DÁIL ÉIREANN

AN COMHCHOISTE UM DHLÍ AGUS CEART, GNÓTHAÍ BAILE AGUS IMIRCE

JOINT COMMITTEE ON JUSTICE, HOME AFFAIRS AND MIGRATION

Dé Máirt, 25 Samhain 2025

Tuesday, 25 November 2025

Tháinig an Comhchoiste le chéile ag 3 p.m.

The Joint Committee met at 3 p.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	**Seanadóirí / Senators**
Tom Brabazon,	Robbie Gallagher,
Michael Cahill,	Garret Kelleher,
Catherine Callaghan,	Michael McDowell,
Gary Gannon,	Anne Rabbitte,
Mark Ward.	Lynn Ruane.

Teachta / Deputy Matt Carthy sa Chathaoir / in the Chair.

General Scheme of the National Cyber Security Bill 2024: Discussion

An Cathaoirleach: No apologies have been received. I remind members and witnesses to switch off their mobile phones.

The purpose of today's meeting is to engage with a number of stakeholders as part of the committee's scrutiny of the general scheme of the national cybersecurity Bill 2024. I welcome the following witnesses: Mr. Barry Walsh, detective chief superintendent and Mr. Pat Ryan, detective superintendent from the Garda National Cyber Crime Bureau; Mr. Sean McElligott, partner at Philip Lee LLP; Dr. T.J. McIntyre, chair of Digital Rights Ireland; Ms Olga Cronin, senior policy officer at the Irish Council for Civil Liberties; and Mr. Erik O'Donovan, head of digital economy policy, and Ms Áine Clarke, digital and AI policy executive from IBEC. Also attending as observers are officials from the Department of Justice, Home Affairs and Migration. They are here to assist the committee if any clarification on the general scheme is required. I welcome Mr. David McGill, principal officer, and Ms Clare Heenan, assistant principal officer. The witnesses are all very welcome.

Before I invite witnesses to deliver their opening statements, I wish to advise them of the following in relation to parliamentary privilege. Witnesses and members are reminded of the long-standing parliamentary practice that they should not criticise or make charges against any person or entity by name or in such a way as to make him, her or it identifiable or otherwise engage in speech that might be regarded as damaging to the good name of the person or entity. Therefore, if their statements are potentially defamatory in relation to an identifiable person or entity, they will be directed to discontinue their remarks. It is imperative that they comply with any such direction.

The format of the meeting will be that I will invite each organisation in turn to make an opening statement of a maximum of three minutes. When all the opening statements have been delivered, I will call members of the committee in the order in which they indicate to put any questions. As always, the committee will operate a rota system. I will give each member seven minutes to engage with the witnesses. If members stick to that, we will have an opportunity for a second round and, perhaps, subsequent interactions.

I invite Mr. Walsh to deliver his opening statement.

Mr. Barry Walsh: I thank the Cathaoirleach and committee members for the invitation to discuss the general scheme of the national cyber security Bill and for the previous invitation to make submissions in respect of it, which was much appreciated.

As a result of our responsibility to investigate cybercrime after it has occurred, An Garda Síochána gets a clear view of the harm caused by cybercrime and the personal impacts that result. Unfortunately, many result from deficiencies in cyber-hygiene practices, even at the most basic level of employee awareness concerning phishing or social engineering. Having regard to the above, the beneficial impacts of the network and information security directive and its transposition into Irish law by means of the proposed national cyber security Bill 2024 are most welcome as mechanisms to create a more secure cyber ecosystem.

In this jurisdiction, the Garda National Cyber Crime Bureau and the National Cyber Security Centre maintain a productive working relationship. The agencies are frequent collaborators and support each other’s respective roles, particularly in the area of cybercrime prevention. By

way of general overview, the cybercrime economy is frequently cited as being the fastest growing in the world. It is estimated that it will be worth just over €9 trillion by the end of the year, up from an estimated €5.5 trillion in 2020. There is little doubt that the cybercrime economy is now an economy of scale and one that is generating immense wealth for those who benefit from it, while causing immense harm to victims.

Despite representing a smaller proportion of the cybercrime economy in terms of financial output, it is my respectful assertion that cyber-dependent crimes, which are offences that can only be committed using a computer, represent the greatest threat of societal level disruptions. Within this category, ransomware, which is a type of malware that encrypts the victim's personal data until a ransom is paid, represents the most significant threat. To support this assertion, I point to the impacts of the largest such attack in Ireland, which was on the HSE in 2021, and, more recently, the disruption to flights in a number of countries, including Ireland, due to an attack on an airline services provider. There was also an attack on operations of a major retailer in Ireland and the UK and the negative impact on the UK's recent GDP figure was attributed to ransomware disrupting the operations of a vehicle manufacturer. These examples display the disruptive impacts and potential for cross-societal harm created by the perpetrators of cyber-dependent crime. In addition, the dynamic in respect of those perpetrating cyber-dependent crimes is becoming increasingly complex. Criminal groupings have become highly organised, employing specialists and sourcing ransomware toolkits as a service. There is evidence of nation-state involvement in cybercriminality. There is access to ever increasing computational power, network capacity and new technologies, such as artificial intelligence, all of which extend reach and create enhanced capacity to deceive.

The net outcome is that cybercriminality in all its forms represents a clear and present danger to the normal functioning of the many services we, as a society, have come to rely upon. It is also very apparent that there is an absolute necessity for all those who operate within this ecosystem, particularly as service providers, to maintain a proactive, resilient, cybersecurity posture to support effective operations. In this context, this Bill is viewed as an important legislative development.

An Cathaoirleach: I now invite Mr. McElligott to make his opening statement.

Mr. Sean McElligott: I thank the Cathaoirleach and members of the committee for the opportunity to speak this evening. I am a partner and head of the technology practice in Philip Lee LLP. Although I am a solicitor, I have a degree in electronic engineering from UCD and before having an early life crisis and deciding to become a solicitor, I worked for 13 years in IT for, among others, Bank of Ireland Treasury and Motorola. The focus of my legal practice is therefore on all things technology related.

The heads of the Bill represent an important and timely step towards transposing the NIS2 directive and placing the National Cyber Security Centre on a clear statutory footing. Stakeholders welcome the Bill's aims of strengthening resilience, improving incident response and deepening information sharing. The emerging EU implementing measures are already adding helpful specificity to concepts such as what constitutes a significant incident, and further ministerial guidance will support a coherent regime.

My observations are focused on the breadth and subjectivity of head 3(1)(d). As drafted, it would allow the regulator to deny the use of network and information systems on grounds that

include being detrimental to the interests of the State, being clandestine or deceptive, or involving a threat to any person, device or essential service. To be clear - and it is important to note that this power does not appear in the NIS2 directive - without objective criteria, clear thresholds and procedural safeguards, it risks arbitrary or inconsistent application. In short, a wellintentioned tool could become a blunt instrument with unforeseen consequences. The practical risks are significant. It goes without saying, that modern networks underpin hospitals, electricity grids, transport systems and so on. A sweeping denial of access, even if intended to address a discrete issue, could inadvertently cascade into outages of essential services with consequences for public safety and economic stability. For example, locking hospital staff out of critical patient records, forcing blackouts when grid operators lose visibility and control, or halting railway traffic due to compromised signalling systems.

In addition, there is an internal inconsistency in safeguards across the Bill. The temporary deployment of sensors on communications networks under head 9 is an intrusive but contained power that requires prior High Court authorisation. Yet, the power to deny network access altogether could be exercised unilaterally, and the supervision and enforcement framework appears not to apply to it. Surely, if deploying a sensor calls for judicial scrutiny, the effective disconnection of an operator cannot require less scrutiny.

For these reasons, I suggest that consideration should be given to either removing head 3(1)(d) altogether or, if the Oireachtas considers that a denial power is indispensable for truly exceptional cases, it should be tightly constrained by law, at the very least akin to the measures envisaged under head 9. Any such measure should be grounded in published, objective criteria that are tied to a clear, imminent and demonstrable threat; preceded by written notice with a fair opportunity to respond and remedy; strictly limited in scope and time with transparent review and lifting conditions; subject to prior independent authorisation or, failing that, to a robust, rapid appeal mechanism; and explicitly brought within the Bill's supervision and enforcement provisions. In this way, explicit protections would ensure that actions taken under the Bill do not inadvertently disrupt essential services.

I will make two further quick points because I am conscious of time. When addressing cybersecurity, priority should be given to technical measures, standards and internationally recognised certifications. Non-technical or subjective factors should not influence cybersecurity outcomes.

The NIS2 directive's shift away from pure organisational and non-technical approaches towards mandatory technical standards is sensible. The NCSC's proposal to adopt the CyFun framework provides a structured, risk-based method for assessing maturity and preparing organisations for NIS2. Although CyFun does not guarantee compliance, it offers a credible basis for demonstrating technical capability. In addition, there is a growing consensus that ISO 27001 certification should be the foundation for achieving and evidencing NIS2 compliance. Its alignment with NIS2 has already led to formal recognition in several member states, including Belgium, where ISO 27001 is explicitly accepted as proof that "essential" and "important" entities meet NIS2 cybersecurity requirements.

Second, a grace period of six to 12 months after commencement would support orderly implementation across both regulated entities and competent authorities, much as a transition period did for GDPR.

This is a strong Bill whose core architecture is widely supported. By removing, or decisively limiting, the application of head 3(1)(d), and by providing a measured transition and sustained transparency and engagement, the committee can assist with the delivery of a regime that is both resilient and proportionate.

An Cathaoirleach: I thank Mr. McElligott. Next is a joint presentation from Digital Rights Ireland and the Irish Council for Civil Liberties. I call Dr. McIntyre.

Dr. T.J. McIntyre: We are very grateful to the committee for the opportunity to discuss some concerns we have with the Bill. We see the Bill as an important step forward in transposing the directive. It is important, however, to avoid compromising cybersecurity in so doing. We see five aspects of the Bill in particular that give rise for concern. There is a degree of overlap with Mr. McElligott's concerns but we have certain further concerns. However, as with his concerns, these are about aspects of the Bill which are purely domestic, that is, they are not required by the directive, that is, they are not required for its transposition. Rather, they are domestic innovations and they can be parked without affecting transposition and our deadline.

The first aspect I would like to flag is head 6, which gives the NCSC power to scan networks for vulnerabilities. The directive requires this only in the context of networks of essential and important entities. This, however, goes well beyond that. It permits scanning without consent of networks of small businesses, NGOs, homes or politicians offices without any justification being given in the explanatory note for this power being extended in this way.

The second aspect is head 7. This overlaps significantly with Mr. McElligott's concerns about the power in head 3(1)(d). Head 6 is, in fact, the way in which the power in head 3(1)(d) would largely be given effect. This creates Internet-blocking powers for the NCSC which would allow it to block access to websites, IP addresses or, possibly, more generally. It is extremely wide, with the powers being unclear in their details and with very limited procedural safeguards. We have set out in our submission the minimal procedural safeguards that are required by the European Convention on Human Rights on this part and we say the head requires substantial revision if it is to be compliant with those safeguards.

Head 8 provides for two new entirely unprecedented powers. The first is to scan and store the entirety of the network traffic in public sector bodies. This could include the contents of sensitive emails within those bodies. They could be emails containing patient health data, emails to and from legal advisers and they could even be the communications of politicians. Second, it would allow the NCSC to do likewise in the sense that it could collect metadata about private communications on public networks, such as mobile phone and home broadband providers and messages sent via social media providers. This information could be stored by them for up to 18 months. Both of these powers could be used without the consent of any of the individuals affected. We say that this is clearly in breach of European Court of Justice jurisprudence, including our own judgment in the Digital Rights Ireland case in 2014 regarding bulk surveillance of communications.

We have a further concern about head 9, which allows for collection of metadata about communications in a similar way, that is, an undifferentiated bulk way, but in this case on a compulsory basis. The previous head, head 8, would only allow for collection of communication data with the consent of the body concerned, not the individual concerned. This, however, would allow the NCSC to compel providers, such as mobile phone operators,

other network providers and data centre operators, to allow it to install equipment on their devices that could collect information about communications about every individual user of the service - this includes services such as WhatsApp and iMessage - for an extended period of time without any individualised justification. This would be done on the basis of national security grounds but notably "national security" is not defined anywhere in the heads of Bill. The concerns we have about these earlier powers are somewhat compounded by the power of the NCSC to share data. Head 10, in particular, is of concern here because it creates a largely open-ended power on the part of the NCSC to share data, including for national security reasons – again, undefined – but without any clear limits on that power.

We thank the committee for its time. We would be very happy to address any questions members may have.

An Cathaoirleach: I thank Dr. McIntyre. Finally, I call Mr. O'Donovan from IBEC.

Mr. Erik O'Donovan: I thank the committee for the invitation to appear today on behalf of IBEC, the group that represents Irish business. I am joined by my colleague Ms Áine Clarke. We are both from IBEC's digital policy team.

In October 2024, we made a submission on the general scheme of the national cybersecurity Bill, which has been shared with the committee. We welcomed the publication of the general scheme as a vital step in transposing the NIS2 directive. NIS2 is an update of the first Network and Information Security, NIS, Directive, which was the first European Union-wide cybersecurity law. NIS2 will introduce much stricter requirements, covering many more organisations and sectors. This reflects the changing world around us, where we see increasingly frequent and sophisticated cyberattacks, with cybersecurity and resilience growing in importance.

Cybersecurity is an economic and social imperative and an opportunity for Ireland, particularly given the amount of EU data we host here - over 30% according to the National Cyber Security Centre. It is fundamental to safeguarding trust in our digitalised economy and protecting our critical infrastructure. This Bill is not just an opportunity to lift the national baseline for cybersecurity; getting this right is an opportunity for Ireland to enhance our competitiveness and resilience, for the benefit of Irish society.

The impact of NIS2 on Irish business will be significant. Fewer than 150 organisations were in scope of the first NIS directive. It is estimated that over 4,500 organisations will be directly in scope of NIS2, with many more indirectly affected by the requirements on in-scope organisations to manage the cybersecurity of their supply chains. For many of these businesses, NIS2 will mark a step change in how cybersecurity is treated within the organisation. It is no longer just an IT issue but a board level concern.

To ensure its success, we believe the Bill must be considered within the broader context of cybersecurity in Ireland. IBEC wishes to focus on four important areas, namely, skills; developing our cyber industry; supporting business adoption; and related issues in the general scheme.

First, on the cybersecurity skills challenge, a lack of cybersecurity readiness, particularly among SMEs, directly impacts the ability of businesses to understand and comply with their regulatory obligations. According to Eurostat, almost one in four companies in Ireland has

reported difficulties recruiting staff with the necessary cybersecurity skills. At the moment, we simply do not have enough skilled professionals to meet the surge in demand the national cybersecurity Bill will create. We implore the committee and the Government to consider directing some of the €2 billion surplus of the National Training Fund towards cybersecurity and other digital skills.

The skills question also extends to regulators. IBEC strongly supports the continued expansion and resourcing of the National Cyber Security Centre. However, the Bill also designates sectoral regulators, many of which will be supervising cybersecurity for the first time. It is critical that these bodies are sufficiently resourced, not just with funding but with the technical experts needed to provide guidance to businesses.

Second, the increase in cyber regulation in the EU, including NIS2, presents a significant opportunity for the growth of our cybersecurity sector, as more regulated entities will mean more demand for cybersecurity products and services. Our cybersecurity sector is already a major contributor to the economy, comprising over 500 firms and generating €2.7 billion in annual revenue. NIS2 can solidify Ireland's position as a leading digital regulatory hub, which is a programme for Government goal. However, it will require greater prioritisation and investment in cybersecurity by Government, particularly in research and development. We urge the Government to deliver on its programme for Government commitment to establish a dedicated, brick-and-mortar centre of excellence for cybersecurity for the development of our cyber industry.

Third, we believe there is an urgent need to support business adoption. NIS2 requirements are far-reaching and organisations will face significant new compliance costs, including but not limited to security audits, technology upgrades and essential training for staff. We welcome the SME cyber improvement grants that have been offered by the NCSC to date and call for additional dedicated and accessible streams of grants and vouchers to help organisations to increase their cyber resilience.

Lastly, I would like to raise several issues we mention in our submission.

In transposing NIS2 into Irish law, we should align with the EU text and avoid gold-plating for coherence and certainty. Any costs levied on organisations should also be proportionate and take into account the financial cost of complying with the law. Many important details necessary for complying with NIS2 have been omitted from the general scheme and further guidance will certainly be needed on areas such as supply chain and the interplay between NIS2 and other laws. As we await the enactment of the Bill, resources like the cyber fundamentals certification scheme and the ISO 27001 standard are very important for business in plugging the gap. It is important that these standards be technical and non-discriminatory, meaning that they are based purely on objective criteria, such as performance, functionality and security outcomes. They should also apply equally to all vendors or market participants. This concept is the bedrock of global digital trade.

In conclusion, we would like to stress from the outset that IBEC supports the broad aim of NIS2 to raise the common level of cybersecurity across the EU. However, we are more than a year on from the transposition deadline and businesses lack clarity on their regulatory obligations. We therefore urge the Government to commit all resources necessary to enact the Bill as quickly as possible to provide certainty for businesses and regulators alike.

We look forward to working with the committee and other stakeholders to increase Ireland's cybersecurity and resilience.

An Cathaoirleach: I thank Mr. O'Donovan. If members wish to indicate, we will open for interactions with seven minutes each. I call Senator Kelleher.

Senator Garret Kelleher: I thank the witnesses for the interesting presentations. I would like to focus initially on something Mr. Walsh said that related to the evidence of nation state involvement in cybersecurity or related issues. Will he tell us more about that?

Mr. Barry Walsh: What we are seeing on the global domain is particular countries - I suppose it is best not to name them - that are involved in various types of warfare. They are countries that are in some way excluded from the normal global ecosystem, employing cyberwarfare and cyberattacks as a mechanism both to generate income and to disrupt nation state services.

Senator Garret Kelleher: I thank Mr. Walsh for the sensitive nature in which he replied. I would also like to know more about the extent to which there is collaboration with international partners in the area, particularly fellow EU member states.

Mr. Barry Walsh: From our perspective, there is extensive collaboration. As the cyber ecosystem has expanded and evolved, Europol services and the range of services it provides have also expanded and evolved. We are an active participant in a lot of Europol activities. We have a presence in all the meetings Europol has in this area. Up until recently, a member of our team was the president of the EU cybercrime task force. Only last week, I was over at the Interpol working group meeting on cybercrime, which is the European working group on cybercrime. Last month, I attended the global counter-ransomware initiative with other government agencies. It is a global issue and requires a lot of partnership to address it because a lot of the offenders are resident in various areas outside of this State. It is important we have that collaboration.

An Cathaoirleach: Just before Senator Kelleher comes back in, there is a vote in the Dáil. Will one of the Senators take the Chair so the discussion can continue?

Senator Lynn Ruane took the Chair.

Senator Garret Kelleher: Will Mr. McElligott expand on what is proposed in head 3(1)(d) and his reference to how it conflicts or is not entirely in line with what is set out in the NIS2 directive?

Mr. Sean McElligott: To be clear, head 3 is not contained in any sense under NIS2. However, it is there to put the NCSC on a statutory footing. That is the aim behind this particular part of the Bill. Speaking as a lawyer, the power under head 3(1)(d) jumps off the page. It seems to say that the NCSC has the power to do whatever it wants to whomever it wants whenever it wants without any regulatory supervision whatsoever. It is a very strange part. The wording is, "deny the use of network and information systems". Someone can be unplugged from the Irish system. At the end, it states, "or involve a threat to any person, device or essential service." It is extremely broad. This is an early draft of the legislation. I have no doubt that this drafting will be looked at but as a lawyer, it jumps off the page. If Amazon, for example, is subjected to a very serious hack, is the NCSC proposing it would disconnect Amazon from the Irish network? This head appears to give it that power. We are all aware of

what happened with Amazon recently when it dropped off for some particular technical reason. There was chaos. I have public and private sector clients looking to put stuff on a cloud. They want to put their services on a cloud and they ask if this will mean the NCSC could for some particular reason take down that cloud.

Senator Garret Kelleher: On a related matter, Dr. McIntyre made reference to the ambiguity in the lack of definition of "national security" in what is proposed. That ties in with what Mr. McElligott said. Will Dr. McIntyre elaborate on that?

Dr. T.J. McIntyre: This is a common problem across Irish legislation. We do not have a general definition of "national security" anywhere in Irish law. That means there are very far-reaching powers that are largely open-ended and are only circumscribed by national security. "National security" is not a defined term in this context and these powers are in effect left to the discretion of the Minister for justice, not even the NCSC, because it must act in accordance with the directions of the Minister. That leaves us with a very open-ended power to order surveillance of the communications of every person in the State on the basis of this undefined concern about national security without any specific provisions regarding the proportionality or necessity of doing this. To give a concrete example of how open-ended it is, picking up on Mr. McElligott's point, head 3(1)(d) would allow the NCSE to block access to X, formerly Twitter, in Ireland if it was of the view individuals were using it to stir up racism, hatred and attacks on migrants in Ireland. While I personally would not be sad to see access to X gone in Ireland, it strikes me that is not an appropriate power to be here without appropriate oversight and safeguards.

An Cathaoirleach Gníomhach (Senator Lynn Ruane): We cut into the Senator's time, so if he has another question, he is welcome to ask it.

Senator Garret Kelleher: I am happy, thank you.

Senator Anne Rabbitte: An interesting array of people are sitting in front us with different viewpoints. At this stage, I would love to involve the Department to talk to the point. I am after hearing two different viewpoints in relation to 3(1)(d). What is the train of thought within the Department, if it does not mind sharing that with us and giving us an understanding?

Mr. David McGill: As Mr. McElligott rightly pointed out, head 3 is very much about putting the National Cyber Security Centre on a statutory footing. It is very much a national provision; it is not something derived from the directive, although some of its functions are. This particular one is a function as opposed to a power. We do not envisage that it will ever be used to just unilaterally compel anybody to disconnect somebody from a network.

If it went in to try to do that, it would not be able to compel them. There are no compulsion powers. The powers can be used after the fact. Head 8 and head 7 allow the NCSC to apply certain powers for certain, specific reasons, some of which is definitely overseen by the courts. In that context, its function is very much to try to deny them the use of these networks but the powers come after the fact.

Senator Anne Rabbitte: I thank Mr. McGill. To go back to Mr. McElligott, having heard that it is a function as opposed to a power, what is his take on that?

Mr. Sean McElligott: I do not want to split hairs between functions and powers but when you read the cold words on the page, it certainly seems to suggest scope for invocation if the

NCSC had a particular view that something was happening. It does not even use the phrase "national security" under this head. As there is no reference to national security, this is not national security related; it is something else. My reading of it is if it so decided, it could look to invoke this particular provision. Speaking as a lawyer, I suspect it would be challenged, to be honest, if someone tried to do something on the basis of this.

Senator Anne Rabbitte: What are Dr. McIntyre's thoughts?

Dr. T.J. McIntyre: I agree with Mr. McElligott's analysis. In fact, I would go a little bit further and point out that under head 7, which I can see as being the head used to apply this function, there is the power to impose an Internet death penalty, as we refer to it, on websites, services, IP addresses and other things on the Internet without a court order. That is a critical point. It could be done without a court order, without provision for independent oversight of the imposition of the Internet death penalty and without a clear appeals mechanism in place against the imposition of an Internet death penalty.

Senator Anne Rabbitte: I will go back to Mr. Walsh. I will leave business until the end. In his opening submission, he said cybercrime is the most significant threat we face. He is probably privy to an awful lot more information than any of us here around the table because he probably has a helicopter view of exactly what is going on and he also sees the damage it is doing on the ground. Let us park the idea of the HSE, make it more local and bring it down to the business-level of the high street, whether it is Shop Street in Galway or one of our medtechs in the city. Could Mr. Walsh bring it to that level for the general public to understand why this Bill is so important in getting this law brought through?

Mr. Barry Walsh: We always look at the harm cyberattacks cause. I say this frequently. People look at cybercrime as a distant reality that never impacts them but you see it when you go to the scene of a small or medium enterprise that has been impacted by a cybercrime - this is just a ransomware type attack, not to mention those who have their life savings taken. People are increasingly living their lives online. The reality is that people will have all their functions in an online space, potentially not properly protected.

We see the utter fear and chaos that follows a cyberattack. Somebody comes in and it is essentially ground zero for them in terms of their capacity to run their business. You look at billing, all of their financials and the ordering process. Everything is online and is impacted by this system being taken offline. It causes real harm and it is real people who are impacted. At a very local level, that is the reality of cybercrime.

Senator Anne Rabbitte: Mr O'Donovan has spoken about how it is a year from when this Bill can be enacted but at the same time, I hear he is saying - he can correct me if I am hearing him incorrectly - there is not enough focus or there are not enough supports to step up and make the gear change that would be required for businesses. Whether one head of a Bill is in it or not in it or there is an understanding of it, either way, the legislation is coming. Where are the businesses on the ground? What is IBEC's policy?

Mr. Erik O'Donovan: As we said in our opening statement, we feel that a lack of cybersecurity readiness, especially for SMEs, is a concern. One quarter of companies are finding it difficult to find skilled staff. To put it n context, if there were fewer than 150 organisations covered by the first NIS and it has now gone up to 4,500, that is a 30-fold increase. There will be 4,350 more companies covered in scope now. They will have to put in

technical measures. There will have to be training involved. There are some schemes that already exist but again, they are for Enterprise Ireland clients and this will see a broader cohort involved.

There are some grants there already and we welcome that. Today, we are calling out that we will need to increase that. When I say that number of 4,500 companies, it is actually greater than that because we must remember some companies have to manage the indirect supply chain. That will bring in SMEs and so on. There will be increased demand for training. We feel the National Training Fund, to which our members have contributed, has €2 billion and is being unlocked but we need signals to say it is being unlocked and part of it will be directed towards digital and cyber skills, especially in this case. It is a case of NIS2 directing demand and businesses asking for a bit of support on the supply side.

It is certainly an imperative but it is also an opportunity for us to grow the supply side and the capacities on our supply side, such as in our indigenous cybersecurity sector. The resource we are calling for with that is an investment in a bricks and mortar centre of excellence that would be a research and development facility.

Deputy Gary Gannon: I thank the witnesses for coming in and contributing. Most of my questions are probably for the Department, following on from its submission. From the Department's perspective or from any of the contributors, is Ireland now an outlier in Europe? Can the Department point to any other EU member state that has introduced a power equivalent to head 3(1)(d) allowing the NCSC to deny the use of networking information systems in the State? Are we now alone in the Union in taking this approach?

Deputy Matt Carthy resumed the Chair.

Mr. David McGill: I am not sure if Deputy Gannon was here when I was explaining this but we view this as a function as opposed to a power. On the function of the NCSC, while it derives some of its functions from the NIS2 directive, some of it is just from a national point of view and we want it to protect and look after our networks from foreign interference. Our powers are the powers that come afterwards in heads 6, 7 and 8, which allow it to carry out its functions. I cannot actually speak to other countries on this matter. I would have to take that away and come back to the Deputy on that.

Deputy Gary Gannon: Okay. If Mr. McGill could come back with further detail, that would be great. In relation to the absence of independent or judicial control, why would the Bill grant the NCSC such broad powers in heads 3, 6, 7, 8 and 9, without any requirement for judicial oversight, independent authorisation or even prior notice to the entities or individuals affected?

Mr. David McGill: Under head 9, there is actually judicial control. For head 9, you have to apply for it to work and it involves judicial oversight. Head 9 is under judicial control and head 8 is done on consent. It is done to the extent which is necessary for the protection of the particular networks of the operators and the public bodies themselves. Just to be aware, this whole general scheme will come under the examination of the Office of the Independent Examiner of Security Legislation. The idea is that this is security legislation and, therefore, there should be that independent oversight over the entire operation of this legislation.

Deputy Gary Gannon: Given the concerns that have been raised by Digital Rights Ireland and the ICCL in their submissions about the bulk data collection, the domain block and the

installation of surveillance systems, can the Department state clearly how these provisions have been assessed for compliance with EU data protection law and the recent CJEU rulings?

Mr. David McGill: This Bill only provides for interception of data and it is on the networks and information systems of their actual networks to make sure they are not under threat. When it comes to the oversight piece, we have submitted the general scheme to the Data Protection Commission for its views and we are still waiting for that to come back.

Deputy Gary Gannon: I am conscious that, as we are speaking and going through this Bill here today, there is also the EU review of the Cybersecurity Act. Will that review have implications for the Bill we are discussing today?

Mr. David McGill: I will be very honest, in that we are still waiting for the review to be published, so we have not seen a full copy of it. Our only anticipation regarding it relates to functions particularly assigned to the NCSC to act as a certification authority. That is the only one we would have a notification for.

Deputy Gary Gannon: We are doing this Bill while we are conscious that there will be a very substantial review from the EU that may impact the work we are doing.

Mr. David McGill: No. The Cybersecurity Act that the EU is reviewing is a very different directive to this one. The Cybersecurity Act is very much around certification schemes. It is about the functioning of those certification schemes at an EU level and how they operate. We envisage that the NCSC will be operating as our certification authority for Irish purposes but that will just be a function and there will not necessarily be any delegated powers to give to the NCSC.

Deputy Gary Gannon: Overlapping all of my questions has been the word "function". How does Mr. McGill interpret "function" as opposed to "power"?

Mr. David McGill: From our point of view, a function is if a body has the duty to carry out certain activities, for example, to act as a certification scheme. That is then executed through powers. In this particular case, if a body's function is to act as a national competent authority in the Bill, it has explicit powers to conduct inspection, demand information and apply for search warrants. They are the ones derived in order to carry out the duties or functions.

An Cathaoirleach: I thank Senator Ruane for taking the Chair. She now has an opportunity to contribute.

Senator Lynn Ruane: If we have time at the end, I might come back to the difference between function and power, because I would see responsibilities, duties and powers all deriving from function, so I am still not clear on the difference between the two, and effectively they are the same. I might come back to that at the end because we could probably get stuck on it.

When I read the submissions from Mr. McElligott, Dr. McIntyre and Ms Cronin, the fear that comes up in me is that there is a kind of policy creep or something is happening that has little to do with cybersecurity and more to do with a wider surveillance that covers more than just cybersecurity vulnerabilities and threats. Do the witnesses see that as the crux of the problem? Could this Bill be used to get particular data or access to WhatsApp or iMessages, which could then be used in other ways that were outside the remit of this Bill?

Mr. Sean McElligott: I agree. Obviously, this is an early draft of the Bill and I am sure it is going to be amended and reviewed. The Senator mentioned policy creep. As a lawyer, I certainly see that phrase as being very applicable to this situation. There are powers and functions - I do not want to split hairs - that, as a lawyer, jump off the page as being extremely broad and would allow somebody to do basically whatever they wanted whenever they wanted to whomever they wanted. I do not think that would work in practice because somebody would challenge it.

To answer the question, I think there is a risk here. The current draft of the Bill goes way beyond NIS2 and it probably gives powers or functions to the NCSC when it is difficult to see why it would need them or how it would ever use them.

Dr. T.J. McIntyre: I will elaborate on that a little bit. If we think about State surveillance in a normal context, it normally involves an independent investigative agency that is applying for judicial authorisation if we are talking about particularly sensitive data, such as the content of communications data, or independent authorisation in the form of an application to the Minister for justice in the context of interception. The operation of that scheme is overseen by a designated judge of the High Court, now the Independent Examiner of Security Legislation. That is done finally with oversight at the judicial stage in the form of challenges to the admissibility of evidence where that evidence is used in the course of a prosecution. The key point there is that we have independent authorisation and, typically, judicial oversight at one stage or another.

We do not have independent authorisation here in respect of most of these powers. Not only do we not have independent authorisation, but this is very unusual in that it combines the authorisation and access to data functions in a single body. After all, this is not going to be a completely independent entity. It is going to be an entity under the direction of the Minister of justice. There is an element of marking your own homework, in the sense that the entity approving the request is part of the Executive and that information could be transmitted further within the Executive. Without wanting to be alarmist about this, it is worth pointing out that there previously were concerns about data being shared within the Department of justice for political purposes.

Senator Lynn Ruane: Would this contradict parts of GDPR legislation? Does it risk that?

Dr. T.J. McIntyre: We have set out in the submissions why we think heads 8 and 9 would be concerning. Insofar as they could be used in that way, they are contrary to Article 8 of the ECHR, the GDPR and the Charter of Fundamental Rights of the European Union.

Senator Lynn Ruane: Why would the piece on scanning for vulnerabilities without consent be necessary? Obviously, if an organisation - a public sector body or whatever - was at risk of having a vulnerability within its critical infrastructure, there would not seem to be a need to do this scanning without consent. I am wondering why.

Dr. T.J. McIntyre: There is a trade-off in this. There are essential entities that are so important to society that it is important that we make sure they are functioning correctly. They may have a profit motive not to do it, so we give our agencies power to scan them without consent to detect problems, but we only give the agencies the power to proactively scan them without consent because we think they are too big to fail and we need to keep them under close

regulation. My home office is not too big to fail, sadly. I do not see why the NCSC should have the power to scan my network without my consent.

Senator Lynn Ruane: Exactly. That is the overreach aspect. It gives the power to scan things for reasons that do not relate to cybersecurity, if they were to focus on an individual.

Dr. T.J. McIntyre: That head could be amended to make it unobjectionable by saying that other than for essential and important entities, scanning can be done with consent of the entity. Or it could say that it is to be done on notice to the entity with the entity having the chance to challenge the decision to scan.

Senator Lynn Ruane: If we are looking at this in relation to An Garda Síochána, is there a risk that this Bill is giving investigative powers that could be used to scan an individual or, under heads 8 and 9, look at particular data? How does that intersect with the question of consent if, for example, we imagine An Garda Síochána says it needs investigative powers relating to some sort of national security threat, however that is defined?

Dr. T.J. McIntyre: There is a certain degree of internal contradiction within the heads of Bill. If we look at heads 8 and 9 and then heads 10 and 11 in parallel, heads 8 and 9 are saying, in essence, that the State wants to monitor the traffic on the networks for security vulnerabilities and wants to do that for security reasons. However, heads 10 and 11 provide a very permissive structure to say it can then transmit that content and communications data - that metadata - to An Garda Síochána for investigative purposes without constraining how that is to be done. We say that this is not compatible with the approach the Court of Justice has developed in a series of cases. It says that if there is going to be bulk, indiscriminate scanning of communications, that can be done only on national security grounds and criminal investigations cannot then piggyback on those national security grounds. Our concern is that this is not laid out clearly here in the Bill. We accept that, if a national security issue was revealed by scanning and that issue was required to be dealt with by An Garda Síochána in its function as a national security agency, that could appropriately be done, but a simple criminal matter could not be detected and passed on in the same way.

An Cathaoirleach: As nobody else is indicating, I will ask a couple of questions. I am interested in Detective Chief Superintendent Walsh's opening statement and the submission we received in respect of the increase in the prevalence of cybercrime. It cites an increase from €5.5 trillion in 2020 to an expected figure of €9.5 trillion by the end of this year. Does this relate to an increased number of instances or increased value, or is it that crimes that might not necessarily have had a cybercrime dimension previously but were nonetheless being committed now have a cybercrime dimension, or is it a mix of all of these?

Mr. Barry Walsh: It is a mix of all of these factors. When we talk about cybercrime, we talk about cyber-enabled crime and cyber-dependent crime. Cyber-enabled crime would be economic frauds. This forms the vast majority in terms of global monetary value. We are seeing increases globally, both in the numbers and the financial outputs that criminals are gaining as a result of those crimes. Similarly, with cyber-dependent crimes, in particular ransomware, we are seeing increases there, as well as increases in the actual financial harm that is being caused. It is not uncommon now to see hundreds of millions of euro in disruptive costs. A ransomware attack obviously has a ransom element, but it also has mitigation and remediation elements, which are often the most expensive because they involve rebuilding the

system and making it safe again. If we look at the most recent ransomware attack in the UK, it impacted the whole supply chain of a car manufacturer. It took the car manufacturer offline for a number of weeks before its ability to construct cars again could be re-established. Not only was the car manufacturer's workforce impacted, but the supply chain was also impacted because clearly, if cars were not being made, there was an impact on jobs and other financial implications for those who supply that manufacturer. We are seeing both scale in terms of volumes and really big scale in terms of financial impacts.

An Cathaoirleach: I just want to play devil's advocate for a moment, by taking up the line of questioning pursued by Senator Ruane and others. I have two questions about the scope of the Bill. By its very nature, this is an area that will evolve all the time. The cybercrimes that will be committed in five years' time have probably not even been thought of yet. Therefore, would there not be an argument on the part of the Department to have perhaps fewer specifics in the legislation than there might ordinarily be in order to be able to respond to what might be a completely changed situation? Second, is the other problem when dealing with cybercrime that it is not always about dealing with large, defined entities? In some cases, the biggest danger to national security could actually come from a young fellow in his boxer shorts in his parents' house. Therefore, might there need to be a greater level of scope? Will Dr. McIntyre or Mr. McElligot address this?

Mr. Sean McElligott: I will start, if that is okay. On the first point, I do not think anyone is suggesting that the NCSC should be hamstrung in what it is going to need to do. There would be broad agreement in this room, I suspect, that NIS2 is extremely important and excellent legislation. It is absolutely necessary to protect Europe Inc. and, by extension, Ireland Inc. However, I would make a distinction between the powers it needs to do the job and the extremely broad powers to do whatever it wants, whenever it wants, unfettered by any supervision whatsoever. As a general policy, Irish legislation is not prepared like that. For example, the GDPR does not give the Data Protection Commission the power to do whatever it wants, whenever it wants. That is not the way it is structured; it is just not like that. Similarly, the ComReg legislation does not do that either. There a balance between protecting Ireland Inc. and Europe Inc. and doing so in a way that does not possibly trample upon the rights of companies and individuals throughout the country.

Dr. T.J. McIntyre: If I could elaborate on that, it strikes me that there is a structural issue here. We have chosen to set up the NCSC as an entity which is still under the directions of the Department, which is fine as far as it goes. However, it means that, compared to, for example, the Data Protection Commission, where there are commissioners who have a quasi-judicial status in terms of independence, prohibition on removal from office and so on, we do not have that in this case. An entity is being created which has these extremely wide powers, but then it is being put under direct political control in a way which I think is very undesirable. To some extent, a decision has to be made about where that trade off is weighted. Do we want to have greater powers in this entity, in which case greater independent authorisation for what it does is needed? Conversely, do we want to have it more under direct political control, in which case we need to scale back those powers or increase the degree of independent oversight elsewhere?

An Cathaoirleach: Will any of our guests comment on the strength within the public sector? At the time of the HSE cyberattack, there was quite a bit of commentary about the software and hardware that was in place. It was described as outdated in a number of reports. Across

the public sector and State bodies, has that now been addressed or do concerns remain? Will An Garda Síochána respond to that?

Mr. Barry Walsh: I am afraid I do not have knowledge of the general public service posture, so I am afraid I cannot answer that question.

An Cathaoirleach: Okay. I will open up the discussion for a second round. Senator Ruane has five minutes.

Senator Lynn Ruane: I will ask some questions to maybe help me understand better when we are writing the report. We have a Bill that is intended to protect us from vulnerabilities around cyberattacks and cybersecurity. The Bill references national security, which does not necessarily have to be cybersecurity. National security, whether it is defined or undefined, is something much larger. Mr. McElligot used the term "detrimental to the interests of the State". This is of concern, in that we would then would be making laws based on what that means outside of the cyber space, in which we obviously need to make sure we have protections in place. I am wondering about things like the suspension of a domain. The term "detrimental to the interests of the State" could be used in situations where people suspend or remove domains. I am trying to understand if the Bill needs to be taken back into the actual world of cybersecurity, unless it is a national security threat because of a cyberattack, because they can be linked then. Is it necessary to redraft parts of the Bill to ensure that the terms "national security" or "detrimental to the interests of the State" are not used to strangle freedom of expression on things that are seen as outside of that and may be seen as threats to the State, or to departmental policy or legislation from the Government of the day? Is this the biggest problem here or am I getting stuck on it? I am just worried that there are other parts of the Bill that we will not redraft. Is that the crux of the issue?

Mr. Sean McElligott: I agree with the Senator. I do think there is an issue here. When we step back for a second, this is about protecting Europe Inc. and Ireland Inc. It is about putting in standards so that we are, to put it simply, more secure and more protected from various threats. From my previous life working in IT, my perspective is that it is about technical standards and baselines that should be put in place so that things are not wide open. That is what NIS2 is about, whereas the Bill seems to have introduced all this other stuff which has nothing to do with that.

It is not based on technical standards. There are these others things, such as discrimination against the State. What does that mean? I do not know what it means. It is almost Big Brother-esque.

Dr. T.J. McIntyre: Yes. It strikes me that the general scheme reads as though it was drafted by two different people, one possibly in communications transposing NIS2 and one in justice taking account of national security concerns. The result is something of a mash-up. Of course, those are domestic provisions. They are not required under NIS2. In a way, we would be better off with a pure transposition of NIS2 and then decide to what extent we want to layer additional national security powers domestically. Perhaps we could have it in a separate instrument, or at least a separate section of the eventual Bill.

Senator Lynn Ruane: Is there anything that has not been asked about today that the witnesses think, in the context of the Bill, should be addressed?

Mr. Sean McElligott: From my perspective, the key issue is policy creep and the idea of non-technical issues being dealt with in legislation relating to security.

Senator Lynn Ruane: Mr. McElligott mentioned a few times that these are the heads of the Bill and that he would expect that they would be amended. That is not always the case. Sometimes, the heads of a Bill will become the eventual Bill. That is why I am asking the question now, because this is the only opportunity we get to try to say that the heads of the Bill need work in different areas. I want to make sure we are not missing something in that regard.

Mr. Erik O'Donovan: As regards the business view on it, strengthening the NCSC and putting it on a statutory footing is really positive. In previous budget submissions we made, we have called for money for the NCSC, which is an important body. National security is important. However, in our submission, and as has been said a few times here, we asked that the administrative powers be clearly defined. From the point of view of business certainty and investment, we are very supportive of the idea of technical standards, which have been mentioned, basing this on technical standards and criteria in order that the objective is performance based and we are looking at the security outcomes we want to achieve. As already stated, we support technical standards and certification schemes because both are in line with WTO ask that this be based on technical criteria. The way we look at this is that it is not an ask for less security; it is just about more certainty and accountability, which protects not only the economy but also the State.

Ms Áine Clarke: Mention was made of parts of the Bill that are incomplete. From our point of view, there are two real aspects we need more certainty on. First, organisations have to report significant incidents. As of now, however, we do not really know what exactly that means. There is no real information on the thresholds for classifying that kind of incident. We also do not have the templates for incident reporting, so that is an area there is still a bit of uncertainty around. Mr. O'Donovan alluded to this already, but, on the supply chain, it is a significant requirement on companies to manage their direct suppliers. We need a bit of guidance on what that really looks like in order that they can actually comply.

Deputy Catherine Callaghan: I apologise for being late. I was tuned in online. I have questions I would like to ask, even if some of them have already been covered to a degree.

In relation to operators of essential sectors such as healthcare, financial services and the financial market infrastructure, they continue to be, as was acknowledged already, among the most heavily targeted by ransomware. The recent Expleo report shows that about 22% of large Irish enterprises now maintain a dedicated ransomware budget and that almost a third paid ransoms in the past year. Creating these kinds of budgets normalises ransom payments and directly incentivises future criminal attacks. In that context, could the witnesses please offer an opinion as to whether they believe that essential service operators should be permitted to plan for or, indeed, pay ransoms? Should this prohibition be made explicit in the eventual national cyber security Bill?

Mr. Sean McElligott: I will start. In my practice, I act for people who have frequently been the victims of data breaches. Ransomware is a major issue. I am not sure - maybe Mr. Ryan will comment - whether there are criminal aspects to this. If I am hacked and there is ransomware involved and if I hand over some money to get the key to unlock my data, I am not sure whether Mr. Ryan is going to come knocking on my door. I am also not sure whether

the Deputy is suggesting that this proposed legislation would give Mr. Ryan the power to come knocking on my door. That is coming at the problem from the wrong side. If I have been hacked and someone is threatening to effectively put me out of business, I am not sure it is very helpful to say, "I am going to put you in jail if you do anything that might possibly assist you from where you are." The resources should be spent in chasing down the guys who came into my house, stole everything and are holding it against me.

Deputy Catherine Callaghan: Yes, but I am wondering about ransomware happening and people or large-scale companies having budgets in place. Do the witnesses think companies should be able to plan for attacks or have budgets in place? Should it even be considered or talked about in the context of the general scheme?

Dr. T.J. McIntyre: Maybe it is outside the scope of the general scheme, but there is a wider question as to the origin of ransomware, which is closely tied with the origin of cryptocurrency. There is a public policy disconnect in that governments are still, to a greater or lesser extent, promoting and normalising cryptocurrency while at the same time dealing with the scourge of ransomware. The single most significant thing we could do to minimise ransomware would be to crack down on cryptocurrencies, adopt proper customer controls on exchanges, eliminate certain exchanges entirely and, frankly, if I had my way, eliminate cryptocurrencies entirely. Somebody once described cryptocurrencies as leaving your car engine idling to produce solved sudokus which can then be used to buy cocaine. There is not any great social value-----

Deputy Catherine Callaghan: I was not expecting a response like that when I asked the question. I like the description, though. Wow.

Mr. Barry Walsh: The one thing we deal with is the reality of the cyber. The main cryptocurrencies, unfortunately, are a large-scale reality, as is ransomware, as are people being victims of ransomware and suffering the harm caused by it. There is a big debate going on as to whether payment of ransom should be legislated for. I do not think it falls into the context of this general scheme, but, from our perspective, people have to deal with the reality that faces them on the ground at a time of crisis. That is a very important perspective. We do not advocate payment of ransoms. The reason we do not is that you are dealing with criminals who are intent on maximising the return from you, as a victim. Our experience, or the general law enforcement experience, is that if you engage with criminals, particularly those who are probably resident in other jurisdictions, they will try to maximise the payout they can extract from you. They may string you along, they may give you more malware, they may get onto your system or they may carry out data exfiltration and try to extort you to pay a bigger ransom. The general consensus is that it is not a good idea to pay a ransom. That is the advice we commonly give people, but the reality of the situation is that at a time of crisis, people may feel compelled to do that.

Deputy Catherine Callaghan: Yes, some people do.

Mr. Erik O'Donovan: I absolutely agree. The advice from the Garda, the NCSC and any of the joint training initiatives we have done with both groups would be not to pay. Mr. McElligott is absolutely right: the resources should be focused on the criminals. In addition, however, maybe there is a need to build up cyber-resilience. I said that at the start. It is a matter of helping industry, and this goes back to the idea of supporting skills, that is, directing part of the National Training Fund towards digital skills.

That includes cyber skills and building the capacities of our indigenous cyber sector and the NCSC. There are at least nine new regulators who will come to this new and will require capacity to be built. I agree with all the points that have been made but we must invest in cyber readiness and boosting digital literacy across the whole population.

Senator Lynn Ruane: Are those nine new regulators mentioned related to the EU AI Act? I mean they are not different regulators in this Bill, are they?

Mr. Erik O'Donovan: No.

Ms Áine Clarke: No. It is a federated regulatory model under NIS2. The NCSC is the lead supervisor and they have delegated supervision to the sectoral regulators such as regulators for the food and drink sectors and ComReg.

Senator Lynn Ruane: So the cybersecurity piece does not intersect at all with the AI Act. Should it?

Ms Áine Clarke: Some of the regulators, I believe, are the same but their functions are separate. I think the Health Products Regulatory Authority, HPRA, is regulating under both but their functions are separate.

Senator Lynn Ruane: Is there anything in this Bill that indicates extra resources for regulators?

Ms Áine Clarke: Not under the Bill, no.

Senator Garret Kelleher: My next question might not be deemed relevant but I am intrigued by Dr. McIntyre's mention of the perceived link between those involved in establishing cryptocurrency and ransomware. Should that aspect fall under the remit of the legislation? Dr. McIntyre made the interesting observation that we should consider banning cryptocurrency and I would like to hear his thoughts on that.

Dr. T.J. McIntyre: The very first ransomware ran on PCs. It locked files and invited people to send US dollars to, I think, an address in the Philippines and, in return, a code would be put in the post and posted which would unlock the computer but obviously that is not going to scale. For ransomware, two things are needed, namely, a distribution channel and subcontractors who will help distribute it and an economy that will incentivise the distribution of malware. However, one also then needs to pay for it and get the money back but the only way that can be done at scale is by using some form of cryptocurrency. Of course cryptocurrency has this a great libertarian origin story whereby it would help promote the digital economy, would help people survive under repressive regimes and would enable aid to reach people in places like Syria where the government might be - or might have been at the time - preventing that from happening. It was going to liberate people who were unjustly targeted by national governments like sex workers by enabling them to get paid. The reality is that cryptocurrency has turned into a tool by which people can buy influence with the US President and is a tool by which people can promote ransomware. I am not entirely sure there is any other great social value to cryptocurrency yet, bar speculation and taking advantage of large numbers of predominantly young men who are investing lots of money in it and watching their fortunes tumble as we speak as Bitcoin falls. I am sorry but that probably sounded a little bit physical.

Senator Garret Kelleher: Does anybody else have a view on a cryptocurrency ban? No. This debate has been very interesting and I thank Dr. McIntyre for his response.

Deputy Catherine Callaghan: I heard Mr. Walsh mention the current threat landscape. Mandatory reporting of significant cyber incidents is a key pillar, as we know, of the NIS2 directive and is essential for protecting the operators of essential services or OES sectors that we have already mentioned such as healthcare services and financial services. It is my understanding that Estonia mandates that all cyber incidents be reported via a secure portal within 24 hours, which is supported by national legislation that specifies sector-specific duty sanctions and reporting thresholds. Does Mr. Walsh have an idea as to the current threat landscape for OES sectors in Ireland? Is there a current full picture of ongoing cyberattacks?

Under NIS2, these entities will be required to report significant incidents within strict deadlines. Are there interim measures in place to ensure rapid detection and reporting of such incidents? How will we ensure that once this Bill is enacted, all OESs are fully capable of meeting mandatory reporting obligations?

Mr. Barry Walsh: From our perspective, there is not currently any mandatory reporting obligation. The general consensus, albeit not necessarily evidence-based, but in terms of the global scale of cybercrime, is there is significant under-reporting of cybercrime. Certainly we realise the value of mandatory reporting in terms of a partnership approach. The earlier we can get on site then the more impact we can have in terms of marrying the necessity to protect our system with the requirement for us to gather evidence to investigate.

Deputy Catherine Callaghan: That pinpoints why it is essential we get the Bill passed and enacted.

Mr. Barry Walsh: The Bill is really a security Bill. From our perspective, we would see a huge value in having mandatory reporting because the more we know then the better we can get of the global landscape. At the moment, it is quite fragmented because there is no mandatory reporting and we only get snippets of information. Even where we cannot detect a crime, because that is not always going to be possible, we can build a picture of those who are involved in this type of criminality. What we see is that ransomware groups come to the fore periodically and then, as a result of a global effort, there is impact and they are closed down. It takes a while to build up a picture of a ransomware group or any cybercriminal group, particularly when they operate in the global domain. Mandatory reporting will give us the opportunity to get a better global picture.

Deputy Catherine Callaghan: Would the bureau welcome mandatory reporting?

Mr. Barry Walsh: Yes. The earlier we can get on site the better. Again, people are in a state of panic and shock when they arrive at the point where they are victims impacted by a cybercrime. We welcome this Bill from the point of view that it is very much orientated towards prevention. In our view, prevention is the best form of attack. We do not want to be the reactive element of the State showing up to a cybercrime because at that point it is too late and the damage has been done. Yes, we see huge value in mandatory reporting as it would give us the capacity to be on site as soon as practicable and would allow us to get a much more in-depth picture of the threat landscape.

Mr. Pat Ryan: To add to what has been said by the detective chief superintendent, the reporting piece is really important to law enforcement and I cannot underestimate the value that we can add when an incident happens, especially if criminality is involved. We are there to support victims and we have expertise in this area so the reporting piece is realty important. As I have seen during my career in the Garda National Cyber Crime Bureau, often we hear about things after the fact and it is nearly too late. So the initial 24 hours, especially where criminality is involved, it is really important that we are included in that initial report and that it is not after the fact. These days, cybercrime happens in an extremely fast moving environment and threat actors will try to hide their trail. So it is very important that where something happens, we are advised at an early stage in order that we can advise and assist with the preservation of evidence to ensure that it is not lost.

An Cathaoirleach: As there is a vote in the Dáil I will quickly ask a couple of questions before we take a quick break. Dr. McIntyre talked about the power to scan and the fear that it could be used for other purposes other than the original intention. Can Dr. McIntyre explain his concerns in terms of how the provision relates to this Bill in 60 seconds?

Dr. T.J. McIntyre: The NIS2 directive requires a power to scan networks of essential and important entities without their consent.

The problem with doing that is it creates a database of vulnerabilities. Sometimes, it can also trigger detection rules on your network and make you think you are under attack but, realistically, the concern is it will create a profile of what networks are vulnerable in what ways and that could be misused. It is probably not as great a concern as some of the others. You can be port scanned by anybody with or without official power and it is not a great-----

An Cathaoirleach: A scan is essentially looking at everything on a hard drive or system. Is that correct?

Dr. T.J. McIntyre: No, sorry. I should have clarified the terminology. Scanning in this context is essentially like knocking on the door and giving the handle a waggle to see if it is unlocked. It is not like the scanning we talk about in heads 8 and 9, where we are monitoring the actual contents and traffic data by communications.

An Cathaoirleach: IBEC mentioned 25% of companies faced challenges filling cybersecurity roles. Is there a quick fix? I presume it is not a legislative change that will address that, but something more practical.

Mr. Erik O'Donovan: A practical thing that can be done is direct some of the money from the National Training Fund towards digital skills, including cybersecurity. The Skillnet networks provide a good existing model that brings government, industry and academia together. Demand-led training is its model and that would give us the agility to address these supply issues.

An Cathaoirleach: The need for a grace period for implementing compliance has been mentioned. What would that look like in real terms?

Mr. Erik O'Donovan: The challenge for businesses is they need to see the final text. We have the text of the NIS2 already but we need to see the text as it applies in Ireland. That gives the certainty. Without that, there is difficulty in finalising compliance plans and budgets and in implementing security measures. It also impacts our national ambition as a regulatory hub.

We have called in the submission for an additional 12 months. Let us see what is in the Bill, but we think there should be a transition to give people time to act on the finalised legislation.

An Cathaoirleach: Is that something the Department can answer at this point? Is an implementation period under consideration?

Mr. David McGill: It is certainly under consideration. We do not know how we can give legal effect to it. We would need to get advice on that in terms of our obligations to transpose the directive and make sure it is operational. We and the regulator have always taken the approach that there will be a ramping-up period. The Bill provides for guidelines first as to the security measures. We intend that that will happen. They will not be exactly mandatory from the start. In a number of years' time, they could become mandatory through secondary legislation or enforcement measures like supervision and compliance notices. Everyone in this State and across Europe recognises that there is a ramping-up period for it to take effect. We will give consideration to the legal effect we may be able to give to that.

An Cathaoirleach: There is a vote in the Dáil and I have no other members indicating, so with the permission of members, I will draw this element of the meeting to a close. I ask for members' agreement that we publish all opening statements on the committee's website. Is that agreed? Agreed.

On behalf of the committee, I sincerely thank all our guests for taking part in this meeting on an extremely important matter. I suggest we return immediately after the vote to deal with some housekeeping matters. Is that agreed? Agreed. Go raibh míle maith agaibh.

Sitting suspended at 4.34 p.m. and resumed in private session at 5 p.m.

The joint committee adjourned at 5.26 p.m. until 3 p.m. on Tuesday, 9 December 2025.