Topic 6

National Cyber Emergency Planning

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

Table of Abbreviations

AAR	After Action Report
AGO	Attorney General's Office
AGS	An Garda Síochána
C3WG	CNI Cyber Coordination Working Group
CNI	Critical National Infrastructure
CyCLONe	Cyber Crisis Liaison Organisation Network
DAFM	Department of Agriculture, Food and the Marine
DECC	Department of the Environment, Climate and Communications
DF	Defence Forces
DFA	Department of Foreign Affairs
DHPLG	Department of Housing, Planning and Local Government
DJ	Department of Justice
DOD	Department of Defence
EU	European Union
GIS	Government Information Services
Gov-CORE	Government Coordination and Response Network
GTF	Government Task Force
IC	Incident Category
IOC	Indicators of Compromise
LGD	Lead Government Department
NCEP	National Cyber Emergency Plan
NCSC	National Cyber Security Centre
NECG	National Emergency Coordination Group
NI	Northern Ireland
NIS2	Network and Information Security version 2
NSAC	National Security Analysis Centre
NSC	National Security Committee
OEP	Office of Emergency Planning
SEM-NSF	Strategic Emergency Management: National Structures and Framework
TLP	Traffic Light Protocol
UK	United Kingdom of Great Britain and Northern Ireland

1 Introduction

The National Cyber Emergency Plan (NCEP) sets out the national approach for responding to serious cyber security incidents that affect the confidentiality, integrity, and availability of nationally important information technology and operational technology systems and networks [1].

1.1 Objectives

By the end of this topic, you will be able to:

- Understand the multifaceted nature of cyber emergencies.
- Familiarise with the National Cyber Security Plan and its operational modes.
- Grasp the roles and responsibilities of key stakeholders in a cyber emergency.
- Comprehend the importance of effective communication and international cooperation.

While this module focuses on the Irish approach, it can serve as a model for similar implementations in other countries.

The NCEP outlines Ireland's approach to responding to serious cyber security incidents.

It's designed to ensure effective coordination between government agencies and key organisations during such emergencies. The NCEP establishes structures and processes for declaring, managing, and coordinating a national response to cyber threats. It also aims to clarify the roles and responsibilities of various stakeholders and provide guidance on communicating with the public. The NCEP is aligned with Ireland's broader emergency management framework and is intended for government officials and essential service providers.

The NCEP sets out the national approach for responding to serious cyber security incidents that affect the confidentiality, integrity, and availability of nationally important information technology and operational technology systems and networks.

2 Cyber Emergencies: A Complex Challenge

Cyber security incidents can take many forms and originate from various sources. They might target government systems, critical infrastructure (such as power grids or transportation networks), or service providers. These incidents can occur within Ireland or in other countries, both within and outside the European Union (EU).

In some cases, cyber attacks may have both digital and physical consequences. For instance, a cyber attack on a power grid could disrupt electricity supply, leading to physical impacts like factory shutdowns or emergency services disruptions.

2.1 Defining a Cyber Emergency

A cyber emergency is a serious incident that poses a significant threat to life, property, the environment, or the economy. It also involves a substantial impact on multiple critical sectors. These sectors might include healthcare, transportation, finance, or energy.

When a cyber emergency occurs, it triggers the activation of the National Emergency Coordination Group (NECG) (Cyber). This group is responsible for coordinating a comprehensive response to the incident, which involves containment, mitigation, and recovery efforts.

2.1.1 Lead Government Department

The Lead Government Department (LGD) has the mandate and responsibility to coordinate all national level activity for its assigned emergency types. The LGD role includes risk assessment, planning and preparedness, prevention, mitigation, response, and recovery. The LGD is assigned within the Strategic Emergency Management: National Structures and Framework (SEM-NSF) [2].

Examples include:

- **Infectious Diseases** (in animals)
  - Department of Agriculture, Food and the Marine (DAFM) or
- **Network Information Systems Incident**
  - Department of the Environment, Climate and Communications (DECC)
- **Energy Supply Emergency**
  - Department of the Environment, Climate and Communications (DECC)
- **Flooding and Fire**
  - Department of Housing, Planning and Local Government (DHPLG)
- **Any Emergency Overseas, affecting Irish Citizens**
  - Department of Foreign Affairs (DFA)
- **National Security Related Incidents** (Including terrorism)
  - Department of Justice (DJ)

2.2 In summary

A cyber emergency is defined as any cyber incident which causes or threatens to cause:

- Death or serious injury or damage to property, the environment or the economy or significant incidents impacting two or more critical sectors [3] and which,
- Requires the activation of the NECG (Cyber) to ensure an effective coordinated response for containment, mitigation and/or recovery.

3 National Cyber Security Plan

3.1 Cyber Incident Categories

Cyber emergencies in Ireland are classified based on their severity. The table lists and outlines the classification of cyber incidents based on their severity. The categories range from Incident Category (IC)1, the most severe, to IC6, the least severe. Each category represents a different level of impact on essential services, national security, government, or the population. Understanding these categories is crucial for effective response and mitigation efforts.

IC1 National Cyber Emergency	A cyber attack which: • Causes sustained disruption of essential services or, • Affects national security, leading to severe economic or social consequences or to loss of life.
IC2 Highly Significant Incident	A cyber attack which: • Has a serious impact on central government, or • Has a serious impact on essential services, or • Has a serious impact on a large proportion of the population, or • Has a serious impact on the economy.
IC3 Significant Incident	A cyber attack which: • Has a serious impact on a large organisation or, • Has a serious impact on wider/local government, or • Which poses a considerable risk to central government or, • which poses a considerable risk to essential services.
IC4 Substantial Incident	A cyber attack which: • Has a serious impact on a medium-sized organisation, or • Which poses a considerable risk to a large organisation, or • Which poses a considerable risk to wider/local government.
IC5 Moderate Incident	A cyber attack: • On a small organisation or, • Which poses a considerable risk to a medium-sized organisation, or, • Preliminary indications of cyber activity against a large organisation or, • Preliminary indications of cyber activity against the government.
IC6 Localised Incident	A cyber attack: • On an individual, or • Preliminary indications of cyber activity against a small or medium-sized organisation.

3.2 Cooperation modes

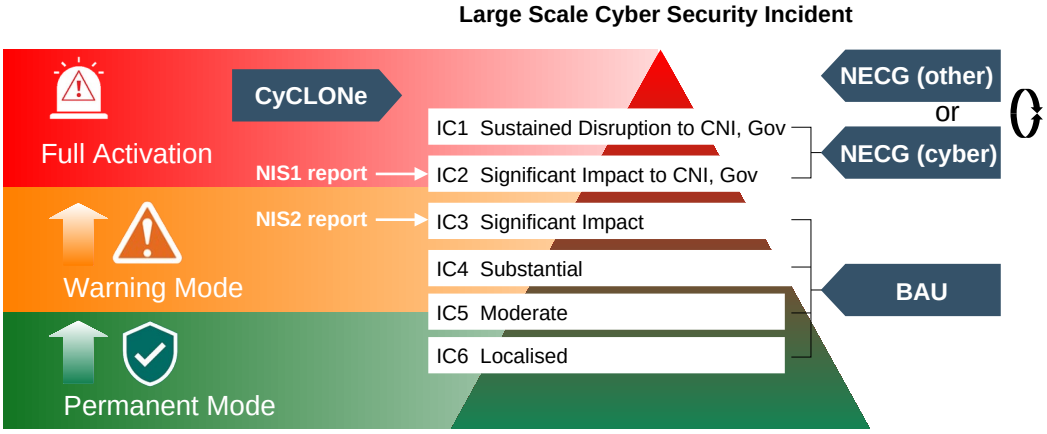


Figure 1: NCEP Modes

The activities described in the NCEP rely upon three cooperation modes:

- Permanent Mode
- Warning Mode
- Full Activation Mode

The following sections describe the procedures and activities associated with each mode.

3.3 Permanent Mode

The responsibility for identifying incidents that could potentially escalate into a national cyber emergency lies with both the LGD or Agency overseeing or regulating the affected entities and the National Cyber Security Centre (NCSC). These organisations receive reports from the public, from entities they oversee, or from technical capabilities that identify incidents that may lead to a cyber emergency. This process is part of the normal course of business, during which situational awareness is maintained and incident preparedness activities are carried out. Communications are maintained through usual reporting formats.

3.4 Warning Mode

The NCSC will activate **Warning Mode** when it receives evidence or inputs from its constituents, the Cyber Crisis Liaison Organisation Network (CyCLONe) network, other international peer organisations, or threat intelligence partners indicating a heightened risk of a cyber emergency incident emerging in a specific sector or sectors. This mode involves communications with stakeholders across government and the private sector to reinforce information exchanges and cooperation to prevent the possible spread of the incident. Additionally, **Warning Mode** serves as a filter to determine if escalation to **Full Activation Mode** is necessary. Information to support the decision-making process for transitioning to Warning Mode may come from various sources, including the NCSC's own incident detection/response or forensic capabilities or from information received from third parties within or outside the state.

3.4.1 Activate Warning Mode

Warning Mode can be triggered by either a national actor, such as a LGD or the NCSC, or through the EU CyCLONe process in respect of an incident in another EU Member State. The NCSC can activate Warning Mode upon receiving an incident report or intelligence indicating an ongoing or imminent incident. A LGD may also initiate this process if they have specific information that an entity or entire sector is at risk of a particular incident. The Office of Emergency Planning (OEP) will notify NCEP stakeholders by email when Warning Mode is activated.

During **Warning Mode**, the NCSC would likely be engaged with potential victims, supporting incident response and sharing relevant information with various stakeholders. Technical details, including forensic analyses of affected devices or networks, would be shared with other potential victims within the state and potentially through relevant EU and NATO information sharing networks. Information regarding potential risks to services or infrastructure in the state would also be shared with key security stakeholders and LGDs. Regular virtual or in-person briefings of members of the NECG (Cyber) would likely take place to maintain situational awareness and prepare for any escalation to full activation mode.

The EU CyCLONe process is a member state-led European incident response and coordination mechanism designed to bring together national cyber incident response entities at a senior level to coordinate and support decision-making for **large-scale cybersecurity incidents** affecting one or more Member States. The CyCLONe network operates through a similar Permanent, Warning, and **Full Activation Mode** sequence as outlined in this plan. If a Cyclone Warning or **Full Activation Mode** is activated in respect of an incident in another Member State or Member States, the national level shall automatically be set to that cooperation mode for the affected sector or sectors.

3.4.2 Exit Warning Mode

During **Warning Mode**, the NCSC or the LGD may organise meetings or briefings to discuss the ongoing incident response process necessary to either contain the spread of the incident and stand down **Warning Mode** or escalate to **Full Activation Mode**.

If the risk to the critical sector is deemed to be successfully eradicated, mitigated, or contained, **Warning Mode** can be exited, with remaining follow-up actions to be taken by the victim, the NCSC, or the LGD. However, if risks continue to grow and no likely mitigation can be foreseen in the short term, or the incident is causing or capable of causing severe operational disruption for a critical sector, the decision will be made to activate the NECG process.

The OEP will notify NCEP stakeholders by email when **Warning Mode** is Exited/Stood Down.

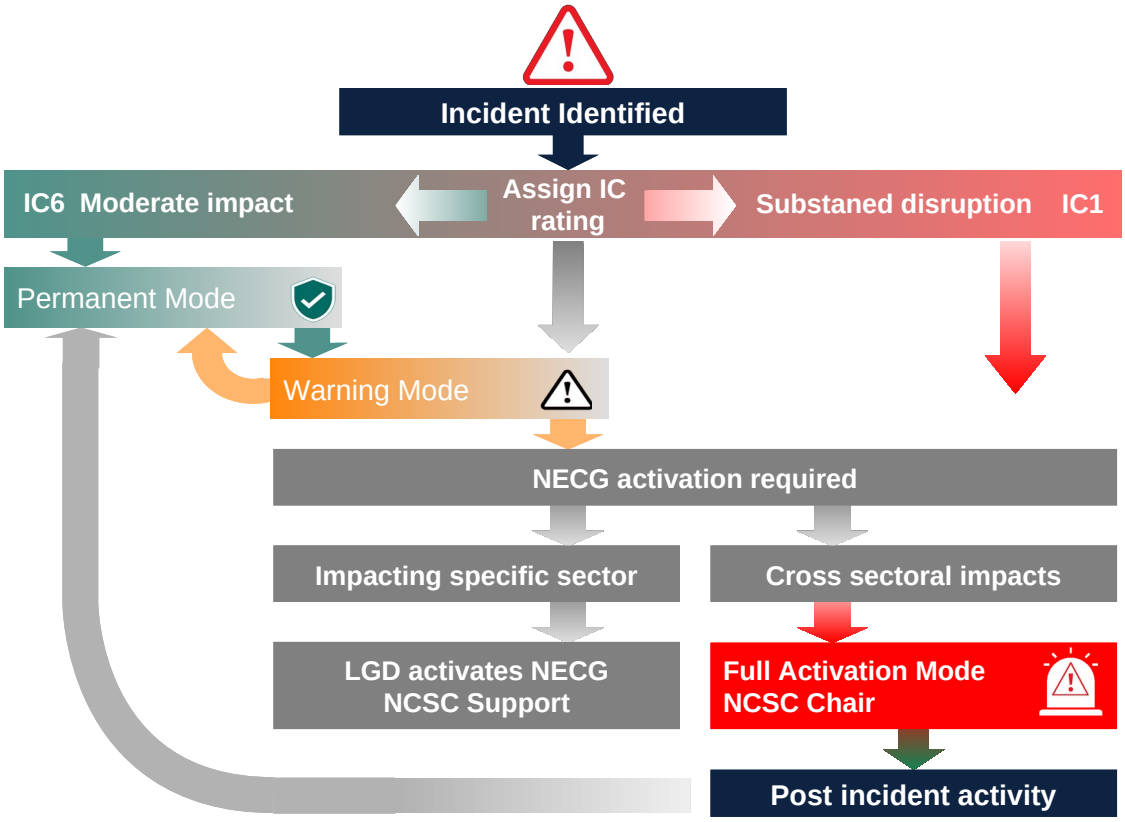


Figure 2: NCEP Co-operation Modes and Escalation Path

3.4.3 Activate the National Emergency Coordination Group

The LGD responsible for leading the response for various emergency/incident types is established in the SEM-NSF [2]. The following guidance is provided to help determine which government department is best suited to assume the LGD role for emergencies rooted in cyber incidents.

When impacts are limited to a particular sector, the identified LGD will lead the NECG process, with the NCSC providing specialist advice in the cyber domain. The NCSC will work through the Government Coordination and Response Network (Gov-CORE) group to empower all government departments to develop scenario-specific emergency response plans for cyber emergencies within their sectors.

However, if cyber incidents impact two or more critical sectors, the NCSC will lead the NECG process and enter **Full Activation mode**. Scenario examples include incidents affecting government networks or those exploiting vulnerabilities in technology products or services used by multiple government departments.

3.5 Full Activation Mode

Full Activation Mode will be activated if an incident meets the threshold of a national cyber emergency requiring the activation of the NECG (Cyber) chaired by the NCSC to ensure an effective, coordinated, multi-agency, and cross-government response for containment, mitigation, and/or recovery.

The decision to transition to **Full Activation Mode** will be made by the NCSC or the Minister for the Department of the Environment, Climate, and Communications. This decision may follow a period of **Warning Mode**, or it may be made directly if an incident is initially reported as sufficiently serious.

In the event of a national cyber emergency declaration, the OEP shall convene the NECG for Cyber Incidents at the National Emergency Coordination Centre (NECC) within one hour, chaired by the Director of the NCSC or Deputy Director (representing LGD DECC for Cyber incidents), and supported by the impacted LGDs who will manage the sectoral impacts within their remit.

This mode may also be activated if a large-scale cybersecurity incident is identified by the CyCLONe network at the EU level or other international peer organisations.

Note: For incidents where national security concerns arise an NECG meeting may not be called, and the incident could instead be dealt with by other means as appropriate.

3.5.1 Exit Full Activation Mode

When **Full Activation Mode** is convened following a National Cyber Emergency declaration, a key task will be to identify the objectives required to exit the "**Cyber Emergency**" It is envisaged that **Full Activation Mode** will end and the cyber emergency stood down when the "**essential services**" of the impacted entities can resume at acceptable levels. However, response activities to fully remediate and harden all systems will often continue long after the initial "**emergency**" period has passed.

Emergency exit criteria will typically require meeting conditions such as: information systems underpinning essential services are functional, priority network communications are reconnected, backups are in working order, the root cause that gave rise to the incident has been identified and a remediation plan initiated, NECG members have reached a consensus that the objectives to end the emergency have been achieved and that acceptable services levels have been restored, and the NECG chair is handed over to an alternative LGD, if for example the cyber specific elements of the incident are contained but sectoral impacts are ongoing.

3.5.2 Post incident activity

When the cyber emergency is stood down, the experiences and lessons learned will be captured in an After Action Report (AAR). These insights will also be used to update the NCEP and other incident response playbooks as appropriate, driving continual improvements to the response processes.

The NCSC will also conduct periodic exercises in collaboration with the wider stakeholder community to test the NCEP as well as the cyber response plans of other sectoral departments and agencies/entities. The outcomes of these exercises will be used to continually refine and improve the response to cyber incidents at the entity, sector, National, and International levels.

4 Roles and Responsibilities

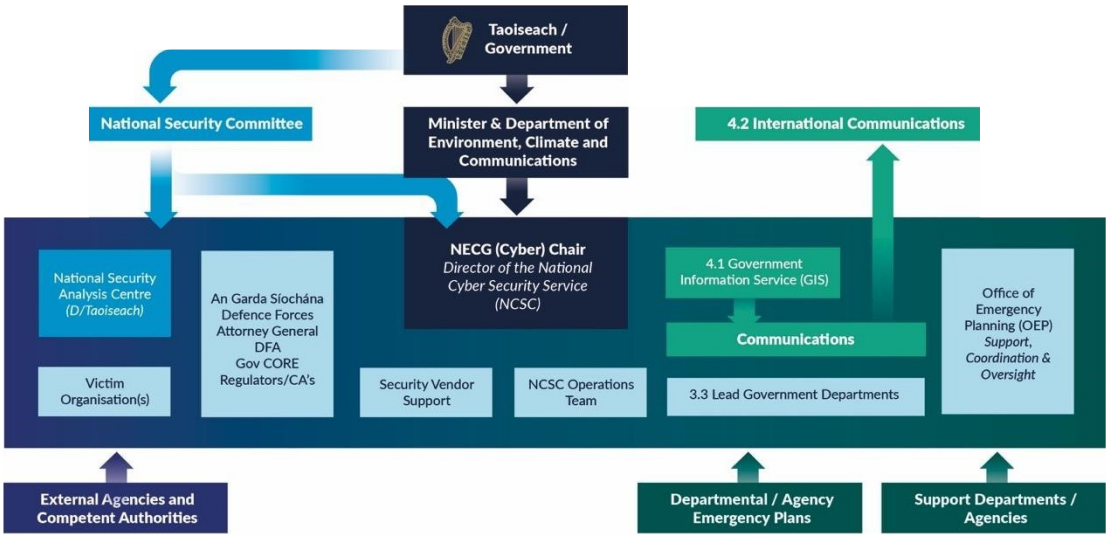


Figure 3: NECG (cyber)

Figure 3 illustrates the key participants in the NECG (cyber). The NECG (cyber) group is aligned with the SEM-NSF model [2].

4.1 National Emergency Coordination Group

The NECG is the national structure established to coordinate and obtain the necessary support and advice from identified support Departments and Agencies during a threatened or ongoing emergency. The OEP will convene the NECG on behalf of the NCSC within one hour of a cyber emergency declaration.

During a National Cyber Emergency, a key role of the NECG will be to maintain overall situational awareness of the incident and to coordinate a whole-of-government response to a cyber emergency with cross-Government and/or cross-sector implications.

When the NECG (cyber) is convened under the conditions for a "**cyber emergency**" declaration, all Government Task Force (GTF) members of the group are obligated to attend the first meeting. Attendance at subsequent meetings is managed based on the nature of the emergency and at the discretion of the NCSC chair. The Chair may establish Sub-Groups to address specific issues that arise or are expected to arise in dealing with the emergency.

The NECG Chair will initially inform all GTF members that a National Cyber Emergency has been declared and will then convene a refined NECG (cyber) group which shall consist of:

- NCSC chair (NCSC Director or deputy)
  - Representing LGD DECC for Cyber incidents
- National Security Analysis Centre (NSAC)
- Victim organisation(s) as required
- Government Information Services (GIS)
- Attorney General's Office (AGO)
- Department of Foreign Affairs
- Department of Justice
- An Garda Síochána (AGS)
- Defence Forces (DF)
- Private cyber security vendors as required
- Office of Emergency Planning (support, coordination, oversight)
- Lead and Support Government Department as required (varies dependent on incident type and sectoral impacts)
- Gov-CORE Chair
- Regulators and Competent Authorities as required

4.2 The National Emergency Coordination Group Chair

The NECG, chaired by the NCSC Director, will coordinate the national response to cyber emergencies. The NCSC will represent DECC as the LGD and be the competent authority under Network and Information Security version 2 (NIS2). The Chair will lead NECG meetings, ensure timely decisions, and seek consensus among members. If consensus cannot be reached, the Chair will refer the issue to Ministers or the Government.

The NECG cannot take a decision that is vested by statute in another government department or agency or other public authority without the agreement of that department or agency.

For urgent or interdepartmental issues, the NECG Chair will seek consensus. If unresolved, the Chair will refer the matter to Ministers or the Government with detailed recommendations. Ministerial approval is required for proposed measures. Cross-departmental issues not resolved at NECG will be referred to relevant Ministers or the Taoiseach.

4.3 Lead Government Departments during a cyber emergency

LGDs are responsible for managing cyber emergency impacts within their assigned sectors. They must manage physical responses and recovery operations, maintain situational awareness, and brief senior officials and agencies. LGDs must also conduct risk assessments, plan, prevent, mitigate, respond, and recover. They will identify Support Departments/Agencies' roles and collaborate during planning and preparedness.

4.4 National Cyber Security Centre Operations Team

The NCSC Operations Team proactively prevents and responds to cybersecurity incidents. During incidents, they focus on technical remediation and inform the NECG of progress. The incident response process includes five phases:

- preparation,
- detection and analysis,
- containment,
- eradication,
- recovery, and
- post-event activity.

During a national cyber emergency, the NCSC Operations Teams will: identify the scope, impacts, and implications of the cyber security incident on Ireland and contain incidents as they occur; analyse, enrich, and share Indicators of Compromise (IOC) and other technical details with relevant stakeholders and peer organisations; guide and support victim organisations and their response team during a cyber incident to enable them to remediate and resolve the incident; capture the technical and non-technical details of the incident and use that information to manage and communicate ongoing cybersecurity risks in the State; request Government Departments, Public Sector Bodies or operators of Critical National Infrastructure (CNI) to take certain actions, for example isolate their network, preserve logs, in response to the incident; provide reports and analysis on incidents to assist law enforcement and national security authorities; and coordinate with NCSC United Kingdom (NCSC-UK) and NCSC Northern Ireland (NCSC-NI) for all-island incidents.

4.5 Victim organisations

Victim organisations initially own incident response, with NCSC providing support. They should swiftly report incidents to NCSC, engage specialists if needed, and provide data and systems to the NCSC for analysis.

4.6 Private Cyber Security Vendors

Technical specialists from NCSC, other agencies, or the private sector may assist in incident response. NCSC may connect affected entities with private cyber security vendors to provide necessary expertise and resources. NCSC accepts no liability for the actions of private cyber security vendors on victim organisation networks.

4.7 Law Enforcement

Cybersecurity incidents should be reported to law enforcement and relevant agencies. The priority during a national cyber emergency is restoring critical services and ending the emergency. NCSC will work with law enforcement to support their response and ensure forensically sound capture of evidence. If there are conflicting objectives, the issue will be brought to the NECG for deconfliction. AGS has primary responsibility for investigating and prosecuting criminal acts related to the national cyber emergency. They may also disrupt cybercrime activities through seizing digital assets or infrastructure. AGS is responsible for liaison with international policing organisations. AGS and NCSC may share relevant information relating to incident response processes.

4.8 Defence

The DF role in cybersecurity is outlined in the 2015 White Paper on Defence. Through the NECG, the NCSC Chair may request support from the DF, which could include deploying technical staff, providing ICT equipment, and providing manpower and logistical support.

4.9 Office of the Attorney General

The AGO will provide legal advice where necessary on any proposed decisions or actions taken by the NECG during the course of the incident lifecycle.

4.10 Intelligence and Security

Intelligence support during a national cyber emergency is provided by national authorities, including the DF, NCSC, AGS, and the NSAC. These organisations will prioritise sharing relevant intelligence with senior leadership and those responding to the incident. Intelligence and related activities can play a crucial role in understanding and responding to a national cyber emergency. The NCSC and supporting organisations will utilise intelligence sources to build situational awareness, share threat indicators and analysis, identify and acknowledge gaps, and create a comprehensive picture of the incident. Sector-level public/private partnership initiatives may also provide intelligence support.

4.10.1 National Security Committee

The National Security Committee (NSC) is chaired by the Secretary General to the Government, and it comprises representatives at the highest level from the DOJ, Department of Defence (DOD), DFA, the DECC and from AGS and the DF. The secretariat to the Committee is provided by the National Security Analysis Centre in the Department of the Taoiseach. The committee is concerned with ensuring that the Government and the Taoiseach are advised of high-level security issues and the responses to them.

4.10.2 National Security Analysis Centre

The NSAC was established in 2019 by the Government and its primary remit is to provide high-quality, strategic analysis to the Taoiseach and Government of the key threats to Ireland's national security. The strategic analysis of threats is undertaken by personnel seconded from the various Departments and other State bodies with functions in the security area, and through liaison and close co-ordination with those partner Departments and agencies, including with the NCSC.

4.11 Attribution and Cyber Diplomacy

Attribution of cyber-attacks to specific threat actors, particularly other States, can be challenging. Authorities such as the NCSC and AGS can often provide technical attribution, but public attribution should be conducted by Government assisted by the NCSC due to political, diplomatic, legal, and policy implications. Cyber Security Emergencies often contain a diplomatic element, and the DFA leads on cyber diplomacy issues.

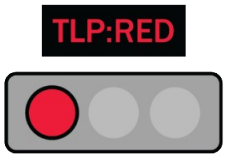
The EU Cyber Diplomacy Toolbox provides a way of coordinating the diplomatic responses of EU member states to malicious cyber activities at the EU level [4].

5 Communications

THE NCSC will use the Traffic Light Protocol (TLP) v2.0 when sharing information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s).

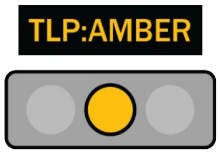
5.1 Traffic Light Protocol version 2.0

TLP is a set of four labels (**RED**, **AMBER**, **GREEN**, **CLEAR**) used to indicate sharing boundaries. It provides a simple schema for indicating with whom potentially sensitive information can be shared. TLP is not a formal classification scheme and does not handle licensing terms or information handling or encryption rules. It is optimised for ease of adoption, human readability, and person-to-person sharing [5].



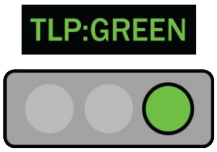
TLP: RED For the eyes and ears of individual recipients only, no further disclosure.

Sources may use **TLP:RED** when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organisations involved. Recipients may therefore not share **TLP:RED** information with anyone else. In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting.



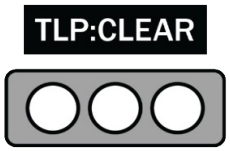
TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organisation and its clients.

Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may share **TLP:AMBER** information with members of their own organisation and its clients, but only on a need-to-know basis to protect their organisation and its clients and prevent further harm.



Limited disclosure, recipients can spread this within their community.

Sources may use **TLP:GREEN** when information is useful to increase awareness within their wider community. Recipients may share **TLP:GREEN** information with peers and partner organisations within their community, but not via publicly accessible channels. **TLP:GREEN** information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defence community.



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.

5.1.1 TLP in email

TLP designated email correspondence should indicate the TLP colour of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP colour must be in capital letters: **TLP:RED**, **TLP:AMBER**, **TLP:GREEN**, or **TLP:CLEAR**.

5.1.2 TLP in documents

TLP designated documents should indicate the TLP colour of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP colour should appear in capital letters and in 12 pt type or greater.

5.2 National Communications

During a national cyber emergency, it is vital to maintain coherent and unified communications with the public, victim organisations, and other stakeholders. The NECG will convene a Communications Subgroup chaired by the NCSC, supported by GIS and OEP. The NECG will work closely with GIS on preparing and delivering communications on all issues related to the emergency. The NECG will provide regular updates to the public through GIS and engage with spokespeople and Communications Teams from other Lead Government Departments and agencies to ensure consistent and coordinated messaging. The NCSC will continue to issue technical security advisories and guidance through its usual channels.

5.3 International Communications and Cooperation

The NCSC and supporting departments will coordinate with their international counterparts, sharing relevant information with other Government departments. Supporting departments will include the NCSC and DFA. Communications at Technical, Operational, Strategic and Political levels will occur through existing EU structures and bilateral arrangements with peer organisations.

Additionally, The CNI Cyber Coordination Working Group (C3WG) is established to strengthen cooperation between officials in the UK, both Stormont and Westminster, and Irish Government in relation to cyber incident response and cross border CNI cyber dependencies.

AGS will be responsible for any international law enforcement engagement.

6 Incident Handover

If at any stage during the incident response life cycle, it is deemed that it is no longer necessary or appropriate for the NCSC (representing DECC) to lead the recovery, the management of the recovery shall be handed over to an agreed alternative Government Department or agency.

Reasons for this could be that the incident is contained within a single sector, the incident severity is assessed as no longer meeting the threshold or an IC1 or IC2 category incident, the root cause is due to a non-malicious event such as systems failure or human error, etc.

7 Post Incident Review

Following an incident, a review will be carried out at the conclusion of the NECG response, chaired by DECC to review the incident and identify lessons learned. This may include interdepartmental reviews and briefings for operational personnel and senior officials, as well as more in-depth post emergency reports.

Responsibility for the review will rest with LGD and will be brought to GTF.

8 Exercise: Cyber Emergency Response

8.1 Objective

To assess participants' understanding of cyber emergency response procedures and their ability to collaborate effectively within a simulated crisis scenario.

8.2 Scenario

A large-scale cyberattack has compromised critical infrastructure systems, including power grids, transportation networks, and financial institutions. The attack has resulted in widespread disruptions, economic losses, and potential security threats.

8.3 Exercise Structure

The class will be presented with a national cyber emergency scenario.

Phase 1: Initial Response *(5 minutes)*

Identify the Incident: Participants discuss the initial IOCs and the potential impact of the attack.

Activate the Emergency Response Plan: Participants identify the appropriate activation level (Warning or Full Activation).

Establish the NECG: Participants assign roles and responsibilities within the NECG, for the purpose of the exercise this will include:

- NCSC chair (NCSC Director) [representing LGD DECC]
- National Security Analysis Centre (NSAC)
- Government Information Services (GIS)
- Attorney General’s Office (AGO)
- Department of Foreign Affairs (DFA)
- Department of Justice (DOJ)
- An Garda Síochána (AGS)
- Defence Forces (DF)
- Office of Emergency Planning (OEP)
- Lead Government Department (LGD)
- Government Cyber Security Coordination and Response Network(Gov CORE) Chair
- Victim Organisation (if appropriate)

Phase 2: Containment and Eradication (5 minutes)

Isolate Affected Systems: Participants discuss strategies to contain the spread of the attack, such as network segmentation and system shutdown.

Eradicate the Threat: Participants brainstorm techniques to remove malicious code and restore compromised systems, including patching vulnerabilities, deploying security tools, and conducting forensic analysis.

Phase 3: Recovery and Lessons Learned (10 minutes)

Restore Critical Functions: Participants develop a recovery plan to restore essential services and minimise business disruption.

Conduct Post-Incident Review: Participants discuss the key lessons learned from the incident, including identifying weaknesses in security practices, improving incident response procedures, and enhancing communication channels.

Discussion Points

Coordination and Collaboration: How can different organisations and agencies effectively coordinate their efforts during a cyber emergency?

Communication Strategies: What are the most effective communication channels for sharing information with stakeholders, both internally and externally?

Legal and Ethical Considerations: How should organisations balance the need to respond to a cyberattack with legal and ethical obligations?

International Cooperation: What role can international cooperation play in addressing cyber threats and incidents?

Additional Exercises:

Tabletop Exercise: Simulate a specific cyberattack scenario and have participants work through the response process, making decisions and taking actions.

Incident Response Drill: Conduct a practical exercise to test the organisation's ability to respond to a simulated cyberattack, including activating incident response teams, isolating affected systems, and restoring critical services.

Cybersecurity Awareness Training: Provide training to employees on cybersecurity best practices, including recognising phishing attacks, strong password hygiene, and reporting suspicious activity.

By conducting regular cyber emergency response exercises, organisations can improve their preparedness, response capabilities, and overall resilience to cyber threats.

9 Bibliography

[1] ‘National Cyber Emergency Plan (NCEP)’. National Cyber Security Centre, Jul. 05, 2024. Accessed: Dec. 16, 2024. [Online]. Available: https://www.ncsc.gov.ie/pdfs/National_Cyber_Emergency_Plan.pdf

[2] ‘Strategic Emergency Management National Structures and Framework’. Department of Defence, Apr. 12, 2017. Accessed: Dec. 16, 2024. [Online]. Available: https://www.gov.ie/pdf/?file=https://assets.gov.ie/90681/71eaf4b4-3c20-488d-b443-620e57a51c2b.pdf#page=null

[3] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[4] ‘EU Cyber Diplomacy Toolbox’. EU, Jun. 07, 2017. Accessed: Dec. 16, 2024. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[5] *Traffic Light Protocol (TLP)*. Accessed: Oct. 09, 2024. [Online]. Available: https://www.first.org/tlp/