Cyber Threats to Ireland's EU Presidency

NCSC

June 2026

ncsc.gov.ie

CLASSIFICATION: UNCLASS

STATUS: TLP: CLEAR

This document is classified using Traffic Light Protocol. Sharing of TLP: CLEAR is unlimited.

https://www.first.org/tlp

Cyber threats to Ireland's EU Presidency

Ireland will take the EU Presidency during a period of mounting geopolitical unpredictability amplifying the risks to our digital infrastructure.

From July to December 2026, Ireland assumes the rotating Presidency of the Council of the European Union. Our public officials assume a central diplomatic role, leading meetings of the EU council bodies and negotiating collective outcomes on laws, budgets, and the EU's internal and external policy.

Our presidency will steer the bloc's efforts on issues of self-reliance in economic, defence and foreign policy, as well as hosting foreign dignitaries. Given this international political agenda, Ireland may be exposed to more geo-political risk than normal. Not because there are more threats or adversaries, but because Ireland's political, diplomatic and cyber domains are of higher strategic value.

NCSC's National Cyber Risk Assessment highlights the link between a dynamic geopolitical environment and malicious cyber activity. Nation States use their cyber capabilities against perceived rivals and adversaries to advance their own political, diplomatic and economic goals. Such incidents can be state directed or conducted by a diffuse network of pro-state proxies.

NCSC considers five categories of cyber threats which could affect Irish networks and information systems during the Presidency.

Financially motivated attacks: Ransomware, where attackers encrypt critical systems and steal data for ransom, is the most impactful type of attack in this this category. These attacks are generally carried out by criminals but can have devastating effects on the operation of critical services and harm the economy. During the presidency, the effect of a financially motivated attack could be leveraged to weaken Ireland's reputation.

Espionage: Cyber espionage is a low-cost, covert and relatively common means of intelligence collection. Sophisticated state directed hacking groups target sensitive data held by other governments and intercept communications for political and economic advantage. Unlike other cyber threats, adversaries prioritise stealth to silently keep access to a victim network or device – maximising the intelligence value of the compromised network.

Hacktivism: State aligned, and ideological hacking groups conduct malicious cyber activity to promote their central message. This usually consists of Denial of Service (DoS) or website defacement attacks, which are designed to get media attention and tend to have limited impact on delivery of essential services. More recently, these groups have also targeted Industrial Control Systems (ICS) which automate and supervise critical infrastructure operations. The overall goal remains to promote, amplify and exaggerate their attacks online to create the impression of widespread insecurity, political inefficiency and where possible polarise societal opinion.

Destructive attacks: A state directed cyber-attack resulting in the loss of critical infrastructure such as the energy grid is not commonly observed outside of conflict situations. In addition to the considerable resources required to carry out such an attack, the political and diplomatic consequences, as well as the risk of direct retaliation is a deterrent. Nevertheless, it is important to be aware of the threat given the transnational nature of some of our critical infrastructure as well as the risk of cascading effects.

Influence operations: Cyber-attacks often form a key element of influence operations. Hack & Leak, Account Take Over and DoS operations can be key elements of foreign interference campaigns designed to influence public opinion and subvert political authority. Advances in AI allow for the creation of convincing video and audio deepfakes as well as language specific phishing emails which act as advanced social engineering lures.

NCSC efforts

*To fulfil our mission of **leading Ireland's response to cyber risk**, NCSC regularly conducts threat and risk assessments which are shared across government. We recently held a national exercise with relevant partners; the scenario rehearsed a cyber incident escalating to a national crisis impacting critical services.*

To detect and disrupt live threats, we watch the global cyber threat environment and proactively defend the national attack surface. For smooth engagement, our teams keep strong relationships with national and international partners.

Links to the 2025 National Cyber Risk Assessment and further advice

2025 National Cyber Risk Assessment

Business Email Compromise and Payment Fraud Guidance

Denial of Service Attack Guidance

Mobile Device Management For Public Sector Bodies

Quick Guide: Phishing

Securing Operational Technology

Quick Guide: Ransomware How to #BreakTheChain

Online Account Security Plain English Guide

Cyber Security For Political Organisations & Election Candidates