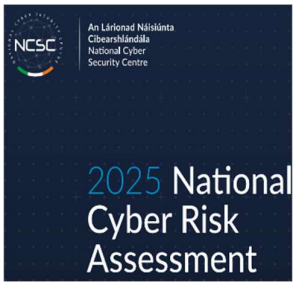
Smarttech
YOUR 24/7 SECURITY PARTNER

Changing Threat Landscape for Public Administration Organisations Linked to Ireland Hosting the EU Presidency

January 2026

Introduction

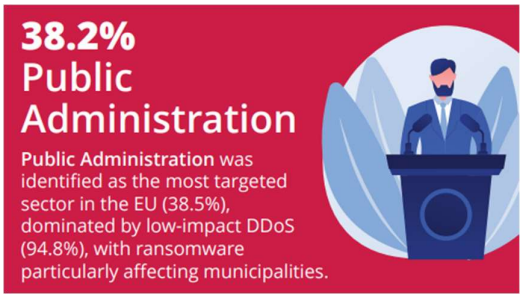
Ireland assumes the EU Presidency in the second half of 2026. This is a time for opportunity due to increased influence, visibility, and responsibility but there are also risks.



The 2025 National Cyber Risk Assessment by the National Cyber Security Centre highlights that increasing digitalisation and technological advancement have made the threat landscape more complex, with potential for significant cross-sectoral impacts. The assessment identifies three systemic risks:

- the dynamic geopolitical environment,
- evolving technology and its security implications
- and vulnerabilities in supply chain security.

ENISA's 2025 Threat Landscape report notes that public administration is the most targeted sector across Europe, accounting for 38.2% of all reported incidents. These campaigns are largely hacktivist-driven, motivated by ideology and geopolitics, often linked to EU support for Ukraine. The vast majority of attacks were Distributed Denial of Service (DDoS) (94.8%), aimed at disrupting critical services and undermining operational continuity. However, a significant number of municipalities were targeted with ransomware.



This report will examine the changing threat landscape for public administration organisations linked to the EU Presidency, and some of the steps that can be taken to mitigate risks.

Why Does Hosting the EU Presidency Need to be Considered a Risk?

Holding the EU Presidency significantly raises Ireland's international visibility. During this period, Ireland will host high-level meetings where ministers and officials from across Europe negotiate legislation, sanctions, security policy and foreign affairs.
This means:

- Large volumes of sensitive political, economic and security-related information will flow through Irish systems.
- Ireland becomes a single coordination point for EU-level decision-making.

For attackers, this creates a simple equation: they don't need to compromise 27 countries, they only need to compromise the one coordinating them.

Targeting the Presidency country offers opportunities to:

- Steal negotiation positions or confidential documents
- Leak or manipulate information to cause political embarrassment
- Disrupt meetings or communications at strategically sensitive moments
- Influence decision making processes, as public administration organisations may be concerned of the potential consequences to their cyber security as a result of political and economic decisions.


RTÉ

Ukraine, Russia and the shadows that will fall on Ireland's EU presidency

Updated / Sunday, 4 Jan 2026 12:05

Critics say EU policymakers have underestimated the scale of change Donald Trump wants to engineer in Europe and the US

By Tony Connelly
Europe Editor

Who Are the Attackers?

The cyber threat landscape is not made up of a single type of adversary. In practice, Ireland faces a broad ecosystem of attackers, each with different motives.

- **Financially Motivated Cyber-Criminals**

  These are organised, professional groups whose primary goal is money. They operate ransomware campaigns, steal data, and increasingly function like businesses, renting tools, running helpdesks, and using AI to improve phishing and fraud.
  Ireland is attractive to them because it is:
  - Highly digital
  - Data-rich
  - Home to organisations where disruption can have wide knock-on effects


BBC

JLR hack is costliest cyber attack in UK history, say analysts

22 October 2025

Share Save

Joe Tidy
Cyber correspondent, BBC World Service

- **State-Backed or State-Aligned Actors**

  These groups are linked directly or indirectly to foreign governments. Their objectives are strategic rather than financial: espionage, intelligence gathering, and quiet access to decision-making processes.

  During the EU Presidency, Ireland becomes especially valuable to these actors because access to Irish systems can provide insight into EU negotiations and policy direction.

- **Hacktivist and Ideological Groups**

  While often less sophisticated, these groups can still cause disruption through website defacements or denial-of-service attacks.

  They tend to target high-profile events simply because they attract attention.

Ireland's Strategic Digital Importance

Ireland's cyber risk is not only political, it is structural. Ireland hosts significant concentration of major global data centres and several critical transatlantic subsea internet cables carrying traffic between Europe and the United States. This infrastructure underpins cloud services, communications, logistics and business operations across Europe. As a result, a cyber incident in Ireland is rarely just an Irish issue.

An outage or compromise affecting major data centre, or a cable landing station can have continent-wide consequences. For attackers, this creates leverage: a relatively small country with infrastructure that supports large parts of the European digital economy.

The Most Likely Cyber Threats Today

The most common and impactful attack types of organisations should expect include:

- Ransomware — systems encrypted and held to ransom
- DDoS attacks — public-facing services overwhelmed and taken offline
- Espionage intrusions — attackers quietly embedded in networks to observe or exfiltrate data
- AI-powered social engineering — highly convincing phishing emails, messages or voice impersonation

These threats are particularly effective during periods like the EU Presidency because:

- Communication volumes increase
- Temporary systems and new platforms are deployed
- International contacts multiply
- Staff are busier and decision-making is more pressured

Cybersecurity Risks of Hosting the EU Presidency

During the Presidency, it is assessed as highly likely that there will be an increase in activity in the cyber domain, including:

- Increased espionage attempts targeting government systems and suppliers
- Disruption-focused attacks against websites, payment systems or communications to create embarrassment or delay EU business
- Targeting of critical digital infrastructure, where impact extends beyond Ireland
- Disinformation campaigns, where even minor outages are amplified using fake documents, audio or misleading narratives

The Supply Chain — the Primary Target

Attackers consistently choose the easiest path in. Increasingly, that path runs through smaller suppliers rather than large, well-defended organisations.

Any business connected to government, EU-related work or critical services becomes part of the risk picture — regardless of size.

Organisations to be especially mindful

- Suppliers to government departments (IT, consulting, logistics, events, communications)
- Cloud and data-centre operators, where disruption has multi-country impact
- Telecoms and internet infrastructure providers, including subsea cable operators
- Critical services such as energy, transport, healthcare and finance

No organisation should underestimate its value to attackers simply because it is “not the main target”.

Practical Steps to Take Now:

1. **Lock Down Access**
   Audit and strictly limit any access connected to government or EU-related systems. Attackers will actively search for weak links in supplier networks.
2. **Patch Quickly**
   State-aligned actors exploit newly disclosed vulnerabilities rapidly. Slow patching becomes a serious risk during periods of heightened attention.
3. **Prepare for Disruption**
   Organisations supporting government, media or events should assume phishing waves or DDoS attempts around key dates. Response plans should be simple, rehearsed and understood.
4. **Train Staff for Targeted Phishing**
   Expect a surge in convincing, context-aware phishing and misinformation. Early detection by staff remains one of the most effective defences.

5. **Strengthen Monitoring and Response**
   Tools matter, but speed matters more. Faster detection and containment dramatically limit impact.

Conclusion - Resilience, Not Invisibility

It is unrealistic to think Ireland can make itself "uninteresting" to attackers. Ireland is already attractive because it is:

- Highly digital
- A major data-centre hub
- A landing point for critical subsea cables
- Temporarily central to EU decision-making

The real question is not whether attackers will try, but what happens when they do.
The lesson from past incidents is clear: resilience (rapid detection, decisive response, and limited impact) is what separates manageable incidents from national-level disruption.

Ireland has made real progress since the 2021 HSE attack. Cybersecurity is now understood as a national resilience and service-continuity issue, not just an IT problem. Investment has increased, leadership engagement is stronger, and collaboration with the National Cyber Security Centre has improved.

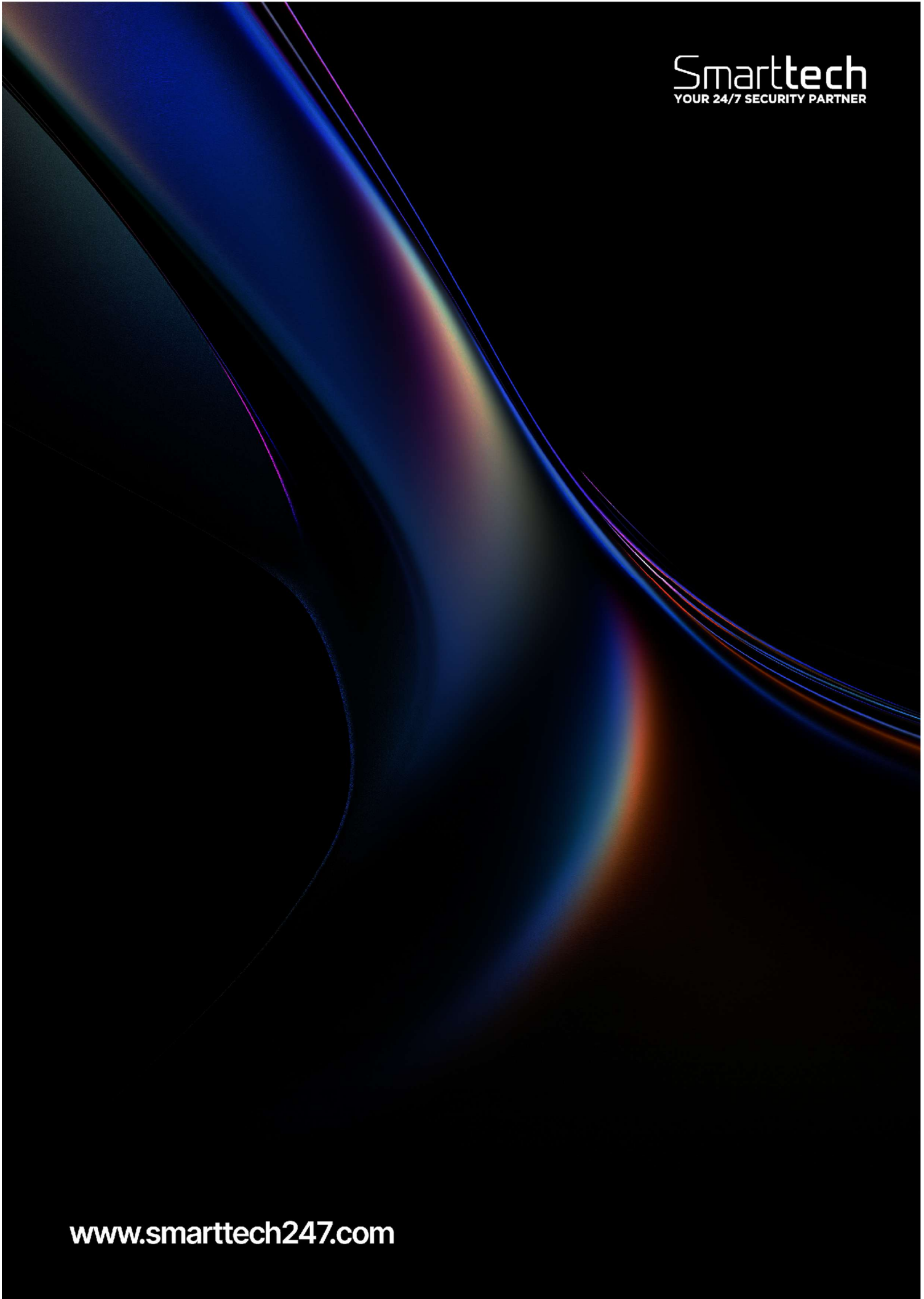
However, challenges remain:

- Legacy systems still in use
- Supply-chain security gaps
- Operational technology that is not sufficiently segmented or tested
- Skills shortages and slow incident decision-making

Attackers are becoming faster, more patient and more automated. Maintaining momentum is critical.

Precedent

Country	Year	Context	What Happened	Why It's Relevant
Denmark	2025	Heightened geopolitical tension	Danish authorities reported cyber disruption affecting government and defence-related public websites, assessed as part of wider geopolitical cyber activity.	Shows continued targeting of politically visible EU states through disruption-style attacks.
Germany	2024	European elections & Ukraine support	German federal institutions and political organisations experienced DDoS attacks, publicly attributed to pro-Russian hacktivist groups.	Demonstrates use of cyber disruption to influence political processes and signal opposition, not just steal data.
Poland	2023	National elections & strong EU/NATO role	Polish government and public-sector websites were targeted by cyber disruption and influence activity during election periods.	Reinforces that election cycles and political visibility increase cyber pressure.
Finland	2023	NATO accession	Finnish government services and public websites were hit by DDoS attacks following NATO membership announcements.	Clear example of cyber activity used as geopolitical signalling rather than purely criminal action.
France	2022	EU Presidency	French authorities warned of increased phishing, DDoS and espionage attempts targeting government bodies and suppliers during the Presidency.	Confirms that EU Presidencies attract elevated cyber activity, including supply-chain targeting.
Czech Republic	2022–2023	EU Presidency during geopolitical conflict	Czech authorities reported heightened hostile cyber activity against state institutions aligned with broader geopolitical tensions.	Shows sustained pressure during Presidency roles, not one-off events.
Estonia	2007	Politically sensitive national decision	Large-scale cyber disruption affected government, media and banking services.	Established cyber operations as a tool of political pressure in Europe.


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com