Tithe an Oireachtais
Houses of the Oireachtas

An Comhchoiste um Ghnóthaí an Aontais Eorpaigh

Cibearshlándáil agus Seasmhacht – An Todhchaí a Dhaingniú

Bealtaine 2022

Joint Committee on European Union Affairs

Cybersecurity & Resilience – Securing the Future

May 2022

33/EUA/07

Joint Committee on European Union Affairs

John Brady T.D.
Sinn Féin

Dara Calleary T.D.
Fianna Fáil

Francis Noel Duffy T.D.
Green Party

Seán Haughey T.D.
Fianna Fáil

Brendan Howlin T.D.
Labour
Leas-Chathaoirleach

Marian Harkin T.D.
Independent

Joe McHugh T.D.
Fine Gael
Cathaoirleach

Neale Richmond T.D.
Fine Gael

Ruairí Ó Murchú T.D.
Sinn Féin

Senator Lisa Chambers
Fianna Fáil

Senator Regina Doherty
Fine Gael

Senator Sharon Keogan
Independent

Senator Vincent P Martin
Green Party

Senator Michael McDowell
Independent

Cathaoirleach's Foreword

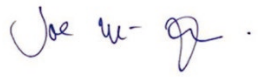
The topic of cybersecurity was identified as an issue for consideration by the Committee. In a world where technology forms an integral part of our daily lives, ensuring that this space is safe and secure is of upmost importance. We have witnessed the disruption and chaos a cyberattack can have on a vital service such as our health system. During a time when our health system was under immense pressure, a very calculated attack was carried out with the ultimate aim of causing mass disruption while also seeking a monetary amount for their despicable actions. It is incomprehensible to think that they achieved their goal with a laptop and internet connection. The Committee wishes to acknowledge the work by the various organisations and agencies involved in an effort to minimise damage and get systems back online. The co-operation shown between national and EU agencies demonstrates the benefits of a harmonised approach to this issue. As a borderless crime, we are only stronger if we work together, and the Committee welcomes initiatives taken at an EU level in an effort to increase a collaborative approach.

Prior to the attack on our health system, cybersecurity has not always been treated with the seriouseness it deserves, with levels of investment not always reflecting the requirements needed to enhance cyber resilience. Cyberattacks are becoming more sophisticated and widespread and the Committee believe that investing in our critical infrastructure and building cyber resilience is of paramount importance.

While investment and enhanced co-operation are all elements that can contribute to increased cybersecurity and resilience, the Committee are of the opinion that responsible and informed individuals are also a key component in building cyber resilience. The internet can be seen as a faceless tool which can lead to a level of complacencey in our online activities. It is this level of complaceney that can leave systems exposed to cyber attacks. Users must be educated about the risks associated with their online activities.

While acknowleding that steps have been taken to produce guidelines and build awareness around this, the Committee believes a more structured approach to cybersecurity and resilience be launched to increase cyber awareness and educate users on the need to be vigilant when online. The Committee believe that educated and informed users are a vital element in securing our systems and networks and that more initiatives are needed to address this.

The Committee held a series of public hearings from November to December 2021 and engaged with representatives from various organisations and institutions. On behalf of the Committee, I would like to express my gratitude to all the witnesses who attended our public hearings to give evidence and who provided briefing documents. We would also like to thank Minister of State Mr Ossian Smyth for his engagement. The Committee has made a set of recommendations and we hope that they will assist the Government and various institutions.



Joe McHugh, TD
Cathaoirleach
Joint Committee on EU Affairs
May 2022

Table of Contents

List of Acronyms and Abbreviations Used

CARD	Coordinated Annual Review on Defence
CSIRT	Computer Security Incident Response Team
DG CONNECT	European Commission Directorate General for Communications Networks, Content and Technology
EDA	European Defence Agency
ENISA	European Union Agency for Cybersecurity
ESSOR	European Secure Softward Defined Radio
HSE	Health Service Executive
ITRE	European Parliament Committee on Industry, Research and Energy
MIC	EU MILCert Interoperability Conference
NCSC	National Cybersecurity Centre
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIS2 Directive	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
PESCO	Permanent Structured Cooperation
UN	United Nations

1. Introduction

The world is an evermore connected place and almost every facet of our lives is affected by improvements in technology and connectivity. It is possible to use online services to apply for a passport, attend a conference thousands of miles away from your kitchen table or pay for items using your phone. The Covid-19 pandemic has only accelerated the transition to online service delivery.

This is a trend that enables significant benefits in society. However, it is also a trend that creates significant risks in society and exacerbates Ireland's vulnerability to cyberattacks. Ensuring protection of IT systems, data services and communications networks is of increasing importance to safeguarding economic and social wellbeing.

The draft National Risk Assessment for 2021-2022 identifies cybersecurity as one of the strategic risks facing Ireland.[1] There is a wide breadth in risks posed by cyberattacks. These risks include data breaches, disruption to service provision, harm to major national infrastructure, economic harm, the undermining of trust and confidence in digital systems, backlash against digitisation, and reputational damage to businesses and the public service.

The vulnerabilities caused by cybersecurity threats were acutely demonstrated by the ransomware attack on the Health Service Executive (HSE) in May 2021. This incident caused nationwide operational disruption to the provision of healthcare in Ireland, compounding upon the existing pressures on the service caused by the Covid-19 pandemic. In addition to the operational impacts, this incident creates a risk that sensitive personal data and corporate data held by the HSE will be leaked online. The scale of damage that can be caused by cybersecurity threats is laid bare by the HSE's independent report on the cyberattack: the attack leading to a full shutdown of the HSE

[1] Department of the Taoiseach, *Draft National Risk Assessment – Overview of Strategic Risks 2021/2022* (2021) <gov.ie - Draft National Risk Assessment 2021/2022 - Public Consultation (www.gov.ie)> accessed 13 January 2022, p. 56.

IT system was ultimately traced to a single user opening a malicious attachment to a phishing email.[2]

Ireland is by no means an outlier amongst its European Union peers in its vulnerability to cybersecurity threats. The European Union Agency for Cybersecurity (ENISA)'s Threat Landscape Report 2020-2021 outlines that ransomware attacks are the prime cybersecurity threat across the EU. The volume and complexity of cyber attacks have increased, and that the Covid-19 pandemic has impacted upon the cybersecurity landscape.[3] The Threat Landscape report further outlines major cybersecurity incidents that have taken place across the EU. The City of Liege in Belgium experienced disruption to public services such as provision of driving licenses and appointments for marriage registration. Düsseldorf University Hospital experienced disruption to patient care resulting in the death of a patient. Over 200 Belgian organisations, including the Government and Parliament, have experienced cyberattacks resulting in a part of the country's internet being taken offline.[4]

Cybersecurity feeds into several of the European Commission's six priorities for 2019-2024. It is one of the issues identified under the "Shaping Europe's Digital Future" policy priority; and is also a component of the European Security Union, an action under the "Promoting our European Way of Life" priority. President Urusla von der Leyen, at her State of the Union address on 15th September 2021, framed cybersecurity as a defence issue, outlining her vision for a European Defence Union:

> *'You no longer need armies and missiles to cause mass damage. You can paralyse industrial plants, city administrations and hospitals – all you need is your laptop. You can disrupt entire elections with a smartphone and an internet connection'*.[5]

[2] Health Servive Executive, *Conti Cyber Attach on the HSE. Independent Post-Incident Review – Executive Summary and Learnings for Other Organisations* (2021) <conti-cyber-attack-on-the-hse-executive-summary.pdf> accessed 13 January 2022, p. 2.
[3] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2021* (2021), <ENISA Threat Landscape 2021 — ENISA (europa.eu)> accessed 13 January 2022, pp. 7-24.
[4] *ENISA Threat Landscape 2021*, pp. 97-114.
[5] Von der Leyen, Ursula, *State of the Union Address* (speech delivered to European Parliament 15th September 2021), <State of the Union Address by President von der Leyen (europa.eu)> accessed 13 January 2022.

President von der Leyen outlined the European Commission's intentions to strive to become a leader in cybersecurity, and to introduce a new European Cyber Defence Policy, including legislation on common standards under a new European Cyber Resilience Act.

President von der Leyen's newly announced cyber defence policy builds upon the existing EU Cybersecurity Strategy for the Digital Decade, presented at the end of 2020. This Strategy includes measures such as a proposal for a new Directive on measures for a high common level of cybersecurity across the Union (NIS 2), the Cybersecurity Act which strengthens the mandate of ENISA, a new Resilience of Critical Entities Directive, and the establishment of a Joint Cyber Unit and European Cybersecurity Competence Centre.

2. Executive Summary

The Joint Committee on European Union Affairs, on foot of President von der Leyen's State of the Union address, identified cybersecurity as an issue of cross-sectoral and strategic interest to the European Union, and agreed to carry out a programme of scrutiny which underpins this report. The Committee held three public meetings, the proceedings of which constitute the core evidence base for this report.[6]

The Committee identified three distinct streams of scrutiny, and the structure of this report follows those streams:

1. "An Overview of the EU Cybersecurity Strategy for the Digital Decade"
2. "Developing an Irish Cybersecurity Strategy in line the EU Cybersecurity Strategy".
3. "The role of the EU Security Union and EU Defence Union in enhancing cyber resilience in member states".

The Committee considered the importance of key EU legislative initiatives in addressing inconsistencies in implementation at member state level of existing cybersecurity requirements. Evidence received outlines that consistent implementation is important in ensuring a high common standard of cybersecurity across the EU, which is particularly important in the context of the cross-border nature of cyber threats. Legislative initiatives such as "NIS2" and the Resilience of Critical Entities Directive will harmonise standards and expand the number of entities deemed "essential service operators". The Committee also considered inconsistencies in the level and model of cybersecurity investment in member states, and the different funding models.

In an Irish context, the Committee considered the government's current cybersecurity strategy, plans to review the strategy, and the role of the National Cybersecurity Centre. The Committee received evidence on the importance of awareness, skills and education in promoting cybersecurity. The Committee also addressed the theme of

[6] See appendix 2 for full details of public meetings.

collaboration between industry, government, and academia, highlighting its importance.

The Committee examined the importance of cybersecurity resilience in critical entities and in supply chains. The Committee received evidence that the dominance of a small number of service providers can have wider effects whereby a single vulnerability can affect a large number of entities. The Committee also heard evidence on the importance of security-by-design in protecting supply chains.

The role of pan-EU cooperation in cybersecurity was also an important theme in the proceedings. The Committee received evidence regarding the sharing of information with EU colleagues following the HSE cyberattack, the role of EU agencies such as ENISA and the EDA in supporting member state capacity building, and proposals for a Joint Cyber Unit to enhance cooperation. The Committee also heard evidence that participation in joint cybersecurity exercises is on a voluntary basis.

The Committee considered the theme of cyber diplomacy, noting the importance of working with both EU member states and with third countries in order to enhance cybersecurity and respond to major cybersecurity incidents.

3. Conclusions and Recommendations

The Committee believes that cybersecurity threats pose a major risk to economic and social wellbeing in Ireland. Actors posing cybersecurity threats operate across international borders, and cybersecurity threats are present in all EU member states. Accordingly, the Committee broadly welcomes EU proposals that will enhance cybersecurity resilience at member state level.

The Committee welcomes the work ongoing to enhance cybersecurity resilience in Ireland, and in particular welcomes both the increased resources and strengthened mandate of the National Cybersecurity Centre, as well as the plans to review the National Cybersecuirty Strategy. The Committee notes the importance of cooperation both at EU level and with third countries and considers cyber diplomacy an important facet of Ireland's cybersecurity framework.

The Committee, having regard to the evidence and analysis presented in this report, makes the following recommendations:

Recommedation 1:
The Committee recommends that Ireland support EU efforts to implement a framework that achieves a harmonised level of cybersecurity across member states, while also facilitating greater cooperation on a voluntary basis.

Recommendation 2:
The Committee recommends that priority is given to ensure that EU legislative proposals in the cybersecurity field such as NIS2 and the Resilience of Critical Entities Directive effectively enhance cybersecurity resilience and capacity at member state level.

Recommendation 3:
The Committee recommends that the upcoming review of the National Cybersecurity Strategy consider readiness for implementation of proposals under the EU Cybersecurity Strategy for the Digital Decade. The revised National Cybersecurity Strategy should seek to implement the requirements of key EU legislative proposals in the cybersecurity field to the highest possible standard.

Recommendation 4:
The Committee recommends that the upcoming review of the National Cybersecurity Strategy have particular regard to the importance of critical infrastructure and of supply chains to the wider cybersecurity ecosystem.

Recommendation 5:
The Committee recommends that in preparing for implementation of the proposed NIS2 Directive and Resilience of Critical Entities Directive, the Government should examine best practice among other member states in identifying and protecting essential service operators.

Recommendation 6:
The Committee recommends that the upcoming review of the National Cybersecurity Strategy should have regard to international best practice regarding budgeting mechanisms for cybersecurity investments.

Recommendation 7:
The Committee recommends that the upcoming review of the National Cybersecurity Strategy seeks to leverage opportunities to drive awareness, education and skills in the cybersecurity field, and to engage in national level awareness activities tying in with European Cybersecurity Month.

Recommendation 8:
The Committee recommends that the upcoming review of the National Cybersecurity Strategy should seek to use the significant levels of industry expertise in cybersecurity in Ireland, enhance collaboration between Government, industry and academia, and should also enhance measures promoting careers, skills and training in the cybersecurity field.

Recommendation 9:
The Committee recommends that Ireland should leverage all possible opportunities to cooperate with other member states and EU agencies in order to enhance cybersecurity resilience on a voluntary basis and in accordance with existing cooperation frameworks to which the state is party.

Recommendation 10:
The Committee recommends that the Government should pursue opportunities to cooperate with like-minded third countries on cybersecurity matters. In particular, the Government should take stock of progress regarding implementation and ratification of the Budapest Convention on Cybercrime.

4. Overview of EU Cybersecurity Strategy for the Digital Decade

The EU Cybersecurity Strategy for the Digital Decade was presented in December 2020 by the European Commission along with the High Representative of the Union for Foreign Affairs and Security Policy. It outlines the key initiatives at EU level supporting greater cybersecurity resilience.

The Strategy focuses on three main angles: firstly, to build resilience, technological sovereignty and leadership; secondly to build operational capacity; and thirdly to build increased international cooperation.[7] Key initiatives under the strategy including a revision to the Network and Information Security Directive (NIS2), a Directive on the Resilience of Critical Entities, a new Cybersecurity Act establishing a new permanent mandate for the EU Agency for Cybersecurity (ENISA), the establishment of a new Joint Cyber Unit and EU Cybersecurity Competence Centre, and the development of a 5G Toolbox.

4.1 NIS2 Directive

A proposed Directive providing for high common levels of cybersecurity across the Union, often referred to as NIS2, is the centrepiece of the EU Cybersecurity Strategy for the Digital Decade. The Committee welcomes NIS2 as an effort to implement a framework that achieves a more harmonised level of cybersecurity across member states and to enhance cybersecurity resilience and capacity at member state level.

NIS2 seeks to build upon the existing Network and Information Security Directive (NIS). NIS required member states to have certain national cybersecurity abilities such as a Computer Security Incident Response Team (CSIRT) in place, provided for cross border cooperation, and required member states to supervise the cybersecurity of critical market operators such as water, transport and health.

Mr Ciarán Cuffe MEP outlined that due to slow progress in the implementation of NIS, that the European Commission introduced NIS2, which Mr Cuffe's European

[7] Joint Committee on European Union Affairs (3 November 2021) <Joint Committee on European Union Affairs debate - Wednesday, 3 Nov 2021 (oireachtas.ie)> accessed 13 January 2022.

Parliament Industry, Research and Energy Committee (ITRE) voted on in the week prior to his appearance before the Joint Committee. NIS2, as outlined by Mr Cuffe, "*aims to strengthen cybersecurity capabilities and to have better information sharing and co-operation on cybersecurity crisis management at national and EU level. It provides for an all-hazards framework to support member states to prevent, resist and recover from disruptive attacks wherever their source may be*."

It is important that in order to effectively enhance cybersecurity capacity and resilience across member states, that NIS 2 is implemented to a high standard across all member states. Mr Cuffe further outlined that "*really it comes down to the individual member state to implement not only the first directive from five years ago but the new directive when it comes into force. This is where the critical weakness is. It is about the implementation of the directives at member state level*."[8]

NIS2 will address inconsistencies in implementation at member state level seen with the NIS Directive. For instance, Ms Lorena Boix Alonso, Director of Cybersecurity for DG CONNECT, outlined that Ireland identified a large number of hospitals as being in the Directive's scope while other member states identified none, and to address this the NIS2 Directive will extend the sectors and entities covered. Mr Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity (ENISA), also highlighted the inconsistencies in implementation of the NIS Directive. For example, Ireland has designated approximately 70 entities as essential service providers, compared to 10,000 entities in Finland. Mr Lepassaar outlined that under the NIS2 proposals in their current format, all entities above a certain size would be included, and member states would have the flexibility to include additional entities below that size. Mr Lepassaar called on the Committee to express its support for the quick and swift adoption of NIS2.[9]

Minister of State Mr Ossian Smyth welcomed the review of the NIS Directive, and outlined that the Government's focus in the negotiations is to ensure NIS2 "*provides a solid basis for practical measures at national and Union level to strengthen the cyber*

[8] JCUEA 3rd November 2021
[9] Joint Committee on European Union Affairs 1st December 2021 <Joint Committee on European Union Affairs debate - Wednesday, 1 Dec 2021 (oireachtas.ie)> accessed 13 January 2022.

resilience of critical services and important industry sectors; to facilitate information sharing and exchange of best practices; and to strengthen our capacity to respond to major cybersecurity incidents".[10]

4.2 Resilience of Critical Entities Directive

In order to achieve high levels of cybersecurity and safeguard the reliable provision of services on which we rely, it is important to identify the important sectors and service providers, i.e., the "*critical entities*", that must be protected from cyber attacks. The Resilience of Critical Entities Directive is the EU legislative proposal that identifies these sectors and lays down rules to ensure a high level of protection.

Ms Lorena Boix Alonso outlined to the Committee that the Resilience of Critical Entities Directive is intended to complement NIS2. NIS2 deals with the obligations on companies to report, notify and take certain security measures on incidents, as well as monitoring and enforcement tools. Complimentarily, the Resilience of Critical Entities Directive deals with the gap that exists regarding products and services currently available that are not covered by cybersecurity legislations.[11]

The new Directive expands the scope and depth of the older 2008 Directive, and ten sectors are now included. Member states will be required to adopt national strategies for ensuring the resilience of critical entities and to carry out regular risk assessments.

4.3 Safeguarding of democratic integrity

The Committee explored the importance of cybersecurity in safeguarding the electoral process. Ms Boix Alonso outlined that the EU CSIRT performed a cybersecurity exercise for the 2019 European election, and that the European Commission has developed a compendium available to national electoral authorities. Mr Cuffe stated to the Committee that IT skills are increasingly important in election monitoring exercises.[12]

[10] JCEUA 1 December 2021.
[11] JCEUA 3 November 2021.
[12] JCEAU 3 November 2021.

5. Developing an Irish Cybersecurity Strategy in line with EU Cybersecurity Strategy

The National Cybersecurity Strategy was adopted in 2019 and follows the first strategy adopted in 2015. It sets out 20 measures including the further development of the National Cybersecurity Centre (NCSC), an updated risk assessment of the vulnerability of critical national infrastructure, the expansion and deepening of the Critical National Infrastructure protection system, the development of baseline security standards for public bodies and compliance standards for telecom operators, the establishment of a Government IT Security forum, measures to promote skills, awareness and training in cybersecurity and promote cybersecurity career options, and measures to support collaboration between Government, industry, and academia.[13] Minister of State Mr Ossian Smyth outlined to the Committee that the Strategy is due to be reviewed in 2022 as required under the NIS Directive and recommended following the NCSC capacity review.[14]

This review should serve as an opportunity to consider Ireland's readiness for implementation of the measures proposed under the EU Cybersecurity Strategy for the Digital Decade and should seek to implement these measures to the highest possible standard.

5.1 Safeguarding of critical infrastructure and supply chains

Key to high standards of cybersecurity resilience is protecting the critical infrastructure and essential service providers that are key to the functioning of the economy and society. Under the existing EU cybersecurity framework there are significant inconsistencies with how entities are designated as essential service providers. The upcoming review of the National Cybersecurity Strategy should consider best practice across member states in identifying essential service providers and should consider the importance of protecting critical national infrastructure.

[13] Government of Ireland, *National Cyber Security Strategy 2019-2024* (2019) <gov.ie - National Cyber Security Strategy (www.gov.ie)> accessed 13 January 2022.
[14] JCEUA 1 December 2021.

Minister of State Mr Ossian Smyth acknowledged to the Committee the discrepancy among member states in the number of entities designated as essential service providers under the existing legislative framework, and that there would likely be a higher number under NIS2 proposals.[15] Mr Ciarán Cuffe MEP outlined that cyberattacks could target critical infrastructure such as health services, water services, undersea communications infrastructure, or the energy network. Mr Cuffe stated his belief that exercises similar to physical exercises conducted by the Defence Forces should take place.[16]

In addition to public infrastructure, cybersecurity resilience also hinges on a secure supply chain. Single service providers can have a wider significance in the supply chain and cybersecurity ecosystem. Mr Juhan Lepassaar outlined to the Committee that risk to the supply chain is increased by the dominance of certain service providers, as one single vulnerability could affect a large number of entities across borders. Minister of State Mr Ossian Smyth outlined the importance of a "*security by design*" approach on the part of developers of software. The upcoming review of the National Cybersecurity Strategy should have regard to the importance of secure supply chains to the wider cybersecurity ecosystem.

5.2 Resourcing

There are disparities in the resources allocated to cybersecurity in the EU compared to the US, that may be a limiting factor in the robustness of cybersecurity standards in the EU currently. Mr Lepassaar outlined research on this topic stating that EU entities spend 41% less on cybersecurity than their US counterparts, and that 67% of essential service operators in the EU believe they need more investment in cybersecurity. Mr Lepassaar noted that in an Irish context, 22 of 36 essential service operators surveyed believe they need more investment in cybersecurity, but that Ireland is "*showing the way*" in cybersecurity investment: Ireland has the highest median number of cybersecurity hires across the EU, and 50% of Irish essential service operators have cyber insurance, compared to an average EU rate of 43%.[17]

[15] JCEUA 1 December 2021.
[16] JCEUA 3 November 2021.
[17] JCEUA 1 December 2021.

There are varying models of ensuring adequate investment in cybersecurity, and the upcoming review of the National Cybersecurity Strategy should consider international best practice in cybersecurity budgeting. Mr Lepassaar called on the Committee to find ways of increasing and ringfencing cybersecurity investments by critical sector entities. Mr Lepassaar pointed to the example of Germany, where all healthcare providers are required to spend 15% of their digital investments on cybersecurity. Minister of State Mr Ossian Smyth outlined that the Government does not support that approach, and that it rather supports measures based on performance and outputs rather than inputs. Minister of State Smyth further outlined public bodies will be subject to a compliance framework on minimum security standards, and cybersecurity concerns will be built into public procurement requirements.[18]

5.3 Ireland-EU cooperation in Cybersecurity field

There are a number of existing and proposed EU bodies that facilitate cooperation between member states on a voluntary basis, such as ENISA, the EDA, the proposed Joint Cyber Unit, and the newly established Euroepan Cybersecurity Competence Centre. This cooperation is an important means in preparing for and reacting to cybersecurity incidents.

The Committee heard evidence regarding Irish-EU cooperation in the cybersecurity field, and in particular in response to the HSE malware attack. Ms Boix Alonso stated to the Committee that in response to the HSE attack, Ireland triggered the EU co-ordination system, and sought support from the European Computer Security Incident Response Team (CSIRT).[19] Mr Lepassaar outlined that through an EU-coordinated network of member-state level CSIRTs, Irish authorities were able to share information with other member states and to extract expertise from the network.

Mr Lepassaar praised the role of the National Cybersecurity Centre in responding to the attack:

> *From the cybersecurity point of view, the Irish National Cyber Security Centre does an excellent job, not only in responding to the crisis, but also in making*

[18] JCEUA 1 December 2021.
[19] JCEUA 3 November 2021.

sure that entities are well prepared. It rolled out procedural guidelines, manuals, trainings and exercises. It responded in an agile and prompt fashion and it shared information with other member states with the computer security incidence response teams, CSIRT, network so that other member states were knowledgeable about what was going on and could prepare as well. It was an exemplary response.[20]

5.4 Building awareness and skills in cybersecurity field

Awareness, training and skills are vital in enhancing levels of cybersecurity across member states. At a high level, cybersecurity expertise is important in designing secure systems, preparing for and reacting to cybersecurity incidents, and protecting vital infrastructure. It is also important that senior management of essential service providers understand that cybersecurity by design should be a central concern rather than a niche IT function. However, at a more local level, basic cybersecurity skills and awareness such as understanding the importance of password security and being wise to common phishing email scams is just as important.

At EU level, there are awareness initiatives such as European Cybersecurity Month, however Mr Cuffe stated that he did not know if these campaigns are permeating through at member state level. Mr Cuffe outlined the need for greater cybersecurity awareness at a local level: "*We are all guilty of simplifying things. In a world where half a dozen passwords are often needed in the course of a day we often take shortcuts. We need to practice better security awareness in our own operations*."[21]

The Committee also heard evidence regarding the availability of cybersecurity skills. Ms Boix Alonso outlined the need for both basic cyber skills, such as awareness of phishing scams on the part of end users, and for specialist skills, outlining the availability of EU funding for universities and workforces to help in specialisation and providing specialist courses on cybersecurity.[22]

[20] JCEUA 1 December 2021.
[21] JCEUA 3 November 2021.
[22] JCEUA 3 November 2021.

Minister of State Mr Ossian Smyth outlined to the Committee initiatives aimed at improving education and standards, such as the publication by the National Cybersecurity Centre of baseline security standards for public sector bodies.[23]

5.5 Cybersecurity ecosystem in Ireland, including role of industry and academia

There is significant cybersecurity expertise available in Ireland. In industry, there are a large number of Irish and Irish-based multinational companies providing cybersecurity services, and academic hubs in the field include the UCD Centre for Cybersecurity and Cybercrime Investigation. This expertise can be leveraged in order to ensure greater cooperation between Government, industry and academia. This cooperation can allow the Government to leverage the significant levels of cybersecurity expertise in Ireland, can promote careers and training in cybersecurity, and can allow Ireland to benefit from the significant economic opportunities offered by the global cybersecurity market.

Minister of State Mr Ossian Smyth outlined to the Committee that Government works with academia in the cybersecurity field, and that Cyber Ireland encourages cooperation between Government, industry and academia.[24]

The Committee notes the proceedings of the Joint Committee on Transport and Communications on the 25th May 2021, where that Committee heard evidence on the state of the cybersecurity industry in Ireland: there are over 40 multinational companies with cybersecurity operations in Ireland, over 60 Irish cybersecurity companies and startups, and 6,000 people working in cybersecurity in Ireland and 30,000 people with cybersecurity skills. Cybersecurity represents an opportunity to Irish firms, with the global cybersecurity market expected to be worth $270 billion by 2026.[25]

[23] JCEUA 1 December 2021.
[24] JCEUA 1 December 2021.
[25] Joint Committee on Transport and Communications (25 May 2021) <Joint Committee on Transport and Communications debate - Tuesday, 25 May 2021 (oireachtas.ie)> accessed 13 January 2022.

6. The role of EU Security and Defence Union in enhancing cyber resilience in member states

The intersection between national security and cybersecurity is demonstrated by the risk profile posed by cyber threats, both in their impacts and origins.

The impacts posed by cyber threats are not limited to IT disruption and personal data breaches – many cyber attacks target states and public service providers, and critical national infrastructure can be harmed by cyber attacks causing major economic and social harm. Ireland is by no means an outlier in experiencing major cyber attacks. Ciarán Cuffe MEP outlined that Europol has noted "*a significant increase in attacks on Governments such as healthcare and education, energy and transport systems. EU institutions and bodies as well as member states have been targeted*".[26]

The origins of certain large scale cyber attacks also demonstrate the intersection between national security and cybersecurity. The ENISA threat landscape report highlights the cybersecurity risks posed by state actors and armed conflict.[27] Mr Cuffe stated to the Committee that the Belgian federal internal affairs department "*was subjected to a cyberattack of such a scale that it raised suspicions of the involvement of a foreign state*", and that "*it is commonly known certain states outside the EU would appear to be the focus for our attention on these attacks*".[28]

6.1 The role of EU Defence policies and the European Defence Agency in enhancing cybersecurity resilience

While EU competences in the Defence field is relatively limited, there is a role for EU Defence policies in coordinating and supporting member state capacity. Due to sensitivities on member state sovereignty in defence issues, this should take place on a voluntary basis within existing cooperative structures.

Mr Olli Ruutu, Deputy Chief Executive of the European Defence Agency (EDA), outlined measures being taken in the defence field to support member states: the 2020 Coordinationed Annual Review on Defence (CARD) idenfities more than 100

[26] JCEUA 3 November 2021.
[27] *ENISA Threat Landscape Report 2021,* pp. 16-22.
[28] JCEUA 3 November 2021.

collaborative opportunities to develop next-generation systems, and a number of capacity building projects are taking place under the framework of Permanent Structured Cooperation (PESCO), including European Secure Software-defined Radio (ESSOR), the cyber rapid-response teams and the Cyber and Information Domain Coordination Centre.

Mr Ruutu further outlined the EU MilCERT Interoperability Conference (MIC), an initiative of the EDA, which fosters operational co-operation among EU military computer emergency response teams and facilitates both strategic discussion and live fire exercises. 17 member states and Switzerland took part in the first edition of MIC. Mr Wolfgang Roehrig of the EDA also outlined that since 2014 the EDA has run cyber strategic decision-making exercises with seven member states, in order to train member states in dealing with a cyber crisis.[29]

6.2 Joint Cyber Unit

The Joint Cyber Unit, an initiative proposed by European Commission President Ursula von der Leyen, will provide a single point of coordination for cybersecurity operations requiring cross-member state or inter-agency responses.

Ms Lorena Boix Alonso outlined to the Committee the rationale and role of the proposed Joint Cyber Unit. Ms Boix Alonso outlined that "*there is a gap*" as cybersecurity incidents can be cross-sectoral in nature, affecting communities in disparate civil, law enforcement, and international contexts, and that the Joint Cyber Unit will provide "*a structure, a network, a one-stop shop, that is, a single point of contact. It can be defined in many different ways but it is a way to co-ordinate all of these communities when something big happens*".[30]

Mr Juhan Lepassaar illustrated how the Joint Cyber Unit may work in practice:

> "*Let us imagine the situation whereby there is a crisis that involves a certain sector which is deemed a critical sector at EU level. Of course it is the member states which are in charge of the response but they may need assistance. The*

[29] Joint Committee on European Union Affairs (24 November 2021) <Joint Committee on European Union Affairs debate - Wednesday, 24 Nov 2021 (oireachtas.ie)> accessed 13 January 2021.
[30] JCEUA 3 November 2021.

EU will then co-ordinate assistance to members states. It could be the agency I am in, it could be Europol or it could be a specific agency in the sector such as the European Union Agency for Railways for the railway sector or the European Maritime Safety Agency for the maritime sector, or the European Banking Authority for the financial services."[31]

6.3 Role of member states

The Committee explored the roles and responsibilities of member states in relation to cybersecurities taking place in the security and defence fields, and in particular examined the tensions between greater cooperation and national sovereignty. It is important that cooperation in sensitive fields such as national defence is voluntary in nature and takes place under existing cooperation frameworks. Ms Boix Alonso outlined that proposals for a Joint Cyber Unit would be "*what member states decide they want it to be*", and that member states through the Council would ultimately decide whether or not to approve the proposal.[32]

Mr Roehrig outlined that exercises which take place under the EDA are voluntary, and at the request of member states. Mr Ruutu further outlined that "*Our approach is based on member states voluntarily engaging in any activities they have sought co-operation for*". Mr Ruutu stated that the development of the EU Strategic Compass will give direction to work ongoing in the defence sphere at EU level.[33]

Minister of State Mr Ossian Smyth outlined to the Committee that Ireland is not excluded from taking part in EU cooperation mechanisms where there is a defence aspect.[34]

6.4 Cyberdiplomacy

The Committee received evidence on the role of diplomacy outside the EU in enhancing cybersecurity standards. Cooperation with like-minded third countries is an essential component in enhancing cybersecurity resilience.

[31] JCEUA 1 December 2021.
[32] JCEUA 3 November 2021.
[33] JCEUA 24 November 2021.
[34] JCEUA 1 December 2021.

Ms Boix Alonso outlined to the Committee that EU engagement with the UN and like-minded countries is important, and noted a US-led initiative on cooperation regarding ransomware and EU involvement in the Council of Europe Budapest Convention on Cybercrime.[35] The Committee notes that Ireland is a signatory of this Convention but has not yet fully ratified it, is the only EU member state that is not yet a full party to the Convention, and that only one other Council of Europe member state (Russia) has not ratified the Convention.[36]

Minister of State Mr Ossian Smyth outlined to the Committee the importance of international cooperation to Ireland's response to the HSE malware attack. Ireland received assistance from relevant agencies from third countries including the US and the UK, and Minister of State Smyth welcomed "*the leadership shown by President Biden and his administration in building a global alliance to combat the ransomware gangs who have caused havoc in recent years*". Minister of State Smyth also outlined the importance of cooperation between Ireland and the UK on both a north-south and east-west basis.[37]

[35] JCEUA 3 November 2021.
[36] Council of Europe, *Chart of signatures and ratifications of Treaty 185* (2022) <Full list (coe.int)> accessed 13 January 2022.
[37] JCEUA 1 December 2021.

Appendix I: Committee Terms of Reference

(1) Go gceapfar Roghchoiste, dá ngairfear an Roghchoiste um Ghnóthaí Eorpacha, ar a mbeidh 9 gcomhalta de Dháil Éireann, chun breithniú a dhéanamh ar cibé nithe a éiríonn—

(*a*) as ballraíocht na hÉireann san Aontas Eorpach, agus

(*b*) as Éirinn do chloí leis an gConradh ar an Aontas Eorpach agus leis an gConradh ar Fheidhmiú an Aontais Eorpaigh,

a roghnóidh sé agus nach bhfuil tarchurtha chuig aon Choiste eile.

(2) Gan dochar do ghinearáltacht mhír (1), breithneoidh an Roghchoiste—

(*a*) cibé Billí a bpléann an Roinn Gnóthaí Eachtracha agus an Roinn Cosanta leis an dlí reachtach ina leith,

(*b*) cibé tograí a bheidh in aon tairiscint, lena n-áirítear aon tairiscint de réir bhrí Bhuan-Ordú 220, agus

(*c*) cibé nithe eile,

a tharchuirfidh an Dáil chuige.

(1) That a Select Committee, which shall be called the Select Committee on European Union Affairs, consisting of 9 members of Dáil Éireann, be appointed to consider such matters arising from—

(*a*) Ireland's membership of the European Union, and

(*b*) Ireland's adherence to the Treaty on European Union and the Treaty on the Functioning of the European Union,

as it may select and which are not referred to any other Committee.

(2) Without prejudice to the generality of paragraph (1), the Select Committee shall consider such—

(*a*) Bills the statute law in respect of which is dealt with by the Department of Foreign Affairs and the Department of Defence,

(*b*) proposals contained in any motion, including any motion within the meaning of Standing Order 220, and

(*c*) other matters,

as shall be referred to it by the Dáil.

(3) Beidh an tAire Gnóthaí Eachtracha (nó comhalta den Rialtas nó Aire Stáit a ainmneofar chun gníomhú ina áit nó ina háit chun na críche sin), ina chomhalta nó ina comhalta *ex officio* den Roghchoiste chun na nithe atá leagtha amach i mír (2)(a) agus (b) a bhreithniú agus beidh sé nó sí i dteideal vótáil in imeachtaí an Roghchoiste.

(3) The Minister for Foreign Affairs (or a member of the Government or Minister of State nominated to act in his or her stead for that purpose) shall be an *ex officio* member of the Select Committee for the purpose of consideration of the matters outlined at paragraph (2)(*a*) and (*b*) and shall be entitled to vote in Select Committee proceedings.

(4) Beidh ag an Roghchoiste na cumhachtaí a mhínítear i mBuan-Ordú 96, seachas míreanna (6) go (10).

(4) The Select Committee shall have the powers defined in Standing Order 96, other than paragraphs (6) to (10).

(5) Déanfar an Roghchoiste a chomhcheangal le Roghchoiste arna cheapadh ag Seanad Éireann chun bheith ina Chomhchoiste um Ghnóthaí Eorpacha, agus, gan dochar do ghinearáltacht mhír (1), déanfaidh an Roghchoiste an méid seo a leanas a bhreithniú—

(5) The Select Committee shall be joined with a Select Committee appointed by Seanad Éireann, to form the Joint Committee on European Union Affairs, which, without prejudice to the generality of paragraph (1), shall consider—

(*a*) doiciméid phleanála straitéiseacha an Choimisiúin Eorpaigh lena n-áirítear Clár Oibre an Choimisiúin,

(*a*) the European Commission's strategic planning documents including the Commission Work Programme,

(*b*) forbairtí beartais tras-earnála ag leibhéal an Aontais Eorpaigh,

(*b*) cross-sectoral policy developments at European Union level,

(*c*) nithe a liostaítear lena mbreithniú ar an gclár gnó i gcomhair cruinnithe de Chomhairle (Airí) Gnóthaí Ginearálta an Aontais Eorpaigh agus toradh cruinnithe den sórt sin.

(*c*) matters listed for consideration on the agenda for meetings of the General Affairs Council (of Ministers) of the European Union and the outcome of such meetings,

(*d*) cibé rialacháin faoi Achtanna na gComhphobal Eorpach, 1972 go 2009 agus ionstraimí eile arna ndéanamh faoi reacht agus is gá de dhroim na n-oibleagáidí a ghabhann le ballraíocht san

(*d*) such regulations under the European Communities Acts 1972 to 2009 and other instruments made under statute and necessitated by the obligations of membership of

Aontas Eorpach a roghnóidh an Coiste,

the European Union as the Committee may select,

(*e*) fógraí arna dtarchur ag an Dáil faoi Bhuan-Ordú 134(1)(*a*),

(*e*) notifications referred by the Dáil under Standing Order 134(1)(*a*),

(*f*) fógraí i dtaobh tograí chun na Conarthaí a fuarthas ón gComhairle Eorpach de bhun Airteagal 48.2 den Chonradh ar an Aontas Eorpach a leasú,

(*f*) notifications of proposals for the amendment of the Treaties received from the European Council pursuant to Article 48.2 of the Treaty on European Union,

(*g*) fógraí i dtaobh iarratais ar bhallraíocht san Aontas Eorpach a fuarthas ón gComhairle Eorpach de bhun Airteagal 49 den Chonradh ar an Aontas Eorpach, agus

(*g*) notifications of applications for membership of the European Union received from the European Council pursuant to Article 49 of the Treaty on European Union, and

(*h*) cibé nithe eile a tharchuirfidh an Dáil chuige ó am go ham.

(*h*) such other matters as may be referred to it by the Dáil from time to time.

(6) Tabharfaidh an Comhchoiste tuarascáil do dhá Theach an Oireachtais ar oibriú Acht an Aontais Eorpaigh (Grinnscrúdú), 2002.

(6) The Joint Committee shall report to both Houses of the Oireachtas on the operation of the European Union (Scrutiny) Act 2002.

(7) Beidh ag an gComhchoiste na cumhachtaí a mhínítear i mBuan-Ordú 96, 133 agus 135 agus beidh aige an chumhacht chun moltaí a chur faoi bhráid an Aire Gnóthaí Eachtracha (nó faoi bhráid Aire Stáit) i dtaobh nithe a bhaineann leis an Aontas Eorpach.

(7) The Joint Committee shall have the powers defined in Standing Order 96, 133 and 135 and shall have the power to make recommendations to the Minister for Foreign Affairs (or Minister of State) on European Union matters.

(8) Féadfaidh na daoine seo a leanas freastal ar chruinnithe den Chomhchoiste agus páirt a ghlacadh in imeachtaí gan ceart vótála a bheith

(8) The following may attend meetings of the Joint Committee and take part in proceedings without having a

acu ná ceart tairiscintí a dhéanamh ná leasuithe a thairiscint:

right to vote or to move motions and amendments:

(*a*) Comhaltaí de Pharlaimint na hEorpa arna dtoghadh ó thoghcheantair in Éirinn,

(*a*) Members of the European Parliament elected from constituencies in Ireland,

(*b*) Comhaltaí de thoscaireacht na hÉireann chuig Tionól Parlaiminteach Chomhairle na hEorpa, agus

(*b*) Members of the Irish delegation to the Parliamentary Assembly of the Council of Europe, and

(*c*) ar chuireadh a fháil ón gCoiste, Comhaltaí eile de Pharlaimint na hEorpa.

(*c*) at the invitation of the Committee, other Members of the European Parliament.

(9) Déanfaidh an Comhchoiste ionadaíocht do dhá Theach an Oireachtais ag Comhdháil na gCoistí um Ghnóthaí Comhphobail agus Eorpacha de chuid Pharlaimintí an Aontais Eorpaigh (COSAC) agus tabharfaidh sé tuarascáil ar an gcéanna do dhá Theach an Oireachtais.

(9) The Joint Committee shall represent both Houses of the Oireachtas at the Conference of Community and European Affairs Committees of Parliaments of the European Union (COSAC) and shall report to both Houses of the Oireachtas thereon.

(10) Beidh Cathaoirleach Roghchoiste na Dála ina Chathaoirleach nó ina Cathaoirleach ar an gComhchoiste freisin.

(10) The Chairman of the Dáil Select Committee shall also be the Chairman of the Joint Committee.

Appendix II: List of Meetings Held

Date & Link to Transcript	Witnesses
3rd November 2021	Ms Lorena Boix Alosno, Director for Cybersecurity, DG Connect Mr Ciarán Cuffe MEP
24th November 2021	Mr Olli Ruutu, Deputy Chief Executive of European Defence Agency Mr Wolfgang Roehrig, European Defence Agency
1st December 2021	Mr Juhan Lepassaar, Chief Executive of European Union Agency for Cybersecurity (ENISA) Mr Ossian Smyth, Minister of State with responsibility for Public Procurement and eGovernment, Minister of State with responsibility for Communications and Circular Economy

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000 or 076 1001700
Twitter: @OireachtasNews

Connect with us

Download our App

Download on the App Store

GET IT ON Google Play