of a cyberattack through which threat actors gather information about their target before launching an attack. Conducting systematic scanning of systems, a threat actor gathers information and identifies vulnerabilities to facilitate a future compromise.

Ransomware

Is a type of malware that encrypts the victim's personal data until a ransom is paid.

Script Kiddies

A pejorative term for an inexperienced or unskilled individual who uses malicious scripts or programs developed by others to conduct cyberattacks, often without a deep understanding of the systems targeted.

Annex IV

Bibliography

1. https://www.europol.europa.eu/publications-events/main-reports/iocta-report
2. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
3. https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/national-cyber-security-strategy/
4. https://www.ncsc.gov.ie/ncra/
5. https://www.weforum.org/publications/understanding-systemic-cyber-risk/
6. https://www.gov.ie/en/department-of-defence/publications/strategic-emergency-management-sem-national-structures-and-framework/
7. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
8. https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/
9. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
10. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union
11. https://www.consilium.europa.eu/en/press/press-releases/2025/05/28/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-behaviour-in-cyberspace-against-czechia/
12. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications
13. https://attack.mitre.org/groups/G1045/
14. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
15. https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access
16. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a
17. https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear
18. https://attack.mitre.org/groups/G0034/
19. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

20. https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations

21. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

22. https://www.picussecurity.com/resource/blog/volt-typhoon-living-off-the-land-cyber-espionage

23. https://www.fbi.gov/news/speeches-and-testimony/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party

24. https://cloud.google.com/blog/topics/threat-intelligence/chinese-espionage-tactics

25. https://attack.mitre.org/groups/G1017/

26. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

27. https://op.europa.eu/en/publication-detail/-/publication/93728fb6-5238-11f0-a9d0-01aa75ed71a1/language-en

28. https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

29. https://merlin.obs.coe.int/article/10222

30. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC_Report_Russian_Influence_and_Paris_2024.pdf

31. https://research.checkpoint.com/2024/disinformation-campaign-moldova/

32. https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners/

33. https://commission.europa.eu/publications/report-2024-elections-european-parliament_en

34. https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

35. https://www.zscaler.com/blogs/security-research/Gen-AI-used-phishing-websites-impersonating-brazil-s-government

36. https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

37. https://www.crowdstrike.com/adversaries/famous-chollima/

38. https://www.justice.gov/usao-ndga/pr/four-north-koreans-charged-nearly-1-million-cryptocurrency-theft-scheme

39. https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/

40. https://insights.integrity360.com/cve-2025-3248-rce-flaw-in-langflow-framework-for-building-ai-agents-exploited-by-attackers#:~:text=The%20vulnerability%20is%20tracked%20as%20CVE-2025-3248%20and%20is,an%20API%20endpoint%20flaw%2C%20in%20the%20%2Fapi%2Fv1%2Fvalidate%2Fcode%20endpoint.

41. https://www.aim.security/lp/aim-labs-echoleak-blogpost

42. https://nvd.nist.gov/vuln/detail/CVE-2025-32711

43. https://tech.news.am/eng/print/6073/

44. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

45. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

46. https://www.gov.uk/government/publications/open-source-software-best-practice-supply-chain-risk-management/open-source-software-best-practices-and-supply-chain-risk-management

47. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

48. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

49. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

50. https://www.bbc.com/news/articles/c0el31nqnpvo

51. https://www.bbc.com/news/articles/cql0ple066po

52. https://attack.mitre.org/groups/G1015/

53. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

54. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

55. https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf

56. https://attack.mitre.org/campaigns/C0024/

57. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf

58. https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

59. https://www.gov.ie/en/department-of-defence/publications/strategic-emergency-management-sem-national-structures-and-framework/

60. https://www.cisa.gov/topics/risk-management/national-critical-functions

61. https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2

62. https://www.weforum.org/publications/understanding-systemic-cyber-risk/

63. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Image Credits:

Shutterstock, Unsplash, Freepik and Vecteezy

Contact Details

National Cyber Security Centre, Tom Johnson House,
Haddington Road, Dublin 4, Ireland, D04 K7X4

✉ info@ncsc.gov.ie

☎ +353 1 6782333

𝕏 https://twitter.com/ncsc_gov_ie

www.ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre