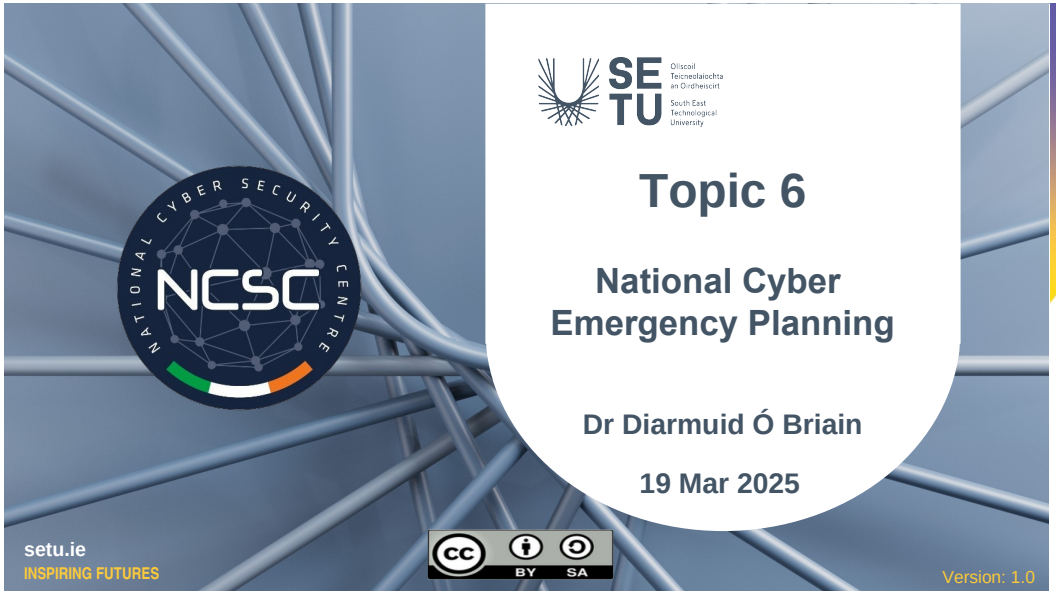


Licence

Learning 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.

National Cyber Emergency Plan

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.

National Cyber Emergency Plan

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 and which,
- Requires the activation of the National Emergency Coordination Group (NECG Cyber) to ensure an effective coordinated response for containment, mitigation and/or recovery.

Lead Government Department

- The LGD is defined for incident types in the Strategic Emergency Management: National Structures and Framework (SEM-NSF)
- Examples include:
  - Infectious Diseases (in animals) — DAFM
  - Network Information Systems Incident — DECC
  - Energy Supply Emergency — DECC
  - Flooding and Fire — DHPLG
  - Any Emergency Overseas — DFA
  - National Security Related Incidents — DJ
- Mandate and responsibility to coordinate all national level activity for its assigned emergency types

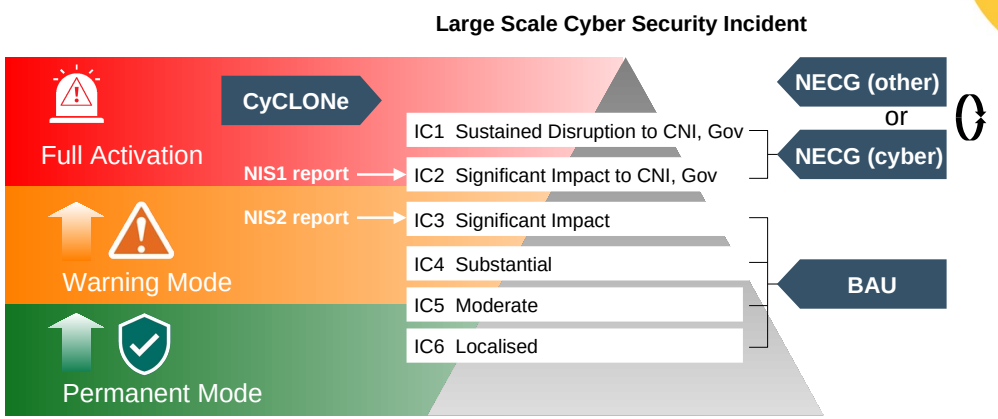
National Cyber Security Plan

setu.ie
INSPIRING FUTURES

Cyber Incident Categories

IC1 National Cyber Emergency	• Sustained disruption of essential services • National security	**IC4 Substantial Incident**	• Serious impact on medium-sized Organisation • Risk to large Organisation
IC2 Highly Significant Incident	• Serious impact on national Government	**IC5 Moderate Incident**	• Serious impact on a smaller Organisation • Prelim indications of risk to larger Organisations
IC3 Significant Incident	• Serious impact on larger Organisation	**IC6 Localised Incident**	• Serious impact on an individual • Prelim indications of risk to medium or smaller Organisations

NCEP Activities



Permanent Mode

- **Shared Responsibility**: Both LGD and NCSC are responsible for identifying potential cyber emergencies.
- **Sources of Information**: Reports from the public, entities, and technical capabilities.
- **Normal Course of Business**: Incident identification is part of ongoing operations.
- **Situational Awareness & Preparedness**: Maintaining awareness and preparing for incidents.
- **Communication**: Regular reporting channels are used for communication.

Warning Mode

- **Warning Mode Activation**: Triggered by evidence of heightened risk.
- **Information Sources**: CyCLONe, international peers, threat intelligence, and NCSC capabilities.
- **Stakeholder Communication**: Reinforced communication with government and private sector.
- **Incident Prevention**: Cooperative efforts to prevent incident spread.
- **Escalation Decision**: Filtering mechanism to determine if Full Activation Mode is required.

Triggering Warning Mode

- **Triggering Authorities**: National actors (LGD or NCSC) or EU CyCLONe.
- **Activation Criteria**: Incident reports, intelligence, or specific threats.
- **LGD Initiation**: LGDs can initiate Warning Mode for specific entities or sectors.
- **Notification**: OEP notifies NCEP stakeholders via email.

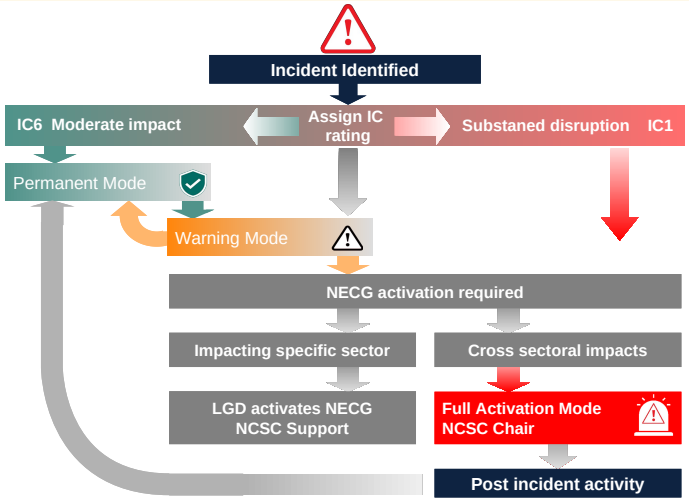
During Warning Mode

- **NCSC Engagement**: Supporting victims, sharing information, and conducting forensic analysis.
- **Information Sharing**: Sharing technical details and risk assessments with stakeholders.
- **NECG Briefings**: Regular updates to maintain situational awareness.
- **EU CyCLONe**: Member state-led coordination mechanism for large-scale incidents.
- **Mode Synchronisation**: Automatic activation of national modes based on EU CyCLONe status.

Exit Warning Mode

- **Meetings and Briefings**: Organised to discuss incident response and potential escalation.
- **Mode Exit Criteria**: Successful eradication, mitigation, or containment of risks.
- **NECG Activation**: Triggered by persistent risks and severe operational disruption.
- **Notification**: OEP informs stakeholders about Warning Mode exit.

NCEP Cooperation Modes and Escalation Path



Activate the NECG

- **LGD Responsibility**: Established in SEM-NSF.
- **Sector-Specific Incidents**: LGD leads, with NCSC providing cyber expertise.
- **Government Coordination**: NCSC empowers departments through Gov-CORE.
- **Multi-Sector Incidents**: NCSC leads in Full Activation Mode.
- **Scenario Examples**: Government network incidents and widespread technology vulnerabilities.

Full Activation Mode

- **Full Activation Trigger**: National cyber emergency requiring NECG activation.
- **Decision Authority**: NCSC or Minister for DECC.
- **NECG Convening**: OEP convenes NECG within one hour.
- **International Trigger**: Large-scale incidents identified by CyCLONe or international peers.
- **National Security Incidents**: May be handled outside the NECG process.

Exit Full Activation Mode and Post Activity

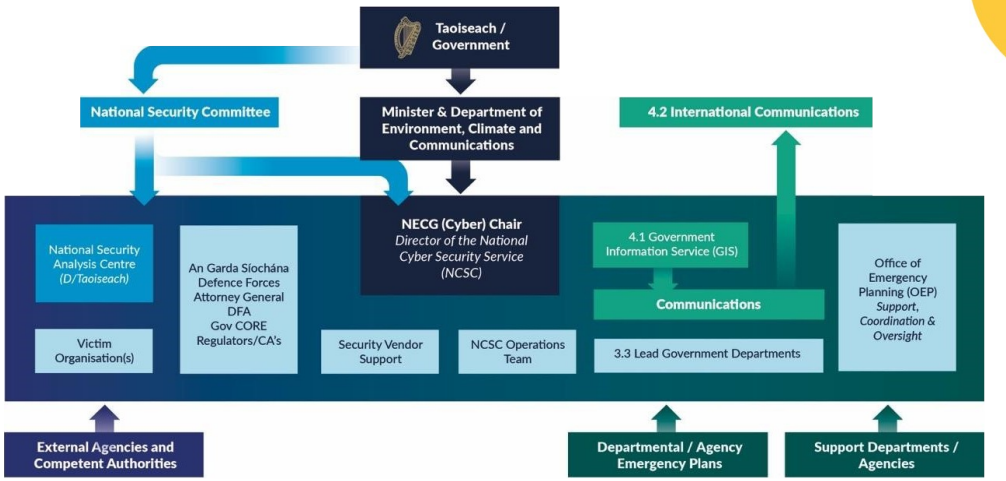
- **Exit Criteria**: Essential services restored, root cause identified, and consensus on emergency end.
- **Post-Incident Activity**: AAR creation and lessons learned.
- **NCEP Updates**: Updating NCEP and incident response playbooks.
- **Exercises**: Periodic exercises to test NCEP and sectoral plans.
- **Continuous Improvement**: Refining response at all levels.

Roles

Roles

- National Emergency Coordination Group
- National Emergency Coordination Group Chair
- Lead Government Department
- National Cyber Security Centre Operations Team
- Victim organisations

NECG (cyber)



National Emergency Coordination Group

- **Purpose**: Coordinate and support during emergencies.
- **Convening**: OEP convenes within one hour of declaration.
- **Role**: Maintain situational awareness and coordinate response.
- **GTF Member Attendance**: Mandatory for first meeting, discretionary for subsequent meetings.
- **Sub-Groups**: Established to address specific issues.

National Emergency Coordination Group membership

- NCSC chair (NCSC Director or deputy)
  - Representing LGD DECC for Cyber incidents
- National Security Analysis Centre
- Victim organisation(s) (as required)
- Government Information Services
- Attorney General's Office
- Department of Foreign Affairs
- Department of Justice
- An Garda Síochána (Police)
- Defence Forces
- Private cyber security vendors (as required)
- Office of Emergency Planning
- Lead and Support Government Department (as required)
- Gov-CORE Chair
- Regulators and Competent Authorities (as required)

National Emergency Coordination Group Chair

- **NCSC Leadership**: NCSC Director chairs NECG.
- **Decision-Making**: Chair leads, seeks consensus, and refers to Ministers if needed.
- **Statutory Limitations**: NECG cannot override statutory decisions of other bodies.
- **Urgent Issues**: Chair seeks consensus and refers to Ministers if unresolved.
- **Ministerial Approval**: Required for proposed measures.
- **Unresolved Cross-departmental issues**: referred to relevant Ministers or the Taoiseach (Prime Minister).

LGDs during a cyber emergency

- **Sectoral Responsibility**: LGDs manage cyber emergency impacts within their sectors.
- **Key Responsibilities**: Physical response, recovery, situational awareness, and briefing.
- **Risk Management**: Risk assessment, planning, prevention, mitigation, response, and recovery.
- **Collaboration**: Identifying and collaborating with Support Departments/Agencies.

National Cyber Security Centre Operations Team

- **Operations Team Role**: Proactive prevention and response.
- **Incident Response Phases**: Preparation, detection/analysis, containment, eradication, recovery, and post-event activity.
- **Emergency Response Actions**: Scope identification, impact assessment, containment, analysis, and information sharing.
- **Victim Support**: Guidance, support, and remediation assistance.
- **Information Management**: Capturing incident details for risk management and communication.
- **Government Coordination**: Requesting actions from government, public sector, and CNI operators.
- **International Cooperation**: Coordinating with NCSC-UK and NCSC-NI.

Victim organisations

- **Responsibility**: Initial incident response ownership.
- **NCSC Support**: NCSC provides support and guidance.
- **Swift Reporting**: Prompt reporting of incidents to NCSC.
- **Specialist Engagement**: Engaging specialists if required.
- **Data and System Provision**: Sharing data and systems with NCSC for analysis.

Private Cyber Security Vendors

- Technical specialists from the private sector can assist in incident response.
- The NCSC may connect affected entities with suitable vendors.
- Vendors provide cyber security expertise and resources for incident mitigation.
- The NCSC is not liable for vendor actions on victim networks.
- Liability is a matter of contractual agreement between the victim organisation and the vendor.

Law Enforcement

- Report cyber incidents to AGS or relevant authorities.
- Prioritise critical service restoration and emergency termination.
- NCSC and law enforcement will collaborate on incident response.
- Ensure forensic evidence is captured during recovery.
- AGS leads investigations, prosecutions, and international cooperation.
- Information sharing between NCSC and AGS is likely.

Defence Forces role in Cybersecurity

- **Primary focus**: Protection of Defence networks.
- **Emergency support**: Can provide resources to the NCSC when capacity is exceeded.
- **Potential assistance**:
  - Technical staff deployment
  - ICT equipment and materials
  - Manpower and logistical support

Office of the Attorney General

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

Intelligence and Security

- **Intelligence providers**: DF, NCSC, AGS, and National Security Analysis Centre.
- **Intelligence sharing**: Prioritise sharing with senior leadership and incident responders.
- **Intelligence utilisation**:
  - Build situational awareness
  - Share threat indicators and analysis
  - Identify and address gaps
  - Create a comprehensive incident picture.
- **Sector-level partnerships**: May provide additional intelligence support.

National Security Committee (NSC)

- Chaired by the Secretary General to the Government.
- Composed of high-level representatives from key departments and agencies.
- Secretariat provided by the National Security Analysis Centre.
- Advises the Government and Taoiseach on high-level security issues and responses.

National Security Analysis Centre (NSAC)

- Established in 2019 to provide strategic analysis to the Government.
- Analyses key threats to Ireland's national security.
- Staffed by seconded personnel from various departments and agencies.
- Collaborates closely with the NCSC and other security organisations.

Attribution and Cyber Diplomacy

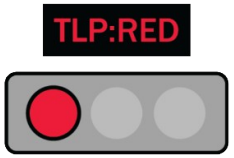
- **Attribution**: Challenging due to technical, political, and legal aspects.
  - **Technical Attribution**: NCSC, AGS, and vendors can provide technical analysis with varying confidence.
  - **Public Attribution**: Government decides based on NCSC advice.
- **Cyber Diplomacy**: DFA leads on diplomatic responses for cross-border incidents.
- EU Tools:
  - **Cyber Diplomacy Toolbox**: Coordinates EU member state responses to malicious cyber activities.
  - **Hybrid Toolbox**: Focuses on identifying and responding to complex hybrid campaigns.
  - **FIMI Toolbox**: Aims to address foreign information manipulation and interference.

Communications

Traffic Light Protocol v2.0 (TLP)

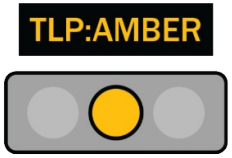
- TLP is a set of four labels (**RED**, **AMBER**, **GREEN**, **CLEAR**) used to indicate sharing boundaries.
- It provides a simple schema for indicating with whom potentially sensitive information can be shared.
- It is optimised for ease of adoption, human readability, and person-to-person sharing. (https://www.first.org/tlp)

TLP:RED



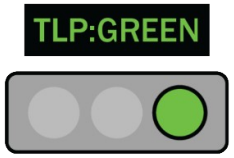
- **For the eyes and ears of individual recipients only, no further disclosure**.
- Sources may use info when it cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organisations involved.
- Recipients may therefore not share this info with anyone else. In the context of a meeting for example, this info is limited to those present at the meeting.

TLP:AMBER



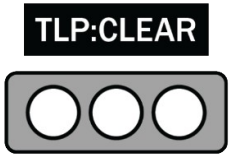
- **Limited disclosure, recipients can only spread this on a need-to-know basis within their organisation and its clients**.
- Sources may use info when it requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organisations involved.
- Recipients may share info 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.

TLP:GREEN



- **Limited disclosure, recipients can spread this within their community**.
- Sources may use info when it is useful to increase awareness within their wider community.
- Recipients may share info with peers and partner organisations within their community, but not via publicly accessible channels.
- Info may not be shared outside of the community.

TLP:CLEAR



- **Recipients can spread this to the world, there is no limit on disclosure**.
- Sources may use info when it carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- Subject to standard copyright rules, info may be shared without restriction.

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:

RED, **AMBER**, **GREEN**, **CLEAR**

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.

RED, **AMBER**, **GREEN**, **CLEAR**

National Communications

- During a national cyber emergency, it is vital to maintain coherent and unified communications with the public, victim organisations, and other stakeholders.
  - **NECG Communications Subgroup**: Chaired by NCSC, supported by GIS and OEP.
  - **Regular Updates**: NECG provides regular updates to the public through GIS.
  - **Coordinated Messaging**: Close collaboration with other government departments and agencies.
  - **Technical Advisories**: NCSC continues to issue technical advisories and guidance.

International Communications and Cooperation

- NCSC and supporting departments coordinate with international counterparts.
- EU Structures:
  - CSIRT network
  - EU-Cyclone network
  - NIS CG
  - Single Point Of Contact networks
  - HWPCI
  - COREPER
  - IPCR
- **JHA Structures**: COSI
- **Bilateral Cooperation**: With peer organisations.

Incident Handover

setu.ie
INSPIRING FUTURES

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
  - Incident is contained within a single sector
  - Incident severity is no longer IC1 or IC2 category incident.

Post-Incident Review

setu.ie
INSPIRING FUTURES

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.

Exercise

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | setu.ie
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Thank you

engcore
advancing technology