An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

General Election 2024 Cyber Threat Landscape

ncsc.gov.ie

Published November 2024 – Revision 1

Status: TLP: CLEAR

This document is classified using Traffic Light Protocol. Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp.

Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

General Election 2024 Cyber Threat Landscape

- State aligned actors have shown a sustained interest in destabilising and manipulating electoral processes in Western democracies to achieve broader geopolitical aims. Ireland is not immune to this threat.

- Based on global trends and incidents observed in Ireland, NCSC assess the risk of cyber enabled attacks targeting election candidates and political organisations, including 'hack and leak' operations to be MEDIUM.

- NCSC assess the risk of cyberattacks during the election cycle to be MEDIUM. While a 'hacktivist' event during the voting period is LIKELY, the potential impact is assessed as LOW.

- NCSC assess the risk of a FIMI campaign targeting societal coherence and democratic processes to be MEDIUM.

- During this election cycle NCSC will raise awareness of the cybersecurity and FIMI threat landscape as well as providing incident management and response services for any electoral cybersecurity related events.

Introduction

In October this year, the US Intelligence Community publicly assessed that Russia and Iran are attempting to influence the 2024 US presidential campaign. China is focused on the congressional and other races.

In the same month European Parliament MEPs adopted a resolution condemning Russia's escalating malicious activities, interference and hybrid operations ahead of Moldovans going to the polls to vote in the country's presidential election and constitutional referendum on EU integration.

This illustrates how State aligned actors have sustained interest in destabilising and manipulating electoral processes in Western democracies. This includes using cyberattacks and disinformation campaigns.

Ireland has a unique position in Europe due to its geographic location, level of foreign investment, key export markets and position as a data centre hub. The outcome of any political event will be of interest to other countries, making it essential to protect the resilience of the electoral process and infrastructure.

Cybersecurity related risks can be considered across three main themes as outlined in the following sections. Attacks can be isolated, but the possibility that they are part of a broader hybrid campaign should also be considered.

Tom Johnson House, Beggar's Bush, Dublin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333 **E** info@ncsc.gov.ie
ncsc.gov.ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Targeting Election Candidates and Political Organisations

In previous election cycles globally, it has been observed that cyber operations target the major figures involved in campaigning, political parties, news, and social media more frequently than actual election infrastructure. This is a persistent risk that becomes more acute in the run up to an election due to the amplified impacts coverage of a compromise can have in the period immediately before and on polling day.

The most common method of a cyber enabled attack is spear-phishing emails. These are becoming more convincing with the use of AI.

AI generated audio, video and image deepfakes have also been used to target political figures and are designed to manipulate them into revealing sensitive information. This can be used to influence or discredit the individual and/or the political party.

Lower sophistication attacks such as DDoS and website defacement can be employed to draw attention to promote a specific narrative or simply to undermine and lower confidence in government and democratic processes.

NCSC Assessment

Based on global trends and incidents observed in Ireland, NCSC assess the risk of cyber enabled attacks targeting election candidates and political candidates to be MEDIUM.

To take account of the evolving threat landscape the NCSC has updated its guidance on Cybersecurity for Political Organisations and Election Candidates, which outlines the types of potential attack to be aware of, security measures to take and advice on what to do in the event of a suspected attack. The NCSC will be engaging with candidates and political parties to ensure that those involved in the General Election campaign are aware of these risks and of the means available to manage them.

Cyber-attacks against Electoral Infrastructure

Although voting in Ireland is paper based, processes across the electoral lifecycle are susceptible to cyberattacks by threat actors seeking to disrupt and/or undermine the democratic processes. These include voter registration, compilation and transmission and publication of results, auditing, and reconciliation.

Certain public bodies have a key role in the effective running of electoral processes in Ireland. Threat actors may attempt to target those entities to disrupt services or spread disinformation relating to the voting process.

State backed “Hacktivist” activity targeting countries during electoral events has been observed globally including a coordinated campaign targeting a number of Member States during the recent EU Elections.

In addition to State aligned groups, criminal threat actors may target political, electoral and transport infrastructure with ransomware attacks in attempt to disrupt the electoral process for financial gain. It is

essential to protect this infrastructure from both real and perceived threats to maintain public confidence in the electoral process.

NCSC Assessment

NCSC assess the risk of cyberattacks during the election cycle to be MEDIUM. While a 'hacktivist' event during the voting period is LIKELY, the potential impact is assessed as LOW.

NCSC has provided a cybersecurity advisory to Local Authorities

The EU Compendium on Elections Cybersecurity and Resilience was updated in 2024 and provides advice on guidance on securing electoral infrastructure. NCSC was a member of the drafting team and its contents have been shared with relevant stakeholders.

Hybrid Threats and Foreign Information Manipulation and Interference (FIMI)

There can often be a crossover between cyberattacks (or physical/kinetic attacks) and FIMI campaigns. These so called 'hybrid threats', use disinformation to exploit or amplify the effects of a cyberattack, with the aim of creating broader narratives of institutional distrust. This combination creates a more complex and damaging threat landscape, making it challenging to attribute attacks and respond effectively.

While the impact of FIMI in Ireland has been low there are ongoing efforts by State backed actors to spread disinformation.

NCSC Assessment

NCSC assess the risk of a FIMI campaign targeting societal coherence and democratic processes is MEDIUM.

Conclusion

The risk of cyber enabled attacks or influence operations increases in advance of any electoral event. Throughout this election cycle NCSC will raise awareness of the election cybersecurity threat landscape and provide advisories, guidance and incident management and response services for any electoral cybersecurity related events.

Further Reading

1. 2nd EEAS Report on Foreign Information Manipulation and Interference Threats
https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

2. ENISA Threat Landscape 2024
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

3. Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape
https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

4. Hybrid CoE Research Report 10: Preventing election interference: Selected best practices and recommendations
https://www.hybridcoe.fi/publications/hybrid-coe-research-report-10-preventing-election-interference-selected-best-practices-and-recommendations/

5. Hybrid CoE Research Report 12: Countering hybrid threats to elections: From updating legislation to establishing collaboration networks
https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/

6. Global Elections Security Report
https://globalcyberalliance.org/reports_publications/global-elections-security-report/

7. Russia Secretly Worms Its Way Into America's Conservative Media
https://www.nytimes.com/2024/09/07/business/media/russia-tenet-media-tim-pool.html?smid=url-share

8. U.S. Announces Plan to Counter Russian Influence Ahead of 2024 Election
https://www.nytimes.com/2024/09/04/us/politics/russia-election-influence.html?smid=nytcore-ios-share&referringSource=articleShare&ngrp=mnn&pvid=9BE588A1-7252-4A2D-8690-CDE828D3FD76

9. Disrupting deceptive uses of AI by covert influence operations
https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

10. Fighting foreign interference to protect our democracy
https://www.eeas.europa.eu/eeas/fighting-foreign-interference-protect-our-democracy_en?channel=eeas_press_alerts&date=2024-06-03&newsid=0&langid=en&source=mail

11. Google confirms Iran-linked hackers targeted Trump, Biden campaigns
https://www.politico.com/news/2024/08/14/google-iran-hackers-trump-biden-campaign-00174046

12. ODNI Election Security Update
https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240906.pdf

13. Meta bans Russian state media outlets for 'interference'
https://www.rte.ie/news/world/2024/0917/1470399-meta-ban-media/

14. Cybersecurity for Political Organisations and Election Candidates
https://www.ncsc.gov.ie/pdfs/NCSC_Cyber_Security_Political_Orgs_Candidates.pdf

15. Quick Guide: Cyber Security Best Practice for Electoral Candidates
https://www.ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Electoral_Candidate.pdf

16. Compendium on Elections Cybersecurity and Resilience (2024 Updated Version)
https://ec.europa.eu/newsroom/dae/redirection/document/103148

17. Framework on Online Electoral Process Information, Political Advertising and Deceptive AI Content
https://cdn.electoralcommission.ie/app/uploads/2024/04/23163750/Framework-on-Online-Electoral-Process-Information-Political-Advertising-and-Deceptive-AI-content.pdf

18. Russian election interference efforts focus on the Harris-Walz campaign
https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/

19. National Counter Disinformation Strategy
Publication pending

ANNEX I: Commonly used Terminology

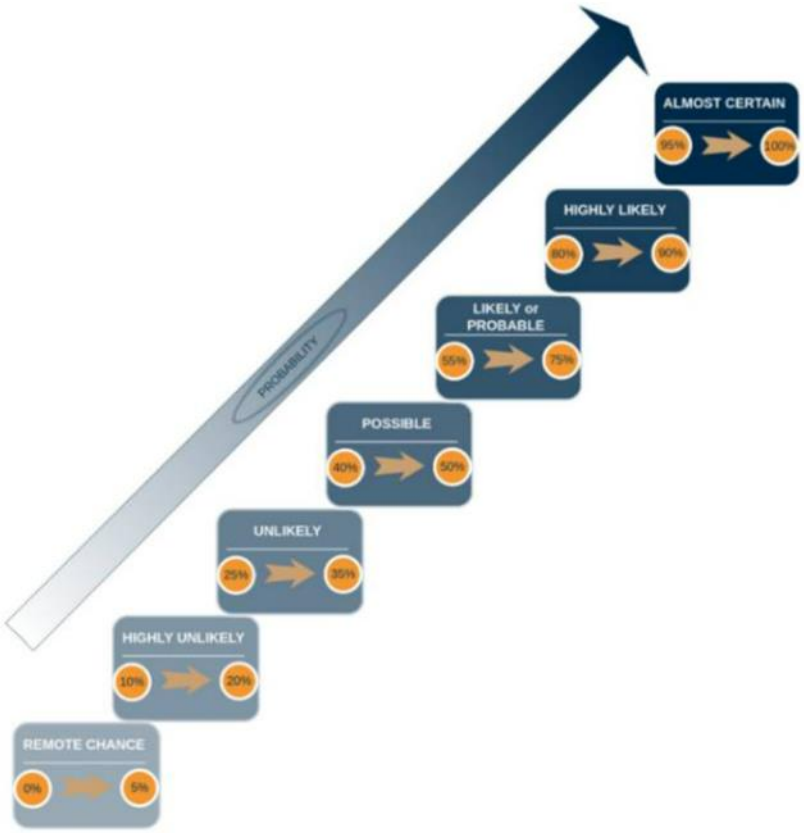
Cyberattack	A digital attempt targeting availability, confidentiality and integrity of data, systems, or networks.
Hack and Leak	The alleged or actual hacking of a candidate's or party's internal systems, followed by the strategic publication of real or faked documents in order to weaken or discredit the candidate political party, or democratic processes.
Deepfakes	AI facilitates the easy creation and spread of realistic but fake videos or audio recordings, so called 'deepfakes'
Disinformation	false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm
DoS **DDoS**	A denial-of-service attack (DoS) is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
FIMI	A pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory
Hacktivists	Actors driven by ideological or political motives. While traditionally seen is independent groups, they are increasingly state directed or aligned.
Hybrid Threats/ Campaigns	Political use of Hybrid Threats refers to manipulative, unwanted interference through a variety of tools: spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyberattacks, economic leverage etc.
Ransomware	Ransomware can be used in 'double extortion' techniques to encrypt data and demand a ransom for its 'release' (provide a decryption key), or the threat actors can sell the data or demand a ransom NOT to publish it. Ransomware infections can also cause severe operational disruption by disabling IT infrastructure
Social Media	Given the pervasive use of social media during elections, Ireland, like most western democracies, is vulnerable to disinformation campaigns delivered via social media which facilitates targeting, reach and impact. These can be delivered through multiple means, including the use of botnets*, compromised social media accounts, or recruiting social media influencers. *A Botnet is a group of internet-connected devices, each of which runs one or more bots. Botnets can be used to perform distributed denial-of-service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection.
Spear phishing	Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as

	a trustworthy entity in an electronic communication. Spear phishing is directed at specific individuals or companies, where attackers typically gather personal information about their target to increase their probability of success.
State Aligned Actors	These actors are typically well-resourced, motivated by geopolitical goals and operate directly for or with the tacit approval of sovereign powers.
Website Defacement	An attack on a website that changes the visual appearance or content of the site or a webpage

ANNEX 2: Assessment Terminology

NONE	No indication of a cyber threat. No acknowledged capacity or intent to carry out cyber attacks. Attacks/harmful activities are highly unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out cyber attacks. Cyber attacks/harmful activities are less likely.
MEDIUM	A general threat exists. Capacity and/or intent to launch cyber attack and possible planning. Cyber attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out cyber attacks and planning. Cyber attacks/harmful activities are likely.
VERY HIGH	A specific cyber threat exists. Capacity, intent to attack, planning and possible execution. Cyber attacks/harmful activities are highly likely.

Threat level Assessment Description used by NCSC



Probability Metric used by NCSC to Quantify Likelihood of Events of Developments Occurring