DÁIL ÉIREANN

AN COMHCHOISTE UM IOMPAR AGUS CUMARSÁID

JOINT COMMITTEE ON TRANSPORT AND COMMUNICATIONS

Dé Céadaoin, 30 Márta 2022

Wednesday, 30 March 2022

Tháinig an Comhchoiste le chéile ag 1.15 p.m.

The Joint Committee met at 1.15 p.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	Seanadóirí / Senators
Joe Carey,	Jerry Buttimer,
Cathal Crowe,	Gerard P. Craughwell,
Michael Lowry,	Gerry Horkan.
James O'Connor,	
Darren O'Rourke,	
Ruairí Ó Murchú.	

Teachta / Deputy Kieran O'Donnell sa Chathaoir / in the Chair.

Business of Joint Committee

Chairman: No apologies have been received. I propose we go into private session to deal with some housekeeping issues. Is that agreed? Agreed.

The joint committee went into private session at 1.19 p.m. Sitting suspended at 1.51 p.m. and resumed in public session at 1.57 p.m.

Cybersecurity and Hybrid Threats Following the Russian Invasion of Ukraine: Discussion

Chairman: The purpose of the meeting is to discuss cybersecurity and possible hybrid threats from the Russian invasion of Ukraine. The meeting is to take place over two sessions. In the first, we will hear from representatives of the National Cyber Security Centre, NCSC, and officials from the Department of the Environment, Climate Action and Communications. Dr. Richard Browne, director of the NCSC, is attending in person. Attending remotely are Mr. Peter Hogan, from the cyberpolicy division in the Department of the Environment, Climate Action and Communications, Mr. Joseph Stephens, the NCSC's engagement head, and Ms Kerri-Ann Woods, from the NCSC administration team. They are all most welcome to the meeting.

All witnesses are reminded of the long-standing parliamentary practice to the effect that they should not criticise or make charges against a 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 with respect to an identifiable person or entity, they will be directed to discontinue their remarks. It is imperative that they comply with any such direction. For witnesses attending remotely from outside the Leinster House campus, there are some limitations to parliamentary privilege and, as such, they may not benefit from the same level of immunity from legal proceedings as a witness who is physically present does. Witnesses participating in this committee session from a jurisdiction outside the State are advised that they should be mindful of domestic law and how it may apply to the evidence they give.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the Houses or an official either by name or in such a way as to make him or her identifiable. I remind members of the constitutional requirement that they must be physically present within the confines of the Leinster House complex to participate in public meetings. I will not permit a member to participate where he or she is not adhering to this constitutional requirement. Therefore, any member who attempts to participate from outside the precincts of Leinster House will be asked to leave the meeting. In this regard, I ask any member partaking via MS Teams to confirm, prior to making his or her contribution, that he or she is on the grounds of the Leinster House campus.

Members and all those in attendance in the committee room are asked to exercise personal responsibility in protecting themselves and others from the risk of contracting Covid-19.

I invite Dr. Browne to make his opening statement.

Dr. Richard Browne: I thank the committee for the very timely invitation. I have a prepared statement, which I will read. I am joined by three colleagues. We will be more than happy to take any questions members may have following my presentation. I stress that there are limitations to what I can say for reasons of national security and the security and privilege of our clients. Let me start with the cybersecurity implications of Russia's ongoing invasion of Ukraine both in general and for Ireland. Ukraine has been victim of a series of cyberattacks over the last decade and has been in many ways patient zero for the more serious and sometimes destructive attacks and incidents we have heard so much about.

Similarly, it is clear that the Russian state possesses and is willing to use very advanced offensive cybersecurity capabilities, and has sought to deploy at least some of these in the run-up to and during its most recent invasion of Ukrainian territory. However, at least as far as can be determined, the effect on target of these has been minimal so far. The precise reasons for this may not be known for some time. However, it appears that a combination of Ukrainian preparedness and targeted assistance from elsewhere has helped reduce the effectiveness of cyber tools in this case, rendering them a less effective complement to conventional weapons.

There are of course manifold implications for national and international security flowing from the war on Ukraine by Russia, including the creation of profound uncertainty about the immediate future. On that basis, threat levels and risks may change, rapidly and seriously. However, at present, the NCSC's assessment of the risks to this State - in general and not just limited to Russian activity in Europe - is as follows. The threat from cybercrime against the State, including Government and private sector, continues to be high, particularly from ransomware. We have not seen any change to the rate or seriousness of these types of incidents since the onset of the war and expect to continue to see attempts to extort money from entities here.

The threat from destructive cyberattacks conducted directly against the State or entities here continues to be low. The NCSC has not observed any evidence to suggest that there has been significant preparatory work under way. However, there have been some reports of increased scanning activity both in Ireland and across the European Union and US. The NCSC assessment is that there is no evident intent by any party to launch attacks against the State. Similarly, there is no evidence of this type of activity being launched against other EU states either. However, the NCSC assessment is that the risks of an incident affecting a service operating at a European or global scale, and of a second or third order effect on services here is moderate.

The threat from cyber activism against Ireland continues to be low. There has been a very pronounced increase in this type of activity in Russia and Ukraine, but there is little evidence of this type of activity outside of this limited environment.

The threat from cyberespionage against the public and private sector in Ireland continues to be high. The NCSC assesses that the State continues to face a persistent, active and serious threat of cyberespionage against both public and private entities, and that this risk remains unaffected by events in eastern Europe. I stress again that this assessment and analysis may change, and change quickly.

The NCSC has been operating at a heightened state of preparedness since late last year in response to the tensions in eastern Europe and ongoing discussions at a European and international level on cybersecurity risks. We have contingency plans in place, in case of escalation of malicious cyberactivity impacting networks and services here. We are working with sectoral regulators and Departments to further develop these plans in key areas. We have arrangements in place to avail of external expert support, as required, including a number of third-party incident-response services which can be immediately made available to support Government or critical national infrastructure.

We have also issued a number of guidance and support documents, including most pertinently our NCSC Cyber Vitals Checklist on 1 February and a detailed advisory note on 17 February. This advisory detailed a risk assessment and appropriate advice regarding the ongoing situation in Ukraine. These documents and much more are publicly available on our website *ncsc.gov.ie*.

We are in ongoing contact with our counterparts across the European Union, as well as the UK, US and other countries to share information and monitor possible threats. We continue to work closely with the Defence Forces and An Garda Síochána and are in frequent contact with operators of critical infrastructure and services to monitor for possible malicious cyberactivity.

The message to organisations and operators at this time is very simple: we urge everyone to take the time to ensure that their cybersecurity risk assessments are updated and that their mitigating measures and response plans match the current situation. The NCSC Cyber Vitals Checklist remains a simple effective place to start for entities of any scale.

As members know, the NCSC is undergoing a period of expansion and development as a result of the Government decision in July 2021 to implement the recommendations of a capacity review which was initiated in the previous year. Since then, we have taken significant steps to expand the resources and capabilities of the organisation. We are in the process of filling 20 new permanent posts, most of which are at a senior level and the fit-out of a temporary facility for the NCSC is in progress with a view to occupation before midyear.

In addition to implementing the recommendations of the capacity review we continue to work on the measures set out in the National Cyber Security Strategy 2019-2024 with a number of measures fully achieved or at an advanced stage. This year we will carry out a midpoint review of the strategy to reassess priorities and incorporate developments and lessons learned since its inception. One critical area to be addressed as part of this review is the ongoing negotiations for a revised network and information security, NIS, directive, which supersedes some aspects of the 2019 strategy. The revised directive, NIS2, is expected to cover a broader range of sectors within a more stringent compliance framework. It is currently the subject of EU Council trilogue negotiations. It is in the latter stages of negotiations.

In the interests of time, I will skip briefly through our future planning. The NCSC headcount will grow to 45 at least by year-end and to 70 by 2024. The Government has committed to bringing forth a general scheme of a Bill to increase the powers of the NCSC by providing the legal authority to properly conduct monitoring and to gather and store intelligence on cyberthreats relating to national security.

The capacity review also recommended that the NCSC cease its compliance role under the NIS directive as it detracts from our core mission to defend cyberspace and act as trusted adviser to critical infrastructure. We are reviewing the options for devolving these functions to existing sectoral regulators in advance of the introduction of NIS2.

I remind the committee and interested parties that our website, *ncsc.gov.ie*, and our Twitter feed remain valuable and up-to-date sources for information on cybersecurity risks and threats. I would be happy to take any questions.

Chairman: We have been calling for a significant appointment within the National Cyber Security Centre. We welcome Dr. Browne’s appointment. Obviously, the matter we are covering today is now of critical importance to Ireland.

Deputy Michael Lowry: I welcome Dr. Browne to the committee and thank him for his presentation. On this occasion he is here in his capacity as director; the last time he was here he was acting director. He is coming here at a time when it is critical to develop and expand the services. His report today is encouraging in that it is progressive. Much is happening and we are moving forward to ensure that we have the capability to defend this space.

Dr. Browne said that work to fill the 20 permanent positions is at an advanced stage. I presume there was an international competition. What skill sets are available to us here in Ireland? Do we have people with the required competences in Ireland to fill these positions? I get concerned when I hear people talking about something being at an advanced stage because it is a phrase that is used frequently by the HSE when it is filling positions and we find that something at an advanced stage could still take a year. Is Dr. Browne satisfied that these appointments will happen imminently?

He mentioned temporary facilities. Obviously, to set up the kind of facility the NCSC needs requires considerable technology and expense. What does he mean by temporary? Will the NCSC be moving on to somewhere else? He mentioned the plan to increase to 45 personnel by the end of the year. Is that achievable? Obviously, it is necessary, but can it be done? He mentioned the capacity review involving devolving the compliance role to existing regulators. What regulators is he referring to?

There is a significant increase in the number of fake messages people receive. The public are alarmed at the expanding range of scams and the financial extortion involved in them. Is the NCSC taking mobile communications under its cyber remit?

Since the HSE network was hit, there has obviously been an increased awareness of the possibility of cyberattacks. Industry is taking it very seriously. The HSE has spent millions of euro redressing the problem. Remediation of this type of damage is extremely costly. Several companies have advised me that they have moved to insure themselves against attack and the cost of an attack. They have been told the insurance companies are refusing to include cyberattacks on their policies. Insurance companies are saying that they treat cyberattacks as acts of war, which is similar to a clause that is used in the case of flooding, which they say is an act of God. This is obviously going to become a serious issue if it is not addressed. What is Dr. Browne's feedback in that regard, and what is his view on insurance cover?

Dr. Richard Browne: There are quite a few questions, some I will address in more detail and others very quickly. Taking the staffing and skill sets questions together, first of all I think having 45 staff members is achievable and with a tail wind we will go beyond 45 this year. We do not have a limitation in regard to resourcing. The limitation is finding people as fast as we can.

When I say "advanced stage", it means we are interviewing at the moment. I am obviously limited in what I can say about that but I am interviewing on Friday and on Monday and multiple times throughout April. It will likely be into June by the time we start to see numbers arriving in force. At that point quite a few people will arrive. We had four separate competitions open, and closed. The closing date has passed. We are in the interviewing process for four separate competitions. There are two more to launch. That is the situation we are in. Four of six are well under way.

In regard to skill sets – this is an important point – it is important to note that we have a very advanced cybersecurity industry here by dint of the fact that we have a large technology sector, which has brought its own cybersecurity services. That has led to the creation of significant offices here working in very advanced cybersecurity fields. It is a huge bonus for us because we have direct access to companies here doing leading-edge cybersecurity research and providing leading-edge global services and skills. It also means of course that there is huge competition for those skill sets. That is a challenge.

The NCSC has focused in particular on incident response and forensics. Historically our primary role has been incident response. Over the next few years the committee will see it become much more diverse in terms of its functions because of European legislation and other things we know we should be doing. We are strong on incident response. We have a significant and deep skill set. The challenge may arise in those other areas as we go on.

In regard to its new strategy, a number of individual programmes are under way via Skillnet, the universities themselves and the universities working with industry to create new masters and degree level programmes, as well as diploma programmes in cybersecurity, but this is still a relatively young industry in that context. The supply chain of talent is becoming an issue globally. We are not unique in that regard.

As for facilities, we have secured a long-term facility. Our permanent facility will be in Dublin 4. It will be built to the full NATO security specification. As that process is also under way, our temporary facility only has to do us from mid-year this year until towards the end of next year. It is a relatively short-term facility. That does not mean it cannot be secure. It is being secured to a very high level. Of course that will be left to somebody else as a secure facility after we leave.

Regarding the compliance role I will not go into detail on the types of regulators but as a general point of principle, in most European countries the NIS compliance functions were devolved out at the outset. For example, the telecoms regulator – and we will talk about nuisance calls in a moment – took telecoms security as part of its general remit. The energy regulator did the same and so on. That is the general pattern we expect to see happen here. On the nuisance calls issue, this is a good example of why that has been the case. Telecoms is a matter for the telecoms regulator, the Commission for Communications Regulation, ComReg, and it has a particular role. It has a series of measures in place including a new nuisance calls committee, which is bringing together An Garda Síochána, people from the NCSC and people from across the telecoms sector to drive a series of measures. We have already taken some measures with it on particular types of nuisance calls, that is, those involving hyperlinks or Internet-facing services essentially. We are seeking to exploit that dichotomy where we make the telecoms and other regulators more directly responsible for regulating their industries and we deal with incident response and the higher level technological challenges.

Lastly, there are two things. The HSE incident is resolved. It was an extremely serious criminal incident which affected not just the HSE but also the medical staff, patients and the families of patients on a national level for several weeks. This is an extremely serious example of what can go wrong in a ransomware incident. It was, as is nearly always the case, a preventable incident. It could have been prevented, which is the really material challenge from our perspective. In terms of the lessons learned, the HSE took the brave and proper approach late last year of publishing a detailed analysis by PwC as to what exactly happened and what went wrong. That provides a very useful baseline for the HSE going forward. We continue to work it as recently as this morning on the steps it should be taking to move that along.

The insurance issue is relatively new. I am not familiar with this act of war concept. Clearly under international law, cyberattack can be an act of war but usually for an insurance company or a commercial contract to reflect that, it would have to be declared as such by a state. That is something we might pursue offline, if the Chairman does not mind.

Chairman: I am on the rota to speak next. We asked the Department of Defence and an Garda Síochána to attend today. They advised us that as far as they are concerned, the National Cyber Security Centre was the body responsible for cybersecurity in Ireland. Is that the situation?

Dr. Richard Browne: Absolutely, yes.

Chairman: How does the NCSC co-ordinate with the Department of Defence and an Garda Síochána?

Dr. Richard Browne: It happens on a number of different levels. This is not a simple-----

Chairman: For example, Rehab Group had a cyberattack in more recent days. We were surprised that An Garda Síochána and the Department of Defence would not come before us. They came back to us and said the sole responsibility in this area in terms of direction rests with the National Cyber Security Centre. Can we put flesh on that? With the Rehab situation that has happened in more recent days, what did the National Cyber Security Centre do? When Dr. Browne is dealing with that, what has the National Cyber Security Centre done by way of emergency actions put in place to deal with the Ukrainian crisis and more particularly any possibility of cybersecurity attacks from Russia at present? Will Dr. Browne respond to both of those questions? Is the National Cyber Security Centre the main body responsible? How does the National Cyber Security Centre interact with the other bodies such as an Garda Síochána and the Department of Defence? How did the National Cyber Security Centre interact with the Rehab Group? What specific action plans has the National Cyber Security Centre put in place to deal with potential cybersecurity threats with the Russian invasion of Ukraine?

Dr. Richard Browne: To clarify the roles, as this is an important point, the nature of the Internet, which is a privatised, fractured network, means that there is a differential response required to other security challenges. The national security issues around this are embedded in more normal corporate governance kind of issues. I will explain how we do what we do. Then I will cover the other points. The NCSC deals with cybersecurity, that is to say, the resilience and protection of critical infrastructure, national incident response and national incident response co-ordination. Increasingly, there are issues on setting standards for issues such as 5G telecoms and other related issues. That is our role. The Garda has two roles in this regard, one of which is investigating and prosecuting cybercrime. That is one issue and it is related to a series of fraud and economic crime activities. Second, it also has a domestic national security role. We deal with it on both of those. The Defence Forces and the Department of Defence, the defence establishment, obviously have the defence of the State against acts of armed aggression from the Defence Acts but they also have a cyberdefence role in terms of protecting their own networks against attacks from whatever in the cyber domain. That is how the roles generally pan out.

How we interact is on a number of different levels. On an operational level in terms of incident response we work closely with all of the uniformed agencies as well as, from time to time, the Data Protection Commission. A significant proportion of cybersecurity incidents are also data protection incidents, which is worth keeping in mind. The national security co-ordination function is exercised here primarily through the NSAC in the Department of the Taoiseach.

Our interactions with national security issues at the higher level flow through that office in close co-operation with the Defence Forces and the Garda and-----

Chairman: What is that office called?

Dr. Richard Browne: The national security analysis centre, NSAC, in the Department of the Taoiseach.

Chairman: Who heads that up?

Dr. Richard Browne: It is headed up by an assistant secretary in that Department.

Chairman: Okay.

Dr. Richard Browne: The way that works is operationally, we work bilaterally with all the parties and collectively we work through NSAC. That is how the national security apparatus works in cybersecurity.

There were two further questions with one on incident response and one on contingency planning. Without naming any individual victims of any incident, the way the incident response process works depends on the type of entity and the type of incident, not surprisingly. It is not the same for everything. The incident the Chairman has referred to happened a couple of weeks ago. It is a relatively straightforward-----

Chairman: The Rehab one.

Dr. Richard Browne: -----low-level incident with no operational impacts on the organisation itself. In other words, it was not shut down and its services were not affected. It noticed something, informed us on a Sunday and it informed the Garda and the Data Protection Commission. For obvious reasons, we do not disclose the details of incidents. We do not disclose exactly what happened. We do not disclose any victim unless the victim themselves comes to the public on the issue.

Chairman: Has the NCSC concluded its engagement with Rehab?

Dr. Richard Browne: The engagement is ongoing. The nature of the incidents can vary widely. Incidents like the HSE one, for example, were extremely high-profile. Much of our work was first, managing the whole-of-government response process and second, dealing with the granular nuts and bolts of the incident itself, that is, what actually happened on the ground. This one is more distant because it has a number of incident-response companies employed. It is not a nationally-significant incident. The organisation is investigating because it saw some activity and was not entirely certain what it was. We are providing guidance, support and some analytical capability for it, which is quite normal in that kind of low-level attack.

National security incidents that might affect a Department, an agency or an entity in critical infrastructure will of course be handled directly by us and there may be no external layer.

Chairman: To go back to the section within the Department of the Taoiseach, can Dr. Browne tell us the full name of it?

Dr. Richard Browne: It is the national security analysis centre in the Department of the Taoiseach.

Chairman: The national security analysis centre. What is its role and what is its role in relation to the NCSC?

Dr. Richard Browne: I worked in that unit for almost a year. Its role is to analyse and prepare briefing and documentation for Government on national security issues. Essentially, in these kinds of incidents - and the Rehab incident is not in that space - the role is to receive and share the incident response, process material, whatever that might be, and then to co-ordinate any briefings required for Government coming out of that.

Chairman: Looking at the situation with the Russian invasion of Ukraine and any potential cybersecurity threats, who heads that up? Is it the NCSC or the unit in the Department of the Taoiseach?

Dr. Richard Browne: For dealing with any cybersecurity risks it is us. NSAC does not have an operational role. It is a co-ordination body more than anything else.

The Chairman asked a specific question about what we are doing to prepare for potential incidents. I referred to it in my statement. We have a substantial incident-response capability ourselves and we work with and procure incident response services to keep as a reserve in case of larger incidents or particular technological challenges that might emerge during incident response processes such as analytical capability, deployed resources and various other things. In this kind of context, what we have done as part of this process and working with European colleagues is identify the number of potential incident types that might arise in the context of, for example, sanctions or related issues. Then we worked with regulators and potential victims to ensure both the incident response planning and the mitigations to deal with the incident types are in place and that we have a co-ordination role that is standing and ready to go if there were to be an incident.

Chairman: Is that in place now?

Dr. Richard Browne: Yes.

Chairman: Who did the NCSC interact with in Europe to come up with that plan?

Dr. Richard Browne: At a European level we interact through a number of different European Commission bodies on a multilateral level, including the European Union Cyber Crisis Liaison Organisation Network, CyCLONe, which is an incident response network. We had a major European-----

Chairman: On this particular response, is there a team in place? Does the NCSC have the Department of Defence, An Garda Síochána and other bodies on board? Has the NCSC, as I said, an A-team on this?

Dr. Richard Browne: I might finish, if I may, on who we are talking to in Europe because I might continue on with some of the other challenges that flow from that. There is a European network, CyCLONe, which is an incident response process for Europe as a whole. There was a very detailed major exercise on incident response earlier this year in which we played a full part. It exercised not just the entities the Chairman referred to but also the diplomatic service, in other words, how we respond to this collectively as a State and how we respond to it collectively as the European Union, which is a really important part.

Chairman: On the Russian invasion of Ukraine specifically, what has been set up in Ireland under the NCSC to ensure Ireland is prepared for any cyberthreats, current or potential?

Dr. Richard Browne: I can answer that to an extent. The Chairman will understand there is a limitation on how far I can go. In very simple terms, we have a much-expanded incident response capability by dint of both our co-operation with other entities in this State, our procurement of services, contingency and otherwise, and much more detailed contingency planning and scenario planning for various different incidents. To the Chairman's point about what is our role versus those of other entities and Departments, the role of managing incident response is ours. If it comes to a major national cybersecurity incident it will be us, just like it was during the HSE one. Other services will flow in as a reserve or in pursuit of their own statutory objectives.

Chairman: In the limited time I have left, all I really want to know is whether a response A-team is in place to deal with the Russian invasion of Ukraine and current or potential threats to cybersecurity and does Dr. Browne believe the NCSC has sufficient resources? It is recruiting 20 staff. What I want to get to is what the centre has done differently to deal specifically with cybersecurity threats related to the Russian invasion of Ukraine.

Dr. Richard Browne: I hesitate to call them an A-team, Chairman, because that has particular military connotations but in this case we have a-----

Chairman: I would not want to call them a B-team, but I understand.

Dr. Richard Browne: Or maybe junior B.

Chairman: We will call them a-----

Dr. Richard Browne: Do we have a fit-for-purpose incident response team? We absolutely do.

Chairman: Are the Department of Defence and An Garda Síochána involved in that?

Dr. Richard Browne: We have secondees working through us from the Garda and the Defence Forces, so they are centrally involved in all of that process. The question the Chairman is getting to is on the competence or capability of the NCSC's response team.

Chairman: Yes.

Dr. Richard Browne: It is worth noting we received our first international accreditation for incident response in 2017 or 2018. We are a computer security incident response team, CSIRT, in the European terminology. We are also a computer emergency response team, CERT, in American terminology. Last year we also received advanced CSIRT accreditation from the Dutch-----

Chairman: Who is chairing the centre's emergency response team in the context of the Russian-Ukrainian crisis?

Dr. Richard Browne: It is an NCSC entity so it is me, Chairman.

Chairman: Okay.

Dr. Richard Browne: To reiterate, on whether the State is ready to deal with major national cybersecurity incidents the answer is "Yes". We deal with 3,000 incidents per year. This is what we do. We have seen incidents of a wide variety of technological types on a wide range of scales.

Chairman: Dr. Browne will appreciate the level of war in Ukraine and the Russian invasion must surely bring greater risks

Dr. Richard Browne: That is literally what I said in my opening statement, Chairman. Absolutely. The thing to keep in mind about this, which is really important so I will be extremely specific, is there have been five significant cybersecurity incidents flowing directly from the ongoing conflict in Ukraine.

Chairman: In Ireland?

Dr. Richard Browne: Not in Ireland. I am sorry, I meant in Europe generally. Four of those were wipers. These were relatively straightforward pieces of malware that destroy data. These were found and detected extremely quickly within Ukraine by major global cybersecurity players. They were reversed and dealt with on a global level within hours. The world is watching this, not just from our narrow perspective but from a global one, extremely carefully and with massive resources. The types of systematic concern we have about European or global systems in financial services or any other system are also being watched very carefully by global and national bodies on a global basis. The world is watching and waiting for any kind of activity coming out of the region - that is the term we tend to use - extremely carefully. It is not that we sit and wait for it to happen. We watch within the jurisdiction of the conflict to ensure it is not coming out of there.

Chairman: Deputy Ó Murchú is next.

Deputy Ruairí Ó Murchú: I thank Dr. Browne for his attendance. He has given a comprehensive opening statement and his answers have provided some element of extra information and put it in the public domain. There have been a couple of publicised cyberattacks over the past while. Dr. Browne dealt with the HSE attack and with the Rehab scenario. There was also talk of an attempt on RTÉ. I believe it was one of those simple enough Trojan horse efforts, as in a physical Trojan horse in the form of a USB, and it was caught. I presume the NCSC is looking on these as criminal attacks but on the relationship that exists in Russia between hackers who may operate virtually as subcontractors and this greater level of scanning activity, Dr. Browne already has said that there are contingency plans for all of this. We know that when this initially heated up, instructions had been given out to the critical infrastructure operators that the centre covers. I imagine that these have been updated as the situation has become more serious. I appreciate that our witnesses cannot go into detail on what these contingency plans are in an escalation. Can I start by asking Dr. Browne about those attacks in the first instance and the ransomware scenario?

Dr. Richard Browne: There are essentially two distinct questions in there. One is on the incidents we are seeing or that are being reported in the media and the second is on our assessment of the links between organised crime in Russia and the Russian state.

On the first, it is very important to note that there has been a very considerable amount of attention on cybersecurity in many different companies, entities and Departments for a long time. Most of that has been very helpful and from time to time that spills over into paranoia, which is a function of what we do. One finds that issues are being reported as major incidents when in fact they may be nothing. That is just accidents and these things happen. It is useful to have a balanced perspective as to the risks here and not to be calling everything a wolf because the day will come when you have a wolf, and then no one will believe you.

Second, there is the much more vexed question on the links between Russian organised crime and the Russian state. The honest answer, and it will be the same answer from many European governments and many private cybersecurity firms, is that no one has been able to pin a direct link there in any material sense. There are many rumours and much supposition and there is a fairly obvious question as to how could they not know, but there has been very little by way of firm links proven by anybody between the Russian state and individual threat actor groups. It is, of course, entirely possible that this might be some kind of symbiotic relationship but right now, and on paper, there is no material proof of that.

Deputy Ruairí Ó Murchú: The national security analysis centre is a co-ordination of the NCSC, the Defence Forces, the Garda and that whole bit that relates to national security. When we had asked questions previously about the NCSC's remit, we would have been told that it relates to dealing with the critical infrastructure companies in ensuring that they follow due diligence and then in dealing with attacks. Can I have a picture of the hierarchy and the very specific details, because I do not believe it makes a great deal of sense that we have not been able to get somebody to appear before the committee from the Defence Forces or whatever? On some level, if we were to paint this as a hierarchy, the NCSC is not the boss of the Defence Forces, which deal with specific issues themselves.

Dr. Richard Browne: On the Defence Forces question, I can quote from the 2015 White Paper that the role of the Defence Forces with regard to cybersecurity is to protect their own networks. We work closely with the Communications and Information Services, CIS, Corps which is the part of the Defence Forces that does this and they have a security incident response team, SIRT, of their own. They are equipped and trained to deal with that. In some ways they operate like any other constituent of the NCSC because we give them threat intelligence information and provide them with guidance and, like the Oireachtas or any other entity, that is their role. Clearly, the Defence Forces have a broader set of roles also but obviously some of those roles are in a space that is not usually discussed, or ever discussed, in public which, of course, also poses limitations for us to talk about them.

On a hierarchy, we all have our roles. The hierarchy is flat in that the Government has sovereignty and that is the way it has to work. There is obviously a question as to why cyber is being dealt with in a separate organisation and we have military, law enforcement and national security functions in both, and yet we have an entirely separate National Cyber Security Centre. That is entirely normal in a European context. Everybody, including in the US, have exactly the same thing. There is a civilian resilience response information provision body. It is the Cybersecurity and Infrastructure Security Agency, CISA, in the US and it is the National Cyber Security Centre, NCSC, in the UK, and so on, and "NCSC" is, in fact, a term used in most of Europe.

The term I tend to use is that cybersecurity is a confounding policy problem. It is in everything and everything is in it. Everybody carries around a computing device in his or her pocket and some of us carry more than one. These devices are privately owned, the networks that serve them are privately owned, the technology they run on is privately owned and yet they can be the subject of a national security incident and, in fact, anybody in this room could be the subject of one immediately. One ends up with organisations like ours that have this cross-cutting and sometimes confusing set of remits but which remain utterly essential. As we look at this, and we have been in the context of our legislation, this model is not waning. The model of an NCSC as a separate civilian organisation is, if anything, becoming more robust. Sweden and others are moving more in this direction also. This is a kind of new normal.

Chairman: The Garda prosecutes. If, for instance, an incident arises where perhaps a mobile phone is hacked, and I get onto the mobile provider, will the provider contact the NCSC, will it contact the Garda, or will they contact both?

Dr. Richard Browne: In the first instance, they would likely get on to both, depending on the situation. Our response to those kind of incidents, when someone brings them to our notice, is that we suggest that the victim also goes to the Garda. They are not bound to and we cannot make them do that. That is, again, quite normal around Europe. We also will not report that to the Garda ourselves because we cannot do that, legally. That is also quite normal around Europe and in the US. It is important to note that our investigation is not a criminal one and we will not be prosecuting anybody or be kicking down any doors. Our concern is to understand exactly what the incident is and working with international colleagues, if we are required to, to understand who is responsible for it. Then, if there is a national security element, that will then go through the normal channels.

Deputy Ruairí Ó Murchú: Basically then, it is dealing with the threat and nullifying it. Dr. Browne spoke earlier about cyberespionage and we understand that in a straightforward way as being spying or, beyond that, even industrial espionage. I think there was an example in respect of Russia, post 2014, when it had difficulty in acquiring particular skill sets or products which they were not allowed to get, for want of a better term. They had set up shell-type companies or whatever in this State in order to get that level of expert technical software or whatever it was that was required. We are all aware of the diplomatic footprint that Russia has here and that there were diplomats-operatives who were given their marching orders in recent times. Could Dr. Browne give us, in as much as is possible, a certain outline to that threat we are under? We all know that this State is almost a tax superpower, to a degree. If one looks to hurt the Western world, there are possibly certain points here in respect of the types of companies that are here with their communication lines, and so forth. Where does the NCSC fit in, in that regard?

Dr. Richard Browne: That is obviously a very significant question and it is probably not surprising that there are clear limits as to how far I can go on any specific threat or risk. It is clear that the State is home to a significant amount of foreign direct investment from a number of different countries, not just the US, but there is a significant number of large US multinationals here. That means that there is a significant amount of IP, or intellectual property here which is a very significant target for threat actors from around the world and not just any individual state. There is obviously a significant amount of interest in that.

Second, it is important to note that this is a relatively wealthy country, an EU member, has a full seat on the UN Security Council for the moment, and is heavily engaged in a large number of international organisations: public, private, civic, private sector, and so on. That makes us a target in a wide number of ways for a broad number of threat actors looking to steal information. This is normal. While cyber potentiates an increased number of types of attacks, it does not change the fundamentals. We have always been a target for this type of activity. Our role in this regard is to ensure that entities, particularly in the private sector and critical infrastructure, are resilient and capable of dealing with these kinds of issues. If they become aware of an issue, they need to have somewhere to turn to for expert advice and guidance. One of our roles in this regard is to understand exactly what is happening and, in some cases, to predict what will happen. We need to ensure that Government is fully aware of the nature of the risks and the nature of the occurrences and incidents that we are seeing and of the need to do whatever is required to deal with those now and into the future.

Deputy Ruairí Ó Murchú: The RTÉ situation was as reported. It was an attempted Trojan attack - I mean in a non-technical sense.

Dr. Richard Browne: The Deputy will probably be aware that there is a long-standing history in industry of commercial espionage by cybersecurity firms seeking to exercise or test companies, including the simple thing of throwing a USB key over the wall in the car park at night and see if somebody picks it up and plugs it in. There are a number of things that that could be. Obviously, I will not talk about any specific entity or any particular incident. However, that kind of activity is not unknown. The long-standing advice - this is a cyber hygiene piece which is a downstream question - is that people should not be picking up or using devices of whose provenance they are unsure.

Deputy Ruairí Ó Murchú: I imagine it would be a worse one to fall for than someone clicking a link they should not click.

Senator Gerard P. Craughwell: I welcome Dr. Browne and thank him for his comprehensive statement this morning. The NCSC has been changed from a reporting to an independent office. Does Dr. Browne believe he has the full independence he requires as the director of the National Cyber Security Centre?

I am disappointed that the staff numbers will be hitting approximately 70. I would have hoped it would have a team of a couple of hundred at least. NCSC staff should be operating in every Department and every semi-State organisation, reporting directly to Dr. Browne and not to the Department. We all know that when something goes wrong, the tendency is to close the hatches and keep it in house, rather than allowing it out. I would be interested in his views on that. As Dr. Browne pointed out in his presentation, we are lucky that the major IT companies based in this country have their own inbuilt cybersecurity teams, because if they did not, some of them might be reconsidering their position with respect to staying in the country.

I would be anxious to see Dr. Browne at the top of a pyramid, but I would want to see him with assistant directors looking after, for example, integration with the private sector. Clearly from what he has said today, if we have a major cyberattack, the NCSC can only oversee other organisations working for it to resolve the problems. I would like to see the NCSC with a director with responsibility for the private sector. The NCSC should have very deep relationships with academia. I would like the NCSC to be in a position where it could fund research. I am not sure what funds are available to it to do that.

I believe the Defence Forces had two seats within the NCSC organisation, but they have not been filled for a number of years as far as I am aware. Dr. Browne might let me know what the situation is in that regard.

Dr. Browne may not want to deal with this, but I will ask it anyway. A number of organisations in the country are involved in gathering intelligence, including the Defence Forces, the Garda, the Department of Social Protection and the Department of Justice. Notwithstanding that we have a national security analysis centre, we do not have a director of homeland security. We do not have somebody who is at the top of the intelligence heap. My personal view is that Dr. Browne is the person who should be co-ordinating all intelligence in the country. It should all be coming into the NCSC because cyber is the new war. Defence in the country in concentrated in the three elements of land, sea and air and we are only beginning to wake up to the fourth element which is cyber.

I wish Dr. Browne well in his appointment. This committee fought hard to get that job recognised properly and I commend the Chairman on his work. Does Dr. Browne have enough power? Does he need more?

Dr. Richard Browne: There is a lot in that. The Senator and I have many areas of agreement. There are two elements to the question of power, authority and independence. Because we have a national security function, independence is something that will never happen for the NCSC. That is a good thing. We are subject to the political system and all the governance and control that come with that. That said, the Senator's last point makes it very clearly; the elevation of the level of the director of the NCSC indicates the importance it is being given across Government, not just in the Department but at a whole-of-system level. It also fully reflects the focus on this across this security system in the state. As the Senator will be aware, there are five domains of warfare, including space. How we manage the fusion of intelligence sources around all that is somewhat in flux. Work on a national security strategy has been in process for a while but it is essentially complete. It addresses many of these questions. As it has not been agreed, obviously, I cannot go into it in any detail.

There are two further questions that are particularly interesting to deal with upfront. The Senator asked how many staff we ultimately need. The figure of 70 is a start, but I agree we will need to go significantly beyond that. The facility we are building in Dublin 4 has space for many more than that. That should be a general guide. I do not think anybody has accused me of lacking ambition in this regard.

The Senator asked about our role in having staff sitting in other organisations. We do not have secondments out of the organisation simply because we are keeping the staff for what they fundamentally need to do right now. The NCSC needs to grow and in due course we will be in a position to have secondees elsewhere. We need to keep two things in mind in that regard. First, we have a sensor platform deployed across Departments. We do not need to have someone in the office because we are watching externally from a distance. Second, we have a rapid-reaction team that can be sent into offices if we have an incident. We use that on a relatively regular basis, most pertinently in the Coombe incident before Christmas, which was a public incident.

Do we have sufficient power under the legislation? No, we do not. There are things we need to do that we cannot do at present. We are limited not by our technology or by our people in some ways, but by our statutory powers. That is in process and work is significantly advanced on all that. I am sure the committee will be engaged in that process when the legislation comes before it. Some of that will clarify our role *vis-à-vis* other organisations in the State. Some of it will create new powers which have not previously been in anybody's hands in the State. I am sure it will be challenging for people to understand why. That is a process we will get to in due course.

Regarding research, we work very closely through Cyber Ireland with academia and bilaterally with academia on the skills piece. Much more remains to be done there. Regarding research, the Senator should watch this space; we hope to make a public announcement quite soon. I agree there is a question. It is covered in measures 14 and 16 of the national cybersecurity strategy around how we fund and structure cybersecurity research in the State. We do not have a singular hub of expertise. We have a number of university departments with significant expertise and universities with a background in this space, but no singular hub. That is something we feel needs to be addressed and it is covered in the strategy. That is also in process at the moment.

Senator Gerard P. Craughwell: I am on record as saying we should be proactively probing organisations. If an organisation is found to have a gap in its security system, the centre should be able to issue a warning and give it a period of time to resolve the possible gap, and if it fails to do that, it should be forcibly removed from the network and denied access to the worldwide web.

Another matter that is a major concern for me is the undersea cables coming to Ireland. We know that a cable was cut in Finland recently. We have the ridiculous situation in this country where the Garda Síochána is responsible for the undersea cables and the Naval Service, which is patrolling the sea, does not have the capacity to see under the sea. Without breaching security, is Dr. Browne comfortable that we have the right organisations looking after the infrastructure or the hardware, as it were?

Dr. Richard Browne: On the first question, the committee is aware that we have a compliance function under the NIS directive covering several different sectors of critical infrastructure. We have powers roughly akin to those suggested by the Senator, including the ability to audit. We have an ongoing compliance process. It does not amount to a full audit, but when we are either uncomfortable with the level of preparedness or we are just doing a circular, it-is-that-time type of audit, we do audits of critical infrastructure operators. Those have found gaps in the past, which we have compelled them to fix and redress. That is a very detailed and complex process for a number of different reasons. In our view, it is much better served if it is mainlined as part of the general regulatory work of the organisation because quite often in regulated sectors funding is provided via regulatory decision and if a regulatory decision is that one must spend more on cybersecurity, that should come via the funding authority. That is somewhat self-evident.

On the issue of physical infrastructure, first, we do not have a role in physical infrastructure. In some of our incident response processes and some of our compliance work, we specify some physical controls that have to be in place. The first thing the committee should always keep in mind on this is that the most pressing threat to fibre infrastructure is always the big yellow digger, BYD, type. The most likely prospect is that somebody will hit it with a digger. The most likely prospect for subsea cables is that somebody will pull an anchor or a trawl over it. In some cases, fibres are armoured and protected against it, but not always. The physical infrastructure is complex, and the Commission on the Defence Forces report makes some recommendations relating to this which will be addressed in due course in a piece. We have spoken to our colleagues in the Cybersecurity and Infrastructure Security Agency, CISA, in the US about this in the recent past and they have outlined what they do. It is not wildly dissimilar to what happens here. There is a question, therefore, but there is no global unified solution to it.

Chairman: In the centre's capacity review, recommendation 7 is to develop a national cyber incident management framework that outlines the role of the NCSC as the lead authority. Have you developed that framework?

Dr. Richard Browne: I will explain what that is. We have a critical national incident response plan. We have had it for some time and we update it. As part of our internal review of the HSE incident response process, we took that piece and identified exactly how we would operationalise it. That work is well under way now. Some aspects of it have been used in our contingency planning for ongoing issues. It is not finalised, because we are using it and operationalising it. It will be finalised once we have finished our contingency planning. Basically, we are learning from this as we are doing it. Also, and this goes to your point, Chairman, a lot of the learning from this is bringing other entities in and explaining to them what our role is and what their role will be in an incident. Then everybody has a much clearer understanding of roles, responsibilities and the incident response process and how it works in a live fire.

Chairman: The simple question to you, as head of the National Cyber Security Centre, is: how exposed is the country in terms of cybersecurity threats at present, considering the invasion of Ukraine by Russia and various other things?

Dr. Richard Browne: It would be silly to suggest that we are in any way invulnerable. Every country and every entity with an Internet connection is vulnerable to some type of incident. Cybersecurity incidents are uniquely complex because of the nested nature of systems. This organisation, every organisation and every individual depend on a networked series of services. It is impossible in some ways to predict what will happen if entity X, Y or Z is affected. It is not just whether we are vulnerable, but understanding the detailed, nested set of dependencies in that vulnerability. We have completed, and it is in the strategy, our most recent risk assessment of critical infrastructure. We have a fairly detailed understanding - I will not say it is 100% comprehensive - of the primary nest of dependencies.

We are lucky in some ways. This is a small State. We have a relatively resilient infrastructure and we have a relatively limited number of touch points, but there will always be challenges. Our role has been to prepare the critical services. We have started with critical, but we will go beyond that in due course to make sure that as many people as possible are aware of and up to speed on this. We face a challenge. To be blunt about it, we have lived for a long time with a benign external security environment. Cybersecurity and the rise and development of these types of cross-cutting, deeply-enmeshed threats pose a new challenge for this State, which we are dealing with without some of the institutional architecture that other states have had in the past. That means we have to invent things and systems as we go. In some ways, that is an advantage because what we are doing is not last year's problem, but this year's problem.

Senator Gerard P. Craughwell: I have a final question. As the director of the National Cyber Security Centre, does Dr. Browne report directly to the Department of the Taoiseach or is he still reporting to a Department? If he were reporting to the Department of the Taoiseach, it would give him significantly more clout, for want of a better description.

Dr. Richard Browne: Having worked in the Department of the Taoiseach, I am not sure that is necessarily the case, but I understand the Senator's point. My reporting line is to the Secretary General of the Department of the Environment, Climate and Communications. However, on national security issues, the reporting line and briefing line is obviously into the centre as well, including bilaterally with-----

Senator Gerard P. Craughwell: My view is that the centre should be under the Department of Defence. However, that is for another day.

Chairman: Senator Buttimer has five minutes.

Senator Jerry Buttimer: I welcome Dr. Browne and thank him for his contribution. I congratulate him on his appointment. Unlike Senator Craughwell, I believe the centre should be under the Department of Justice. We have a department of homeland security and it is called the Department of Justice.

In *The Irish Times* today, one of our witnesses today, Dr. Michael Scott, is reported as saying that he will tell us later that our response as a state to cybersecurity is "pretty woeful". How would Dr. Browne react to that?

Dr. Richard Browne: First, I would not. I have never met or come across Dr. Scott and I am not aware of the basis of his concerns. There was a mention of a 2012 EU report, but that was before my time.

Senator Jerry Buttimer: I thank Dr. Browne. In his presentation and in response to a question he referred to the telecommunications regulator. With regard to telecommunications, the banking sector, the HSE, Rehab and the charity sector, is there a silo mentality in operation or is there now joined-up thinking? Dr. Browne referred to the HSE being a preventable incident and commented on the PwC analysis. How are members of the committee to assume or to take it that the telecommunications regulator is working with the director and others to ensure there are not other attacks happening if we are operating with a silo mentality, or are we?

Dr. Richard Browne: It is important to stress that some sectors were well ahead of others in terms of preparedness for cybersecurity. That is backed into sectoral-specific legislation, and banking and financial services are an obvious case in point. Also, in telecommunications, for example, they have 2011 obligations on network and information security, which means they were slightly further ahead. The mentality question is difficult to answer because there is no single unified organisational culture across these organisations. They are very different. The HSE faces huge challenges in balancing a large clinical workload and the care responsibilities for 5 million people with cybersecurity responsibilities that come in on top of all that late in the day, so to speak.

I do not think it is fair to say there is a singular mentality of any kind. There is a broad and much more focused understanding of the risks associated with cybersecurity incidents, not just since the HSE incident but going back years prior to that. There is a growing collective understanding of the things that need to be done to deal with that. The challenge is that some of these changes are structural. They are not just the need to buy better computers, but a structural change to organisations, which takes time. That is happening across the public service, particularly thanks to the work of the Office of the Government Chief Information Officer, OGCIO, the national digital strategy and a much greater focus on unified digital processes. Across the private sector, some areas are going to struggle, and were always likely to, especially in the voluntary sector. In some cases, such sectors handle personal data, personal information and relatively large amounts of money but may not have strong corporate governance around their function. If members look at our recent baseline standard for the public sector, to our mind this needs to be a governance question and needs to be mainlined as part of corporate governance. When we speak about regulators taking on and mainstreaming cybersecurity as part of their regulatory function, the same argument needs to be made in corporate governance more generally. Work is ongoing with the chartered accountants' organisations to look at exactly that.

Senator Jerry Buttimer: The NCSC referenced in its presentation that its headcount will grow from 45 to 70 by 2024. Will Dr. Browne comment on the excellent work being done in higher education by Dr. Eoin Byrne, the cluster manager at Cyber Ireland, on a collaborative approach to recruitment? How does he see the role of the NCSC in working with Dr. Byrne on that? I compliment Dr. Byrne on the work he is doing with the Munster Technological University, MTU, in Cork.

Dr. Richard Browne: The committee is probably aware that Cyber Ireland is a collaborative group run out of MTU in Cork city but originally funded by IDA Ireland and Enterprise Ireland. Corporate governance responsibility for that organisation runs through that stream. For full disclosure, I am on the board of Cyber Ireland. The NCSC is fully engaged with that organisation and has been since its origins. It is also important to know that Cyber Ireland was centrally involved in helping us draft the national cybersecurity strategy. Some of the measures came from that process and from the group that makes up the board of that organisation. Cyber Ireland has a very important role to play in all this. It operates as a cluster and focal point for industry, the Government, the private sector and the third level sector in general. It has already had significant success in bringing these organisations together. The cluster membership alone is extremely comprehensive in terms of the industry in the State. It is bringing out a very substantial publication in the next couple of weeks, which will explain a lot of this in much greater detail.

I tacitly referred to this in my responses to Senator Craughwell, but it is important to note there is a European national co-ordination centre, NCC, role for research and development which includes this kind of clustering industry co-operation and academic co-operation piece. That process is under way at present. The formal designation of the NCC role will be clear in the next couple of weeks. After that point in time, our role with regard to Cyber Ireland may be changed slightly as well.

Quite aside from the Cyber Ireland perspective, we always work closely with academia in respect of our ongoing and, more recently, contractual relationship with University College Dublin, for expertise in some cases, but also with other universities in the State for little things. For example, when we need people to interview staff members, we tend to lean on universities because they have the technical expertise we need to determine what best practice actually is, and in understanding what the leading edge of technology is. Some very high-end research and development is happening in universities in the State right now, which is of extreme use to us.

Senator Jerry Buttimer: My final contribution is to thank Dr. Browne for his remarks. That collaborative project in MTU he spoke about, aimed at the critical skills shortage in the area of professional cybersecurity, began before any attack was imminent. I commend Dr. Byrne and others in MTU on their work. I thank Dr. Browne for attending.

Deputy Joe Carey: I confirm that I am in my office in Leinster House. Dr. Browne is very welcome. I congratulate him on his appointment and thank him for his engagement with the committee. There is considerable concern about Russia and its noted involvement in cybercrime, including the potential for an acceleration of its activities in cybercrime, coupled with its unlawful invasion of Ukraine. The most noted cybercrime in Ireland was the recent attack on the HSE. Can Dr. Browne confirm that Russia was involved in that particular attack? I would also like to know if the NCSC has a hotlist of other countries that are involved in this type of activity. What recourse is there for a country like Ireland, which has been subjected to such an attack on the HSE end of our health system? What inroads has Dr. Browne and his organisation made in following up on that?

Dr. Richard Browne: There are four questions in total from the Deputy. I thank him for them. They are extremely pertinent. In the first instance, it is important to explain in a little detail - I will not take up too much time - that there is a formal process known as attribution, where states attribute a cybersecurity incident. This State has never independently attributed any incident to another state. It is a diplomatic process that, in essence, involves calling out an attacker. We have taken part in and joined several European attribution processes-----

Chairman: Attribution.

Dr. Richard Browne: Yes. We have not ever named a state as being responsible for a cybersecurity incident in this country. The widely promulgated responsible actor for the HSE incident is in Russia and is largely regarded as being based in a Russian city. We would not demur from that analysis, although we have never named the threat actor involved. That is an important detail.

On top of that, regarding the hotlist of most active countries, I will refer to a recent Microsoft report that backs up decades of industry experience. The four countries seen as largely responsible for the bulk of cybersecurity incidents are the Russian state, which is responsible for up to 65% of cybersecurity incidents globally, according to the Microsoft report published late last year, China, North Korea and Iran. Those are the four states generally regarded in the literature as being responsible for the majority of cyberattack offences. They do different things and focus on different types of actions, but that is what it is.

Chairman: Have those countries been called out by other member states?

Dr. Richard Browne: Some member states have called them out, especially in their published intelligence assessments. If we look at the national cybersecurity strategy, the White Paper on defence and the White Paper update, some of these things have been called out in those cases, but we have never formally attributed an attack to any one of those states.

Chairman: Why not?

Dr. Richard Browne: It is a question of diplomacy. I am not saying it has or has not happened. It is a very vexed question in the sense that, to do so, one has to be very sure the attack emanated from the state being named and be extremely sure it can be substantiated in a public way.

Chairman: To go back to Deputy Carey's question, was Russia involved in the HSE cyberattack?

Dr. Richard Browne: As I said, the threat actor largely named as being responsible for it is regarded as being based in Russia. Whether it was the Russian state is a different question. We cannot substantiate that. The other reason attribution is challenging is when one tells the world one has found an incident, one has also told the world how one found the incident. Tradecraft and capability is given away.

Chairman: Is the attribution against a member state? Is the state complicit in the cybersecurity action by someone based in an individual country?

Dr. Richard Browne: It varies from time to time but, in most cases, attributions name the state and the threat actor. In some cases, including many recent US cases, the individual officers responsible were also named.

Chairman: Can that only be done on the basis of a member state being found to be complicit?

Dr. Richard Browne: It has to go beyond complicit. It has to be "actively involved in". An official of the state must have conducted the attack.

Chairman: Okay.

Deputy Joe Carey: I have one last question. What recourse have we as a State? Dr. Browne said this attack emanated from Russia. What recourse have we? As a country, are we linking with other jurisdictions and agencies to get some recourse? This cyberattack caused major interruption, and continues to do so, across our health system, yet these people can walk off into the sunset. It is not right.

Dr. Richard Browne: The short answer is there is nothing the State can individually do to chase down entities or individuals, if they are hiding in another jurisdiction. It as simple as that.

Chairman: It is fair to say, however, that the State could take abatement action against another state such as Russia in respect of the HSE. That option is there.

Dr. Richard Browne: It is much more complex than that. I will explain in slightly more detail. In the first instance, the recourse under international law is usually against states, not individuals. Therefore, if an individual happens to be in a state, the action is usually criminal. It is an extradition-type process. Obtaining sufficient proof and identifying individuals in these cases is extremely difficult. This is a criminal matter for the Garda. The Garda has had some success in taking down a domain used by the attackers and has traced some of the route of the data as they made their way out of HSE systems and, presumably, back to the systems of the threat actor. All of that gets you only so far. If the host nation is not willing to play ball on a law enforcement basis - and in this case the Russian state does not have a very positive history of engagement with criminal investigations in this way - then one is relatively limited in what one can do in that regard. That is not to say nothing can be done. That is a really important point. We have joined an international counter-ransomware initiative run by the National Security Council, NSC, in the White House. We engage very closely with our European and international colleagues on incident response and investigations - not law enforcement investigations as that is a criminal issue, but in the cybersecurity world. That is to understand exactly who these people are individually, what tools they use, how to better defend against them and how to ensure that, in due course, albeit maybe not this year, somebody will be able to put a finger on them and arrest them or whatever. That is a long process but, similarly, there is a long history of cybersecurity actors and criminals being picked up and arrested in international airports after multi-annual, multinational investigations. That is how you get these guys: not with a solo run by any individual but with a collective effort.

Deputy Joe Carey: May I ask just two short follow-up questions?

Chairman: Yes, briefly.

Deputy Joe Carey: How does our system now measure up compared with other jurisdictions in respect of confidence and headcount? I note that the NCSC intends to bring its headcount up to 45 by the end of this year and to 70 by 2024. In the event that it does not reach those figures, does it have any contingency plans?

Out of interest, will Dr. Browne give us an overview of the college courses available in Ireland on this growing area of cybersecurity? Do we have courses available to train people?

Chairman: Have you another question, Deputy Carey?

Deputy Joe Carey: That is it.

Chairman: Dr. Browne, please respond briefly. Three or four other Members are indicating.

Dr. Richard Browne: Of course. I will be quick. I will respond to the matters raised in no particular order.

As for the competence level of the NCSC, I have explained this already but I will give the committee the chapter and verse. We have all the various accreditations required of a CSIRT. Most pertinently, there is a comparative element to this. We received advanced CSIRT accreditation in 2019 during the European Union Agency for Cybersecurity, ENISA, peer review process. Our peer review process involved the Dutch CSIRT. We are regarded by our peers as being an advanced CSIRT, a status not held by many CSIRTs in the European Union. In and of itself, that should not be surprising. This is what we do. As I said, we are lucky.

There has been a master's in cyberforensics in UCD for many years. A great number of our staff have been through that course, some recently, some a long time ago. Some of our staff have taught on the course for years. Incident response is our core competence. There are a large number of degree and master's courses and diploma and higher diploma courses. Most universities have several. However, cyber is a complex compound discipline involving entities from computer science to governance to technology. It is not a simple thing.

Chairman: I now move to Deputy O'Connor. You have roughly five minutes, Deputy. We need to conclude this session by 3.30 p.m.

Deputy James O'Connor: I welcome Dr. Browne to the committee. First, how long has he served in his existing position?

Dr. Richard Browne: I have served in my current role since July of last year. My position was formalised in January.

Deputy James O'Connor: It has been a very difficult time for the employees working under Dr. Browne. I am sure his role is currently under a lot of scrutiny, and rightly so. We are in a very different time from three or four years ago. There is more global instability. I think we would all agree on that point. There appears to be an increase in espionage activity in this State. That has proven to be the case with the expulsion of four Russian diplomats. Although not much information on that has been given, it was done in the context of espionage in other European countries, so it is clear that that is going on. Has Dr. Browne confidence that if we were to come under attack again in a similar way to what happened last year, our services, particularly the HSE, would be able to sustain such an attack? Has the NCSC put defensive measures in place that would allow the HSE's IT system to be better protected than it was over a year ago?

Dr. Richard Browne: There were two very distinct questions there but there is a common theme to them. It is really important to note that entities are responsible for their own security, so the HSE and hospitals are responsible for and own their own security risk. We can say with certainty, however, that the HSE has taken very significant measures to defend and to harden its own systems and to identify issues as they arise. Without going into any great detail, incidents happen all the time. For the very most part, they are dealt with long before they get to the point of last May's incident. We see incidents happen very regularly. It is not that we have an incident once every six months; we have one several times a day. Most of them, however, are dealt with long before they ever eventuate to that point. This goes to the Deputy's other point as to what we would do if we were to have an incident. We have incidents all the time. The question is what we do. The-----

Deputy James O'Connor: With respect, we have very limited time. I asked Dr. Browne a very direct question. Will the NCSC be prepared if there is another major cyberattack on the HSE? May I spell out to Dr. Browne how serious that incident was? We had no access to the parliamentary questions system to put issues relating to people's health and other serious questions that need to be regularly put to the HSE because its IT systems were effectively knocked out. Dr. Browne must appreciate that that is a huge concern for us as Members of the Houses of the Oireachtas and as members of this committee, which has to scrutinise the NCSC's work. I take issue with one of the remarks Dr. Browne made. He said that each entity is responsible for its own cybersecurity. If that is the case, the NCSC's role is pointless.

Dr. Richard Browne: That is one analysis. It is important to point out, though, that entities have to own their own security risk because they make their own investment decisions and they own their own systems. We can exercise, as we do in the HSE, an oversight role in respect of compliance. We can give bodies support and assistance, which we do. Ultimately, however, because the HSE owns the system, it must own the risk. That is-----

Deputy James O'Connor: Has Dr. Browne in his capacity advised the Government to change the current structures of how we manage cybersecurity, taking a more defence analysis to it? Would Dr. Browne like to expand on that?

Dr. Richard Browne: The way we do cybersecurity is the way Europe as a whole does it, and that is exactly on the basis I outlined. The Deputy asked me a very direct question, whether the HSE is ready for an incident-----

Deputy James O'Connor: Hang on a second. I asked Dr. Browne a question; I ask him to answer it. Did he advise the Government to change its protocols in respect of how we manage our cybersecurity on foot of what has happened?

Dr. Richard Browne: I do not need to advise the Government to change its protocols because we do cybersecurity incident response. When it comes to changing cybersecurity incident response, that is something we do and have done. I have explicitly referred to this already. I am not sure the Deputy was in the room. We did a post-incident response review process after the HSE incident and we fundamentally changed the way we do incident response, so yes, we categorically did in a number of different ways, some of which I can explain, some of which I cannot.

Deputy James O'Connor: May I raise one further issue with Dr. Browne in the limited time I have left? I apologise for being so direct with him but I have very limited time. As for the IT advice and support given to Members, who would be classed as politically exposed persons, as is the case in financial services, we are not given any cybersecurity advice of note. Although those of us in public office, particularly those serving at Cabinet level, are given some IT equipment, Dr. Browne's agency should look at working with us on that with other key personnel, whether they work in high-ranking roles in the Defence Forces, an Garda Síochána or in other roles that may be subject to espionage, which we now know is going on. That has been confirmed by what has happened with the Russian Embassy. That is a concern. Does Dr. Browne accept that?

Dr. Richard Browne: We have published explicit advice for elected representatives and candidates on our website-----

Deputy James O'Connor: Did the NCSC do a clinic or an interaction or does it sit down with people?

Dr. Richard Browne: We have sought to do that for quite a while. We will do that directly with Ministers. Ministers have been given cybersecurity advice directly, and we will continue to do that. We will also give advice in this House. We have dealt directly with the Houses of the

Oireachtas on the cybersecurity of this institution and its Members. It is challenging because Members are not employees of the Houses of the Oireachtas, obviously. This is a very unusual organisation in that regard. Let us be very blunt, and we have seen this in other European jurisdictions, it is also a target. Let us not shy away from that either.

Chairman: What was that last point?

Dr. Richard Browne: The Houses of the Oireachtas, and parliaments in general on a European level, are targets for cybersecurity incidents seeking to-----

Chairman: Is Dr. Browne aware of any incidents in the Houses of the Oireachtas to date?

Dr. Richard Browne: Not in the Houses of the Oireachtas, but we have seen incidents in Germany and other European countries.

Deputy James O'Connor: I am of the view that sensitive information leaks out of here like a sieve. If foreign governments want to engage in the monitoring of telephone calls and so on, they can do so. It has been done for generations and is not necessarily something that starts today. I encourage the NCSC to reach out directly to all Members. We have a role to play as part of our constitutional function. Better advice should be available to us on how to protect the work we do.

Chairman: I suspect the old-fashioned leak would not be covered under cybersecurity.

Deputy James O'Connor: I would not put journalists in the same bracket as that.

Chairman: Does that fall under Dr. Browne's remit?

Dr. Richard Browne: We focus on network and information security.

Deputy James O'Connor: I ask the representatives to take my point on board.

Dr. Richard Browne: We are more than happy to do that.

Deputy James O'Connor: I wish the NCSC well in the work it is doing. I accept it is not easy.

Chairman: I was not being facetious. I was just giving a complete view.

Deputy Darren O'Rourke: I thank the representatives for the information so far. I have a quick question to start. What is the current staff complement at the NCSC?

Dr. Richard Browne: At present, we have 33 staff in total working on cyber, three of whom are in policy. There are 30 people purely in the NCSC.

Deputy Darren O'Rourke: Dr. Browne said he would give an indicative timeline on the four streams of recruitment. I will pick up on his point regarding the NCSC's ongoing contact with its counterparts across the EU and with operators of critical infrastructure. Who did he mean by "operators"? What is his definition of critical infrastructure?

Dr. Richard Browne: There is no formal definition in law for "critical infrastructure" in this country. We use seven sectors in respect of the network and information systems, NIS, directive, including telecoms, which is covered in a number of different ways. We also cover energy, which includes electricity, gas and oil and their transmission and distribution, etc.;

transport, including land, sea and air transport; and healthcare and, more specifically, healthcare environments. If the Deputy wants to talk about how we designate in respect of healthcare, I am more than happy to do so at any length he wants. We also cover two different classifications of financial services, although it is important to note that compliance for those is dealt with by the Central Bank of Ireland. The final sector we cover is drinking water supply.

Deputy Darren O'Rourke: On the NCSC's responsibility, I take on board the previous points made about bodies being responsible for their own house. Will Dr. Browne comment on the oversight structure that is in place and his role, if he has one in that regard, to provide people with reassurance on the current state of their cybersecurity preparedness or good health?

Dr. Richard Browne: I will try to keep this answer short. In the first instance, critical infrastructure operators were, individually, completely aware of their responsibilities in this regard, even before the NCSC ever existed. We found, when we did our initial interdependency study and assessment in 2016, that-----

Deputy Darren O'Rourke: Since I know the NCSC has documentation, will Dr. Browne give us a sense of the nature of the engagement? Is it regular?

Dr. Richard Browne: I will leave aside all the work we do on instant response, planning and contingency and focus on compliance. The NCSC has a compliance team that focuses on five of those seven sectors and engages with the designated operators of essential services on a daily basis. We require all the entities to produce a detailed assessment of their own security. We then give them a gap analysis of where they are versus where they need to be. If that gap analysis and that process identifies issues, we audit them using an external company, not the NCSC. We have an independent audit of company X, Y or Z, or the entity involved. The result of that audit is then brought to the operator of essential services or entity to ensure it is moving on.

The important point is that we have been able to demonstrate, over the four years we have been doing this kind of compliance, a stepwise improvement year-on-year across critical infrastructure. This process - it is a process and not a single event - has brought people along a journey towards much greater understanding of the risks and their responsibilities in this regard, in addition to the things they need to do. Some of the audits we are doing this year are essentially catch-up audits. We are checking up to ensure everything they said had been done has been completed. We are in a much more highly advanced and mature stage than we were when we started out. It is one of the reasons handing off the compliance process is now possible. We are not at a baseline anymore. We have a set of critical infrastructure operators that are operating mature, largely compliant models. Where they are not compliant, they are in a process with us whereby they will be by the end of the year. To be very clear, most of the audits found minor structural issues or minor governance lines or chains of command that were not clear. They were not fundamental cybersecurity challenges.

Deputy Darren O'Rourke: The climate committee, which met yesterday, has been doing a body of work on energy security. Brexit shifted the ground in respect of our technical compliance with European standards. We were measured and assessed on a reasonable basis with Britain, but it now looks like we might not meet a standard for energy security. On the general landscape and the war in Ukraine, many of the sanctions relate to energy, gas and oil. From a cybersecurity perspective, is there a particular weakness that relates to energy infrastructure? Is there anything to report in that regard other than what was indicated in the opening statement?

Dr. Richard Browne: Energy is obviously fundamental to the economy and society. It is a heavily protected and defended, and very heavily regulated, sector, with its own energy security of supply and security provisions already in place. Our role in energy has included all the audits and all the processes we talked about. Brexit has had some effect, but it is not material because our European requirements are supplied regardless. In addition, and this is very important, national security is not a European competence. There is ongoing engagement with the UK on North-South and east-west security issues. I will come to the Russia situation in a second. We are very much aware of the changing landscape as a consequence of Brexit and have already adapted. We have a new North-South, east-west organisation on cybersecurity, involving officials only, with the UK to cover all-island issues.

Speaking specifically to the recent conflict and the implications for us, it is a given that energy is a major dependency for this State, as is the case for every state. As a State on an island, we have a number of obvious challenges with regard to interconnection and the nature of our grid. We are very much aware of those. Much of our work has focused on mitigating those risks. Again, this is not new to us. This is an issue we have been very much aware of and across for five or six years. There is nothing to report regarding gaps or vulnerabilities in that regard.

Deputy Darren O'Rourke: That is important because pre-Brexit the State was compliant with an n-1 standard, from the perspective of the Commission for the Regulation of Utilities, due to our relationship with Britain. We were assessed on a reasonable basis. We do not meet that standard now because we do not have redundancy in the system, which raises the question of whether there are additional cybersecurity threats regarding, for example, the Moffat interconnector for gas. I appreciate Dr. Browne's response in that regard.

Chairman: I have a final question. The HSE is obviously a critical piece of infrastructure and service. The NCSC did its audit at the time the cyberattack took place. Why did that attack take place? Have the necessary changes been made in the HSE to ensure it could withstand a further cyberattack? It is a critical piece of infrastructure.

Dr. Richard Browne: I will start with the last question first, if the Chairman does not mind. Could it happen again? Potentially, but I very much doubt it now, given what the HSE has put in place since the incident. When the incident occurred, we brought in the world's biggest external incident response company. The fundamental issue is that the HSE network is huge. Agents were put on all the machines and every endpoint on the HSE network is being watched extremely carefully so that type of incident will not happen again. That does not mean a different type will not happen but it is what it is.

As to how the incident occurred, very simply an individual device - a laptop - was compromised. That laptop remained compromised for seven weeks and then, eight days before the incident, the attackers broke out of that laptop and started exploring around the HSE network and extracting a limited amount of data from the HSE network.

Chairman: This was done through the laptop.

Dr. Richard Browne: It was done through a number of different links, not only the laptop.

Chairman: They infected the laptop, however.

Dr. Richard Browne: The initial access was via the single device. Once the individual device was affected, that could have been caught, not that it necessarily would have been. In and of itself, that is not the end of the world. However, it should have been caught and the PwC report from December of last year makes the migration of the actor across the network very clear. There were multiple signals that should have been caught. People did find these signals so it was known that there was activity but not action was taken. That is the fundamental challenge.

Chairman: Dr. Browne is saying that one small PC effectively brought down the HSE's system.

Dr. Richard Browne: It is more accurate to say that the actor used that toehold - and it was a toehold rather than a foothold - to migrate but that the migration should have been seen. That is the important point.

Chairman: Dr. Browne is happy that would not happen now. I call Deputy Cathal Crowe, who has five minutes. I wanted to ensure he could get in.

Deputy Cathal Crowe: I have to go to the Chamber shortly so five minutes suits me fine. I thank Dr. Browne for attending this committee meeting today. I have been following the meeting remotely from my office. I apologise that I am only now arriving in the committee room.

On 9 March, we were all here in Leinster House when the email system for the entire building collapsed. Within about ten minutes of that incident, the entire computer system in the Passport Office also collapsed. Has that been investigated? Specifically, has it been linked to any Russian hacking?

Dr. Richard Browne: It has been investigated and there were no links to Russian hacking.

Deputy Cathal Crowe: There were none whatsoever.

Dr. Richard Browne: There were none whatsoever. We know exactly what happened. It was not a threat actor. It was not a cyberattack.

Deputy Cathal Crowe: There was no hacking whatsoever related to that incident.

Dr. Richard Browne: No.

Deputy Cathal Crowe: It was a systems failure of some sort which was then rectified.

Dr. Richard Browne: It was exactly that.

Deputy Cathal Crowe: There is an understandable sense of paranoia in all public offices at this time because the use of cyberattacks and hacking against states that are not on its side at a given time is a known weapon of the Russian state. I am glad that is being monitored.

The situation at the Russian Embassy is very live. Four diplomats have been expelled. From the media coverage, you would gather that they probably were not diplomats to begin with and were fulfilling a different function. Is Dr. Browne's office aware of any element of hacking or related activities being involved in that action?

Dr. Richard Browne: I really cannot comment on that. I am sorry.

Chairman: We appreciate that.

Deputy Cathal Crowe: That is understandable.

Chairman: The Deputy has raised the point.

Deputy Cathal Crowe: It is a question rather than an accusation.

Chairman: It is sensitive from a security perspective, however.

Deputy Cathal Crowe: I hope we will find out more about that in due course. The public and all of us who serve the public deserve to know the full extent of any such activities in due course.

I will ask a question on a point I touched on when this committee last considered cybersecurity. I was a teacher and other members were in different walks of life before entering the Houses of the Oireachtas. It concerned me that the computer in my classroom held very sensitive data relating to child protection and children's vulnerabilities, learning needs, educational needs, parental circumstances and so on. There was a whole lot of data on that computer, which was just in a primary school classroom. If you go half a kilometre down the road to your local HSE public health centre, you will find another data set. There is another in the local Garda station. There is a data set in each community service. People talk about hubs and spokes but the Government has tentacles of public service in each and every community in the country. Some of those data are held on computers that are 15 or 20 years old and are operating on old systems. They might be connected to the mother ship of the Department of Education or the Department of Justice but they are outposts and I do not believe they are sufficiently protected. Does Dr. Browne share that concern?

Dr. Richard Browne: I have referred to this already in respect of the voluntary sector. It is a very significant challenge. Colleagues in other European jurisdictions had this exact discussion with the UK relatively recently. There is no cheap or simple solution to these questions. The UK's public sector cybersecurity strategy commits to having systems in place to deal with these kinds of questions by 2030, so this is a common issue elsewhere. These kinds of challenges arise because cybersecurity has arrived on top of an extant structure of IT and IT governance which evolved over a long period of time. As the Deputy has said, individual schools, clinics, clinical settings including dental surgeries and a wide range of other organisations hold data, including, in some cases, clinical data, on services that are not certified or unified. In many of these cases, the solution is to unify IT services or to change the structure through which they are provided. This is happening in central government, in the university sector and in other sectors. There are other sectors, including the education sector, that will be really challenging to deal with. We do not have a specific programme in place for securing educational IT but this is something that will have to be dealt with by means of centralised ICT procurement in the Department of Education. It is not a simple process. Who owns the school? Who owns the computer? Who owns the data? Who is the data controller? None of these questions are readily resolvable by anybody in the system.

Deputy Cathal Crowe: I will wrap up by referencing one final thing. A national debate on neutrality is kicking off at the moment. We are militarily neutral. That has been reiterated time and time again. However, when it comes to cybersecurity, I hold the view that we cannot be neutral. We need to lean on other countries that have a superior system to ours to defend themselves. Does Dr. Browne share that view and is he co-operating with his counterparts in other European countries to bolster Irish defences? We can definitely work with partners beyond our shores to have a more resilient Irish cybersecurity system.

Chairman: I ask Dr. Browne to make his concluding remarks.

Dr. Richard Browne: My concluding remarks are on exactly that point. To take the last question first, we work very closely with colleagues across Europe, in the US and much further afield to ensure that we and the people of the State have access to the best information and the most contemporary and up-to-date cybersecurity protections we can provide. That means we deal with entities of various different types, in uniform and out of uniform, in various different jurisdictions on an ongoing basis. Neutrality does not affect my work. I am not a military officer nor do I work in the Department of Defence.

Deputy Cathal Crowe: Cybersecurity does not require neutrality.

Dr. Richard Browne: This is an important point. Military neutrality does not affect a civilian official working in a civilian department, so there are no restrictions on us with regard to engaging or working with other parties. I am sure there would be some constitutional limitations on us joining a defensive alliance on cybersecurity but, since that does not arise, the issue does not arise.

Chairman: Dr. Browne follows the trail.

Deputy Cathal Crowe: Keep up the good work. I apologise; I have to go to the Chamber.

Deputy Ruairí Ó Murchú: I have a semi-question. It is in the public domain that those who attacked the HSE were also involved in the attack on the Rehab Group. I saw that earlier and was wondering whether there is any information available in that regard.

Dr. Richard Browne: If there is information on that in the public domain, it has not been verified by anyone I know.

Deputy Ruairí Ó Murchú: All right. I can ignore it then.

Chairman: I thank Dr. Browne for coming in. We look forward to continuing engagement with him. We will suspend for a few minutes to allow the other witnesses to come in for the second session.

Sitting suspended at 3.38 p.m. and resumed at 3.48 p.m.

Chairman: To our second session, I welcome Dr. Michael Scott, cybersecurity expert and former head of the school of computing in Dublin City University, DCU, who is attending remotely, Mr. Pat Larkin, CEO of Ward Solutions, who is here in the committee room, and Mr. Padraic O'Reilly, chief product officer of CyberSaint Security, who is also attending remotely. Mr. Larkin and Mr. O'Reilly have appeared before the committee previously, and I welcome Dr. Scott as well.

All witnesses are reminded of the long-standing parliamentary practice to the effect that they should not criticise or make charges against a 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 with respect to an identifiable person or entity, they will be directed to discontinue their remarks. It is imperative that they comply with any such direction. For witnesses attending remotely from outside the Leinster House campus, there are some limitations to parliamentary privilege and, as such, they may not benefit from the same level of immunity from legal proceedings as a witness who is physically present does. Witnesses participating in this committee session from a jurisdiction outside the State are advised that they should be mindful of domestic law and how it may apply to the evidence they give.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the Houses or an official either by name or in such a way as to make him or her identifiable. I remind members of the constitutional requirement that they must be physically present within the confines of the Leinster House complex to participate in public meetings. Reluctantly, I will not permit a member to participate where he or she is not adhering to this constitutional requirement. Therefore, any member who attempts to participate from outside the precincts of Leinster House will be asked to leave the meeting. In this regard, I ask any member partaking via MS Teams to confirm, prior to making his or her contribution, that he or she is on the grounds of the Leinster House campus.

Members and all those in attendance in the committee room are asked to exercise personal responsibility in protecting themselves and others from the risk of contracting Covid-19. I ask all the witnesses to confine their contributions to five minutes to allow us time for the members to ask questions. I invite Dr. Scott to make his opening statement.

Dr. Michael Scott: I will dive straight in. In 2012, I retired at the rank of associate professor as head of the School of Computing in DCU. My research area is cryptography. Immediately after leaving DCU, I co-founded a start-up, Miracl.com, based on this research in the area of cybersecurity. I am currently employed full-time working in a cybersecurity role in Abu Dhabi. I was a contributor to the report from the Commission on Electronic voting that lead to the scrapping of insecure electronic voting machines in Ireland back in 2006. While in DCU, I shared responsibility for pioneering a master's degree in security and forensic computing, one of the first cybersecurity master's degrees in either Ireland or the UK, and which has been running for at least the last 20 years. I have been keenly following cybersecurity-related developments in Ireland.

There can be no doubt that the Russian invasion of Ukraine has heightened the global concern around issues of cybersecurity and their potential impact on our sovereignty. There is no Geneva Convention in cyberspace; anything goes. Attackers can be hard to trace, and they often maintain a plausible deniability relationship with their governments. Critical systems depend on computers that can be hacked. The ransomware attack on the HSE demonstrated the real-world damage that can be done. Incurring the displeasure of physically distant foreign governments can now have serious local consequences.

On our response to date, fortunately, due to our intervention back in 2006, the Irish electoral system is secure, based as it is on complete transparency and the non-use of Internet-connectable devices or "stupid old pencils", as members will recall them being called. Thus, our electoral system is beyond the reach of cyberattackers. However, that was a close-run thing. There was a lot of naivety back then, but as luck would have it we avoided a trap that many other countries have stepped into in the supposed interests of modernising their electoral systems, while completely ignoring the complex security issues that can arise. Therefore, more by accident than design, we got off to a good start in the cybersecurity stakes.

Academia was not slow either. In academic circles, the growing importance of cybersecurity as a discipline was realised early on. Indeed, since the turn of the millennium, universities have maintained a steady stream of cybersecurity graduates to satisfy a growing demand from the private sector. There was a lot of awareness that cybersecurity was going to be a big thing.

However, in 2012, six years after the voting machine controversy, the European Network and Information Security Agency, ENISA, published a report which described the evolution of cybersecurity strategies of each of the EU member states. The report is still available online.

Even Luxembourg gets a mention, but Ireland is not mentioned at all. Clearly, we were right at the back of the European pack, literally doing nothing at a national level that the EU could detect, back in 2012. Thus, 2012 is year zero for Ireland's national efforts in cybersecurity. Probably as a consequence of the ENISA report, the NCSC was established. However, I suspect that we were just doing the minimum necessary to placate the EU. Investment was minimal. As far as I could make out at the time, the NCSC was a kind of two-men-and-a-dog operation working out of a couple of rooms in UCD.

Fast forward, then, to the Government's completely inadequate response to more nudging from the EU, with the launch of the National Cyber Security Strategy 2019-2024, which I interpreted as a can-kicking exercise. The NCSC was to be expanded and provided with more resources. When the HSE hack happened in May 2021, it was certainly a wake-up call. The response was not at all impressive. While I was following the media coverage, I was unaware of any expert response from the NCSC, and I could not name the equivalent of the Tony Holohan figure who might have provided some reassurance to the public that we had this under control. In fact, despite closely following the media coverage, I was unaware of any NCSC response whatsoever to the crisis. The NCSC itself is shrouded in secrecy, so I can only make a few observations about it. It appears to have been under the same leadership since its foundation. Its website contains no names. There is not a single name of an individual on the website. All the articles are anonymous. The *Irish Examiner* published an interview with the centre's director in 2021. Such an interview was described, in the article, as being rare, and no photograph of the director was allowed to appear next to the article. I can conclude, therefore, that a culture of secrecy exists within the NCSC. Personally, I have seen no job advertisements for the NCSC. My suspicion is that it is, in fact, largely staffed by secondments from other services.

At a meeting of this committee in September 2021, the Minister of State, Deputy Ossian Smyth, said "Most of what is being done is not secret and does not need to be hidden from people". However, in reality, it is secret and it is hidden. At the same meeting, an independently commissioned report, which was heavily redacted, nonetheless concluded that the NCSC was not fit for purpose as it was under-resourced and overtasked and its structural legislative foundations were totally inadequate. In short, the NCSC is secretive to the point of being invisible. Based on the redacted report and the HSE debacle, it seems reasonable to conclude that it is also largely ineffectual.

Here we are, facing into a deteriorating cybersecurity landscape, a situation made worse by the crisis in Ukraine. We are woefully unprepared, while being an attractive target for attack. We are, after all, a member of the UN Security Council. Expelling Russian diplomats can almost be guaranteed to provoke a dangerous response. We really need to start taking this seriously. Given our generally high standing in the world of IT, it is all rather embarrassing. As stated, I am currently working in the United Arab Emirates, a country comparable in size to Ireland, where they take cybersecurity very seriously and have shown themselves willing to make the necessary investment to build a strong centre of excellence in the area of cybersecurity to defend their national interests. This stands in stark contrast to the situation in Ireland.

I wish to make one last point. As I said in my introduction, there is no Geneva Convention in cyberspace. Therefore, the ability to counterpunch is an absolute necessity. It may go against the grain and against our traditions to develop an offensive capability, but as a means of deterrence, I believe it to be absolutely necessary.

Chairman: I thank Dr. Scott. I invite Mr. Larkin to make his opening statement.

Mr. Pat Larkin: It is my pleasure to attend the committee today, give an opening statement and answer any questions that members may have. The last time we were here, members asked contributors about the emerging trends we saw in the cybersecurity realm affecting our clients and what was required to mitigate such threats. The last hearing took place in the ominous shadow of the HSE attack. Since then, cyberwarfare threats have escalated in a manner and in a timeframe which has blindsided the majority.

On foot of the Ukraine invasion, Ward Solutions, the organisation of which I am CEO, notified our clients in our situational security advisories of what we believed to be significantly increased risks to them, including increased criminal activity capitalising on the emotive curiosity arising from the war; increased cybermilitia activity from both global and local activists, attacking Russia, Ukraine or western countries with commensurate direct or collateral damage and the associated problems with attribution and blame; increased nation-state activity responding to geopolitical objectives, for example, cyberactions as part of hybrid warfare, malicious reaction to sanctions and counterstrikes to actual or perceived nation-state cyberactivity; failure of risk transference mechanisms, such as cyberinsurance, arising from policy exclusions for cyberevents originating from nation-state activities or acts of war; attacks and disruption to nearstream and downstream supply chains of national and global critical national infrastructure providers such as finance, health, utilities, telecoms, cloud services, software-as-a-service and transportation; the lack of capacity issue for already stretched cyberservice providers to support wider-scale attacks; and accelerated segregation or cyberbalkanisation of the Internet.

We continue to advise our clients on actions that should be undertaken, based on urgently revising risk assessment, mitigation and security operation plans. This encompasses increasing awareness, increasing security controls, performing basic and advanced cybersecurity tasks better, testing and rehearsing incident response plans, and disaster recovery. We have advised our clients of the need to maintain a hypervigilant security posture for the long term, planning their programmes and resources accordingly.

When we consider the tragedy and adversity of the Ukraine invasion, where Ireland is not politically neutral, along with the previous HSE cyberattack, where Ireland was at that time in a politically neutral state, we can see that neither aligned nor non-aligned status offers us effective protection from nation-state, militia or criminal cyberattacks. On a daily basis, Ward Solutions continues to deal with ever-growing operationally and financially crippling cybercriminal activity against our clients, regardless of the current geopolitical situation.

Once again, I am appealing to this committee and to anyone who will listen. I am advocating the need for a more comprehensive, robust, better resourced and highly innovative national cybersecurity strategy that is integrated as part of our national security strategy to protect Ireland. We have started the journey and made some inroads, but we are nowhere near the levels of protection we require for this decade and the rate at which the threats are developing. Time is of the essence. We have seen malevolent nation-state activity for over 15 years. Ireland has been hit both directly and indirectly. National cybersecurity strategy, practice, capacity, resources, research and capability is not something that we can switch on in days and weeks in response to a specific crisis. It requires deliberate planning and constant adaptation to extract short- and long-term success. The strategy is needed to protect our society, citizens, public and private services and our prosperity. If it is well executed, it will also bring very significant economic benefits to Ireland. The direct cybersecurity market is estimated to be worth $270 billion by 2026. There is a significant digital sector, which is heavily cybersecurity-dependent. An effective national cybersecurity strategy offers multiple levels of payback which can not only fund the strategy but also return real profits in terms of investment, jobs, export revenue and corporate taxes from the direct cybersecurity sector and from the cybersecurity-dependent sectors. The State's role in this strategy should be that of leader, co-ordinator, enabler, incubator and accelerator.

I am also a member of Cyber Ireland, the chairman and cluster manager of which made a presentation to the joint committee in 2021. We have been steadily working over the past four years to co-ordinate the triple helix of industry, government and academia in order to make Ireland a cybersecurity global leader. As part of our work, Cyber Ireland recently commissioned an international expert study of the cybersecurity sector in Ireland and will launch this study and an accompanying sectoral policy paper in May 2022. Both will be submitted to this committee. We believe they will be invaluable to members' considerations on Ireland's cybersecurity strategy.

Chairman: I thank Mr. Larkin and invite Mr. O'Reilly to make his opening statement.

Mr. Padraic O'Reilly: This topic is timely and of significant consequence. As we all saw last year, certain nation states and criminal gangs that operate within those states pose a significant threat to the public and private sectors throughout the West. Much of my work is in advancing the maturity of risk management practices inside large and small entities. I work with critical infrastructure, or essential services, across large enterprise corporations, governments in the US and elsewhere, and smaller concerns such as state and local government and small to medium-sized companies. Consequently, I have a fairly broad understanding of the challenges in critical infrastructure and shifting threat actor profiles. I also work closely with many of the firms that model cyber-risk and suggest an efficient path to mitigation and the hardening of systems. This gives me a good, high-level sense of where weaknesses persist and what efficient and cost-effective paths to the prevention of cyberincidents look like.

As we all saw in 2021, there was, effectively, a plague of ransomware. Several of these attacks became very high profile and did serious harm to citizens. Any attack on a health service should be off limits, yet criminal gangs have crossed that line several times. Attacks on critical infrastructure also become political very quickly, as we saw with the Colonial Pipeline attack last year in the US. To get an idea of frequencies and impacts, almost one third of all healthcare organisations have reported an attempt at ransomware. The rate is almost double in manufacturing. Slightly over 40% are able to restore their system from back-up and only about one third will pay the ransom. The average loss in healthcare from a ransomware event is $1.27 million, but the secondary losses drive that figure much higher. There are then the human costs, which are, obviously, even more significant.

The heightened threat in the wake of geopolitical events should concern all essential services or critical infrastructure firms, and all should be on heightened alert and take measures to harden systems. More than 80% of critical infrastructure is in private ownership in the US, which produces a difficult circumstance in that public goods and services and their protection often fall outside the purview of regulation. This means the government has to be a helpful partner, stay apprised of a multitude of potential threats and get that information to the private sector in an efficient manner. Government has an important role to play in combating these threats and in helping essential services to understand current best practice. Many sectors are underfunded and the authority for security is decentralised. Water treatment is a prime example of this.

Attackers use many different tactics, techniques and procedures. The practice of risk management combines an analysis of the threat actors, their methods and the existing vulnerabilities in systems, and then looks at the essential functions of the business. After a probabilistic analysis has been carried out, the potential impacts can be understood, including the human cost, financial impacts, downtime, reputational damage and lawsuits - all are factored. It is complex, but the results are often simple. Reporters often ask me what can be done, as though the challenge were insurmountable, but it is not. There are many simple and cost-effective strategies both to prevent attacks and to mitigate the potential losses if an attack gains a foothold, but they require proper risk management and full engagement from governance structures.

In cyber, when we hear intelligence that criminal gangs with nation-state cover are preparing for attacks, we think of essential services. We think of the grid, healthcare and the supply chain for food and water, but many resources are available and not all of them are expensive. Many attacks begin because of a trivial oversight or a failure to have trained employees properly. The message of proper risk management in cyber is a largely positive one. That is not to say it does not entail significant complexity; it does. It also requires resources, but resources that are deployed wisely. The recent cyber Bill in the US details how risk management in cyber should operate and is a big step in countering the advanced persistent threat. It also puts more requirements around cyberincident reporting, which will get better information into the hands of practitioners faster. The practice of cyber is changing, as it must to meet the current challenges. I look forward to our discourse today.

Chairman: I thank Mr. O’Reilly.

Senator Jerry Buttimer: I thank our guests for their excellent contributions. This meeting should be a precursor to ones we will hold in the future. We have learned an awful lot.

Dr. Scott spoke about there being no Geneva Convention in cyberspace. How can we ensure there will be a new convention that, in a modern world, will take cybersecurity on board? As a Government and a State in collaboration with the European Union and others, how can we ensure that will take place?

Dr. Michael Scott: It would be great if something could be done in that regard and a rules-based system could be introduced in cyberspace, in order that countries could be held to account and treaties could be signed. That is the way things could go. As I pointed out, Ireland sits on the UN Security Council and, therefore, is in a position to introduce such an idea, which would be good. At the moment, however, there is nothing there. It is the Wild West, basically.

Senator Jerry Buttimer: Is a Geneva Convention for cybersecurity and cyberspace attainable?

Dr. Michael Scott: I am not sure. Unfortunately, cyberattacks can come from many quarters. Governments can be at arm’s length from them and plausible deniability is a reality. Often, we do not know the vector of the attack or where it originated. With good police work and investigative work, sometimes that can be traced, but it is one of the major problems in policing cyberspace.

Senator Jerry Buttimer: Dr. Scott spoke about the United Arab Emirates as a country with an approach that stands in contrast to ours in that the issue is taken very seriously there. How can we take a similar approach here? What sort of infrastructure should the Government put in place in that regard?

Dr. Michael Scott: We need to invest. It is not going to come cheap. The kind of expertise required is expensive and there is a great deal of competition for it, both in the private sector and from other states. It will require a significant level of investment. In Ireland, we have not made that investment. We have shied away from it and done the minimum necessary to get the EU to stop annoying us about it, but we have to step up to the plate and that will cost big bucks.

Senator Jerry Buttimer: I thank Dr. Scott. My next question is for Mr. O'Reilly, in light of Dr. Browne's comments on the legislation and Mr. O'Reilly's reference to the landmark US Bill, the Strengthening American Cybersecurity Act. How far away is Ireland from coming up with our own cybersecurity Bill such as that which the US has introduced? In the context of our collaboration and engagement, what do we need to do? Mr. O'Reilly stated in stark terms that 80% of critical infrastructure is in private ownership, which presents a difficulty. Will he elaborate on that?

Mr. Padraic O'Reilly: On the previous occasion I appeared before the committee, we spoke about the response to the health service attack and about the infrastructure the State had in place to address it. The analogue for me, when I was thinking it through, was the Colonial Pipeline attack and how a small number of staff at the US Transportation Security Administration, TSA, were looking at it and being supervisory. That was woefully inadequate and it was directly analogous to what Ireland was dealing with at the time, in respect of the size of both the staff and the problem. The essential services sector here is large, as is the critical infrastructure sector. A small group, therefore, of five or six employees at TSA with oversight for pipeline security was not going to get the job done. Immediately, therefore, our legislators put more regulatory heft behind it and it is now being moved from being voluntary to more direct requirements and regulation. We are transitioning that.

As for the recent Act that has emerged, I do not think there is any analogue in Ireland, as far as I know. That said, while we have an entire agency - the Cybersecurity and Infrastructure Security Agency, CISA - with a very large budget that is in charge of critical infrastructure, we still have problems. The Russians have still infiltrated the government and energy sector here. We recently had an alert and unsealed some indictments around Russian actors from 2011 to 2018 who were doing espionage and basically exfiltrating data. While it is obvious that Ireland needs to devote more resources to it, the story is maybe not as dark as it could look. We are finally getting our act together here in the United States with respect to risk management and we are maturing a programme.

Senator Jerry Buttimer: If I am not mistaken, Mr. O'Reilly is in Boston.

Mr. Padraic O'Reilly: I am.

Senator Jerry Buttimer: To take the state of Massachusetts, Mr. O'Reilly referenced Logan Airport and there is the Massachusetts Bay Transportation Authority. How do those entities compare with us in terms of cybersecurity?

Mr. Padraic O'Reilly: I cannot speak directly to all of that. I would say that Ireland is in an interesting position because it is advanced in the IT sense and it has a lot of infrastructure around tech companies. The practice of cyber in Ireland is very strong. What Ireland does not have is more of a centralised approach that gets some knowledge about the status of the critical infrastructure or central services there. Ireland does not really know what is going on and a lot of the operators are not held to task. Here, we have sectors that are under very strict regulation.

Senator Jerry Buttimer: I thank our witnesses for attending. Again, this is just the tip of the iceberg and I think we need to come back, as a committee, and have more substantive hearings. I hope that we can learn from the witnesses' presentations but also from the events of the past. Dr. Scott's point in regard to a new Geneva Convention is one that we need to pursue as a committee. We should perhaps bring the Minister of State, Deputy Ossian Smyth, to the committee to discuss that further with us, with a view to advancing it from a European perspective and also from an NCSC point of view.

Deputy Ruairí Ó Murchú: I thank all of the witnesses who have attended. In fairness, some of them have dealt with it in the sense that Ireland is almost a tech superpower and, on that basis, there is the idea that we have a huge amount of cybersecurity expertise, although we have not necessarily put that together. We all welcome the fact there was a capacity review of the NCSC and, following that, premises were put in place and the numbers are being increased. We also had Dr. Richard Browne before the committee. We have probably got a greater amount of information than we were able to get at the time of the HSE attack but the fact is the world has changed following the invasion of Ukraine by Russia. A number of Russian diplomats or operatives, or whatever term anyone wants to put on them, have been expelled.

We all know about the idea of asymmetric warfare at this point in time, and whether it is hybrid or cyber, we have to take it into account in a major way. It is something we have to look at. We all got the idea of what we were facing at the time of the HSE attack. We have an imminent threat from criminal enterprises and I would make an argument that some of these may operate as subcontractors of the Russian state and others who can employ them from time to time. Dr. Browne stated that that has not been proven, but he was not inferring there was no chance that this was the case and he was just putting the facts on the table.

I would like to get the expert opinion of the witnesses. I understand that a significant amount of the defences are making sure that decent digital hygiene is being operated. In the case of the HSE, we saw that was not the case. Obviously, there was a way in that allowed it to happen and, beyond that, there were no fire doors to cut it off and the connectivity did not have the protections that were required. To deal with the present circumstances, I would like to get the knowledge from the experts in the field. I ask the witnesses to state very specifically the risks that we are facing and what exactly it would require for us to protect ourselves. I think there is confusion in the sense that the NCSC works technically at the national security analysis centre. It is a body that works out of the Department of the Taoiseach and it seeks to-----

Chairman: It has an analysis bias.

Deputy Ruairí Ó Murchú: Yes, it is the control body and it seeks more to ensure there is co-operation among all others. We have seconded personnel from the Defence Forces in the NCSC but the Defence Forces also operate just like a critical infrastructure company that basically takes advice from the NCSC. In regard to whatever requirements we have from a defensive point of view and all of the rest of it, I am not sure we necessarily have the exact structure that we need. Similar to what Dr. Scott said earlier, I believe European legislation and the network and information systems, NIS, directive are being updated at this time, and that will probably put manners on us to a degree.

Chairman: If I could come in on that point, did the witnesses get an opportunity to listen to Dr. Browne's presentation to our committee?

Dr. Michael Scott: No.

Chairman: I would be interested to hear the witnesses' view on the Irish set-up at the moment, where we have the NCSC, a body within the Department of the Taoiseach, which is kind of an advisory body, and then each individual organisation, for example, the Garda-----

Senator Gerard P. Craughwell: With respect, it is more analysis of intelligence in the Department of the Taoiseach.

Chairman: Prosecution is through the Garda and the Department of Defence looks after its own infrastructure. I might just feed into the questioning from Deputy Ó Murchú. We would be interested to hear what the view of the witnesses is on what is now Irish policy around cybersecurity.

Deputy Ruairí Ó Murchú: The other thing we could throw in is the fact the NCSC had a serious role in regard to regulation and it seemed to be looking to offset to other bodies within the State while it would deal specifically with the critical infrastructure companies and then, beyond that, its primary function would be dealing with attacks. It is the CSIRT-----

Chairman: We might go to the witnesses, who can give us their overview.

Mr. Pat Larkin: The issue is that no one agency can solve this, and that is very clear. We have to treat this as a national security problem in which we are dealing with land, sea, air and cyber. We have resources deployed to protect and police those, with different responsibilities and so on. With regard to land, we have had reasonable integrity for the last 100 years or so, and we have not really had a viable land threat in the recent past. We are obviously worried about sea and air but, realistically, that is not impacting us. Cyber is impacting on us daily. We are dealing with customers who are losing millions of euro in cyberattacks, and that is in the commercial sector and some critical national infrastructure providers. The cyber realm is being penetrated daily. In the current geopolitical circumstances, we get the sense that in being on the wrong side of a particular alliance or in not being politically neutral, a cyberthreat can be effected very significantly against Ireland. If we look at the resources struggle to respond to the HSE attack, the NCSC response was broadly good given our experience in this field, but if there was a wider-scale attack, there are not the resources, public and private, in Ireland to deal with it significantly. There is a huge skills shortage. Companies like ours and all our peers are currently tied up trying to respond to the customer base we have. We have difficulty taking on new customers to respond to. That is both in security monitoring and instant-response circumstances. We have to treat cybersecurity as a national security problem. The realm in which the problem exists is being penetrated daily. One strongly suspects that much of our critical national infrastructure has been penetrated to some degree, effectively meaning there are ticking time bombs waiting to be activated. We must deal with this as a national security problem and a national economic problem. This presumes escalation to a level in government that can cross-co-ordinate and provide the leadership and resources needed to co-ordinate defence, policing, foreign policy, law and international relations. It should be the responsibility of the Department of the Taoiseach as a national security problem. It requires a multi-agency response that demands co-ordination and policy. No matter how many resources we throw at the NCSC as an agency, it will not solve the problem entirely. Therefore, a public private partnership is needed to address it also.

Mr. Padraig O'Reilly: Not wishing to be too US-centric, I take as my model some elements of the approach here in the US. While it has taken some time to shake out, CISA effectively liaises between the public and private elements. It does a lot of the associated co-ordination. It aggregates the threats, takes the intelligence and does the information-sharing. It posts a lot of pretty helpful information. It is free and available to anyone anywhere. The Shields Up initiative, which CISA came out with recently, pretty much details the mitigation strategy in light of the current threat landscape.

The FBI investigates cybercrime. Also involved is United States Cyber Command, with which I have worked on occasion. It is a branch of the military whose concerns are more offensive. There are also multi-agency involvements. The United States Department of Energy has oversight of the grid. Many of the regulations concerning the grid are updated continually in light of the current threat landscape. Sometimes they lag a bit, which is one of the major concerns. When we talk about the NIS directive, we should note there is a lag time.

To me, the major problem is risk management. The issue is not one that can be tackled without risk management. There is a list of a hundred things any organisation can do to harden systems in light of the threat landscape, and risk management involves determining which are the most effective. That is an area in which the NIS directive can come into play because it can give an idea of the posture of individual companies at present. I agree that a multi-agency, multifunctional approach is required. That is the way to tackle it.

Dr. Michael Scott: It is a complex issue that requires the involvement of multiple agencies. One of the main issues people have is that of which body they should call first in an emergency. In Ireland, it is not at all clear. Do you call the Garda or Army or try to get through to the NCSC via its website? There is no clarity on the chain of command regarding how things are done. It is good to see somebody is now involved in the Department of the Taoiseach. When matters get taken in under the auspices of the Office of the Taoiseach, it indicates that somebody somewhere believes they are important. That is good to see but the agencies need to be well led and well co-ordinated. I see a problem in this regard.

Senator Gerard P. Craughwell: I am going to address my questions to the three witnesses, whom I thank for being here. They paint a very dark picture with respect to cybersecurity in Ireland. My first experience of cybersecurity was in 1997, I believe. I managed the IT system for the college I worked in and our MicroVAX was hacked over a weekend. It was a simple attack, simply to try to break the password. Nonetheless, it brought home to me how small the world was becoming at the time. That was a long time ago.

Chairman: Did the Senator withstand it?

Senator Gerard P. Craughwell: No, we did not.

With regard to Dr. Scott's presentation, the secrecy around the NCSC is a matter of deep concern to me. It is also a matter of deep concern to me that when we first advertised the post of director of the centre, we offered a salary of €79,000 per year. This was when seeking somebody to head up national cybersecurity. It goes to show what the thinking was concerning cybersecurity at the time. I ask all the delegates to deal with this in their own way.

Dr. Scott said that there was no strategy for cybersecurity up to 2012. Given that the NHS was hammered in the UK and we did not test our systems in this country, I would have believed there was zero strategy up to 2021. We were paying lip service to it.

Let me outline what I want to establish today. Dr. Scott said that if a matter is put under the Department of the Taoiseach, it gives it an air of importance. In our recent encounter with the director of cybersecurity, the latter disputed that. He said that being under the Department of the Taoiseach did not necessarily make it any better than it was. However, in my view, giving responsibility to the Department of the Environment, Climate and Communications rather than the Department of Defence seems a nonsense. We are not analysing matters through a security lens all the time. Everything we do now should be analysed through a security lens, particularly a cybersecurity lens. I would like the witnesses to give their view on this.

I am interested in Mr. Larkin's point that we have been good at looking at land, sea and air, albeit with major restrictions and diminishing capability, but I do not believe we have looked at cybersecurity and taken it seriously. I still do not believe we are doing so, considering that we are talking about a staff of 70. I asked earlier today whether we should have cyberpersonnel reporting directly to the head of cybersecurity in every State and semi-State department. To protect the economy, should we not be proactively hacking organisations ethically to find breaches and telling them they will be removed from the wide-area network if they do not repair the breaches within a limited time that is specified? Mr. Larkin was very clear that this is an economic issue as well as a security issue. A nanosecond of carelessness could cost us our entire economy. It could cripple it.

Chairman: The Senator might ask his questions.

Senator Gerard P. Craughwell: What I am trying to do is map out what I believe cybersecurity should be. Please tell me if I am wrong. Cybersecurity should be under the Department of Defence. The director of cybersecurity should have a position that places him above everything in the country. People should be able to report directly to the NCSC. The centre should be integrated with the private sector, police and defence, and it should be running its own academic programmes and funding academic research on cybersecurity. It should have a staff somewhere north of 400 or 500. I ask Mr. Larkin to comment first, followed by Dr. Scott and Mr. O'Reilly.

Mr. Pat Larkin: To go back to the main point, I agree that the Department of Defence has a role. I can understand why the NCSC ended up where it is, in the Department responsible for communications. This is because it was regarded as a technical matter historically. It is not; it is a national security matter. It is a matter of citizen and societal safety. Therefore, we have to escalate co-ordination, leadership and responsibility to that level.

Chairman: Is there a model of that anywhere worldwide?

Mr. Pat Larkin: There are models emerging. I regard the UK as a model. It has had a number of goes at it, the most recent of which has been pretty good in respect of the role of the UK National Cyber Security Centre and the level of leadership it has provided. That is not a bad model. Again, it is a matter of continuous improvement and evolution because circumstances change. What does perfect look like? What does the desired state look like? The desired state looks like one in which everybody takes cybersecurity seriously and responsibly. Most commercial institutions, regardless of whether they are quasi-semi-State, take cybersecurity seriously. Why? It is because it is about protecting shareholder investment and revenue. If Ireland Inc. treated it the same way, it would be about protecting our tax flows, health service, foreign direct investment and national output, meaning everybody would take it appropriately seriously. We have seen the escalating threat. I use the term "lucky" advisedly, but we have been lucky that the HSE was able to recover as quickly as it could. I am sure there has been worse patient mortality as a result of it, as well as significant costs, and it is not finished yet. The model should be that everyone is educated and takes cybersecurity seriously, with co-ordination and leadership at the top. It will be impossible if it is left to a single body to drive, execute and implement all of this. Leadership is needed, with a clear statement that it is a national and economic security priority. It should be addressed with all involved agencies. We have a problem, which is that this is very much an infinite defence mindset, which we are not resourced for. Regarding Dr. Scott's earlier point, infinite defence is fine if one is confident about the ability to tire the enemy exhaustively or is in a position to launch a counterattack. There need to be consequences for cartels or nation states that launch or facilitate cyberattacks, otherwise we will be in an infinite defence model and a cyber arms race.

Chairman: Is it this abatement that is spoken about?

Mr. Pat Larkin: There have to be consequences. It is clear that some of the groups that have perpetrated ransomware and are of interest here in Ireland, without prejudicing anything, have strong nation-state affiliation. There have to be consequences for that. We have danced around it. President Biden set red lines, where if one of 16 sectors was attacked, the USA would launch a counterstrike. I am not saying it will stay this way, but it is telling that cyberwarfare has not broken out as a result of what is happening in Ukraine. I suspect that is because there is a point at which people do not want to cross a red line.

Senator Gerard P. Craughwell: Could we become a hub for those who want to attack? Would safe little Ireland be used as a proxy for those involved, such that it would damage our reputation internationally?

Mr. Pat Larkin: That could be launched anywhere. Whether people are physically here or not, infrastructure can be used. If there is a good ethical and moral regime, that is policed and shut down. If there is not, this is facilitated and encouraged. That is what has happened in many cases where attacks and cybercriminal activity have been launched. It is perfectly apparent that cybercriminal activity goes hand-in-glove with nation states in certain territories.

Dr. Michael Scott: Coming back to one of the first points, the Department of Defence is the obvious place for it to be. I do not know why cybersecurity is handled where it is at present. It seems slightly bizarre. I am sure there is some historical justification for it. I will explain one of the differences in Ireland. Countries like the UK had something in place prior to cybersecurity being an issue - they had signals intelligence with organisations such as MI5, MI6 and GCHQ. They always had an interest in this area, and cybersecurity fitted nicely into and developed from that. The military complex was a good starting point for issues of cybersecurity. We did not have any of that in Ireland. We came naked into the world in 2012. That could have been an opportunity to get it right, but unfortunately we did not. We lagged behind and were tardy in our response. We have got to the current situation, where danger has ramped up far ahead of our defensive capability. We are in a sorry state, one of confusion, about how to proceed. We need to take this seriously, make a serious investment, and try to get it right.

Mr. Padraic O'Reilly: We have a strong deterrent capability in the USA. In the UK, this was always on the radar of the military. President Biden's announcement, red lines and so on are a strong deterrent. There is tacit acknowledgement by criminal gangs that certain types of critical infrastructure attacks are off limits. It looks like we are maybe in a holding pattern. The ability to take criminal gangs offline, which the FBI, CISA and the military demonstrated last year, is a powerful deterrent. The problem is that it quickly gets geopolitical. It can probably escalate. I cannot speak for my Government, but there is probably much caution with this because it can escalate. This is brand new territory. There is no real theory of cyberwarfare yet. There is the beginnings of one. Cyber moving to kinetic is also a threat and we need a deterrent capability for that. While it is a good exercise to think about whether a stronger, more robust programme can be developed, from my experience of risk management for critical infrastructure, even when there are strong recommendations for defensive capability, there is still resistance.

There is still much work to be done on risk management and getting the private sector that is involved in critical infrastructure to do the right thing. This has largely been a governance problem. I have seen many clients in the USA that had to report a breach. The governance structure was then addressed. Regulators put them on a programme to put in place a cybersecurity programme, report on it, and tie executive compensation to it, which tended to produce some results. It is about a carrot and a stick, whether it is offensive or defensive capability. While risk management has advanced significantly, we still have a problem with governance structures that are asleep at the wheel, though I do not mean to be unkind. That has to be addressed.

Senator Gerard P. Craughwell: Dr. Scott made the point that we do not seem to advertise positions publicly. For all intents and purposes, the NCSC seems to have great high walls around it. It is a case of "there is nothing to see here, move on". Should it not constantly talk about cybersecurity in public and educate people on such matters as opening files or following unknown links? Is that not what it should be doing rather than its current, inward-looking approach of telling people to move on and that they cannot even see its photograph?

Dr. Michael Scott: The NCSC set-up seems strange. I cannot make sense of it. It is as if it is modelling itself on MI5. I am surprised the director's name is even known. Maybe we should call him "M", but the British may have copyright on that. It is not appropriate or what an organisation like that should be. The website should have such information as saying to people that they can contact Joe Bloggs, the phishing expert, if they have a phishing problem, or a ransomware expert, and so on. Seventy people are employed, but I could not name one apart from the director, who I found using Google. They are invisible. What is the problem? Are they afraid? Maybe they think they will come under personal attack, but that is not how other people do it.

Chairman: Obviously we are casting no aspersions.

Dr. Michael Scott: No, no.

Chairman: When Mr. Larkin was last here, I asked him about what we should spend on cybersecurity. The redacted report in the capacity review indicated that the numbers in the NCSC were increased from 25 to 41, with 28 more being recruited. Mr. Larkin said the spending should be the same *per capita* as in the UK. It came out at about €50 million per annum. Does he still hold to that?

Mr. Pat Larkin: Yes. It is what we should ask the NCSC to do.

Chairman: Mr. Larkin says €50 million per annum and we are spending a fraction of that, at €8 million or €9 million.

Mr. Pat Larkin: Roughly.

Chairman: It would be roughly five times that. Is that what the UK is spending?

Mr. Pat Larkin: Over a five-year period, the UK is spending between €2.7 billion and €2.9 billion.

Chairman: So if we spent a *pro rata* amount, we would spend about €50 million per year. How many staff would that entail? Why is Mr. Larkin saying that?

Mr. Pat Larkin: The NCSC originated from an attempt to satisfy EU requirements regarding critical national infrastructure. My understanding and experience is that it remains focused on critical national infrastructure. From our perspective, if our clients are attacked, we do not contact the NCSC unless they have a critical national infrastructure remit. We might contact An Garda Síochána and-or other bodies.

Chairman: If Mr. Larkin has a client whose operations involve critical national infrastructure, who does he phone?

Mr. Pat Larkin: If critical national infrastructure is involved, we would try to provide the service ourselves, because it would be our client that would be affected. We would also, however, contact the NCSC and An Garda Síochána.

Chairman: Has the response been good?

Mr. Pat Larkin: We must build the structures and communication. The industry must reach out to the NCSC as much as the NCSC must reach out to the industry. Again, Cyber Ireland has produced a paper to outline a model that would allow us to build that increased collaboration. The problem for the industry in this context centres on resources and firepower. We have several open roles we cannot fill, and this is an industry-wide problem. It has been estimated that 3.2 million roles are unfilled in the sector globally, and the number is increasing. In some respects, then, even businesses wishing to grow aggressively must almost constrict the level of new business they take on.

Chairman: Would Mr. Larkin accept that the State's cybersecurity activity is grossly underfunded?

Mr. Pat Larkin: It is not just the budget involved for the NCSC. The budget for the NCSC is allocated to a leadership, regulatory, informational and advisory role and to the building of networks and co-ordination of the overall structure. Each agency and entity implements cybersecurity measures in its own right and that involves significant budgets as well. Arguably, that aspect is always under-resourced.

Chairman: Is Mr. Larkin talking about the public or private realms?

Mr. Pat Larkin: Both. It is a constant battle. In some respects, cybersecurity does not add to the bottom line. It is like insurance in that way. It is necessary to pay the damn thing-----

Chairman: Why has cybersecurity moved front and centre now? Three to four years ago, this was not common parlance. It is now.

Mr. Pat Larkin: Cyber-based crime is bigger than the illicit narcotics trade. Returns made by cybercriminals now outstrip those in the illicit narcotics trade.

Chairman: Since when?

Mr. Pat Larkin: For the last three or four years. It is a trillion-----

Chairman: It is more lucrative to be in cybercriminality than in the drugs trade.

Mr. Pat Larkin: Yes, it is. Think about how this type of crime is perpetrated. It can be done from a laptop at home and millions can be extracted. It is now a norm for the cyberinsurance industry to facilitate payouts for ransomware incidents. The mice, so to speak, are being given a crumb and then they come back for the whole cookie.

Chairman: Are these mainstream insurance companies?

Mr. Pat Larkin: Yes. The default incident response now from cyberinsurance companies is to roll out the fire brigade in the form of service providers, but they are also providing ransomware negotiators, legal and PR experts, etc., and mechanisms to facilitate payment in such ransom situations.

Chairman: What is the average amount paid out?

Mr. Pat Larkin: The adversary will try to make an estimate and highball that amount, and the negotiation proceeds from there. Payouts range from tens of thousands to millions.

Chairman: How many cybersecurity breaches are settled with cash payments?

Mr. Pat Larkin: They are settled with cryptocurrency payments.

Chairman: What percentage of such breaches are settled in that fashion?

Mr. Pat Larkin: I would say that a high percentage of ransomware attacks are settled. I estimate it could be as high as 50% to 60%. That is because the option for companies is-----

Chairman: Two thirds of all cybersecurity breaches-----

Mr. Pat Larkin: Of ransomware attacks.

Chairman: Which is what happened with the HSE.

Mr. Pat Larkin: Ransomware is only one form of cybercrime.

Chairman: It is prevalent, however, and the companies attacked are paying out.

Mr. Pat Larkin: Yes, they are. Cybercrime methods include ransomware, denial of service, invoice redirection-----

Chairman: It is not even the companies themselves. Their insurance companies are paying these ransoms.

Mr. Pat Larkin: It depends on the cyberinsurance model. Offerings in this regard are evolving. Increasingly, because of the degree of this type of crime, the cyberinsurance sector is restricting its services and the payments it makes. It is reducing this scope significantly. There is facilitation, however, because of the assumption that the only way out of such situations for affected organisations is to pay. The other option is to try to back up and recover information. In some cases, the situation is so catastrophic for organisations that even if they have back-ups and their infrastructure is encrypted, the time to recovery could be business-ending.

Chairman: How can that be overcome? How can companies fight back against such breaches?

Mr. Pat Larkin: Especially in the US, we are starting to see a model evolving where the FBI and similar organisations are tracking these criminals. Some traceability and recovery is possible through the cryptocurrency exchanges and systems, and the intention is to try to break those as financial gateways. Regulation of cryptocurrencies must increase and there must be consequences in this regard. Just fighting cybercriminals would be a major battle in its own right, but fighting nation states that are hand-in-glove with the cybercriminals and facilitating and building cybercriminal ecosystems is a much larger problem.

Chairman: Will the State have to move to abate such activities, similar to what we have done previously? Will we have to call out states involved in cybercrime?

Mr. Pat Larkin: Yes, we will have to tackle these bad cyberactors. There must be consequences for those involved. Looking at this strategically and in the long term, it is an arms race and one that is increasingly costly for commercial organisations and the private sector.

Chairman: We need something like the Geneva Convention in this area, as Dr. Scott has suggested.

Mr. Pat Larkin: The chair of Microsoft has proposed a digital Geneva Convention. It is a sound concept. From a foreign policy and geopolitical perspective, and given we have a seat on the UN Security Council, it is an agenda we should be pursuing as a global abatement solution.

Chairman: I hand the floor back to Deputy Ó Murchú because I took some of his time. He has five minutes and then we will conclude.

Deputy Ruairí Ó Murchú: I again thank Dr. Scott, Mr. Larkin and Mr. O'Reilly. I also record that Dr. Scott was one of my lecturers, and a very good one.

Chairman: Dr. Scott has much to answer for.

Deputy Ruairí Ó Murchú: Unfortunately, I was not a particularly good student. I am also aware of someone, who, by chance, after attending DCU, now works in the NCSC. I will not make an argument regarding whether he was a good or bad student either.

We have discussed a fair amount. In fairness, the witnesses have put on the record the reality of the world we live in. There are two parts to this. One is the ransomware and financial gain by criminal elements. I have heard of many companies that have paid sizeable amounts of money in this regard - €10,000, €20,000 or €30,000. I am not referring to huge companies, but SMEs. Part of the reason they paid the money is that they did not want news getting out that their systems had been penetrated. This type of criminality is also at times facilitated by rogue states. We can state clearly that Russia, in doing that, provides itself with a subcontractor outfit that can do business for it when required. We know the situation we are in now. We are an IT superpower and that means we are wide open to this sort of stuff happening.

What do we need to do? There are two parts to addressing this issue. We must deal with regular criminal cyberattacks for financial gain. Additionally, we must talk about state actors, cyberespionage and the difficulty involved with the denial of vital services. The worst-case scenario in that context is where cyberattacks transfer to the physical realm. We are accepting the idea here, in respect of protecting ourselves, that we will be fine if everyone operates the best-case digital hygiene. Someone has to co-ordinate that system, however, and be in charge of it. The NCSC has a particular role, but many gaps remain in regard to the threats we are facing. In fairness, Mr. Larkin spoke about how globally, but especially in Ireland, we must get the show on the road concerning workforce planning and ensure we have sufficient people to fill the roles that must be undertaken.

Another issue that goes beyond cybersecurity involves connected networks. Ireland has social media companies that facilitate these networks. This is sometimes the stuff of conspiracy theories, but state actors have the ability to use such networks from a disinformation perspective, which can be part of such actors' hybrid warfare strategies. I ask all the witnesses to comment on all these aspects in the few remaining minutes.

Chairman: We will start with Mr. O'Reilly. I see he is keeping Irish writers in a prominent position in his office. It is good to see Samuel Beckett and James Joyce prominently on view. His Irish roots are obvious.

Mr. Padraic O'Reilly: My father is a Leitrim man. Regarding the aspect of social media warfare, that must be countered. This also connects with Ireland wanting to get some of its agencies more proactive in how they address the public. One of the good things that CISA has done recently in the US is to talk regularly to the public. It talks regularly to the critical infrastructure sectors. The White House makes weekly announcements on cybersecurity. There has been a big public relations push. I regularly talk to reporters. It is in the news all the time and should become a part of the culture. The countering of cyberwarfare must become a part of the culture. Everyone, in some respect, is a soldier. That goes to the idea of training the requisite staff to address these issues. The cyber skills gap is profound. It is profound when I look for help in my company and across the entire country at the moment. It is a wonderful and fascinating field and it should be characterised as such to get young people interested. It is endlessly fascinating.

I work in risk management and build software that deals with risk management. It is necessary to have some idea of where one is at the moment. In the cyber world, we call it a baseline. One can consider an offensive capability but that is only a part of the picture. When we deal with companies that are trying to ward off these threats, we give them the tools of risk management. That is the ability to identify bad things, how likely they are to happen, how they might impact the company and how systems should be hardened in response. That concerns incident response.

When forensics are applied after an event, it is clear that cybercriminals are not using the most sophisticated techniques. There is a lot of spear phishing and brute force password attacks. Some of the highest profile breaches in the US were the result of not having two-factor authentication on a remote desktop protocol. It is not the most expensive thing in the world. Cyberhygiene and risk management are vital. It is also necessary to have some idea of where one's essential services sit at the moment with respect to those practices. That is going on over here in the US. Risk management came through the Strengthening American Cybersecurity Act, two sections of which deal with metrics around risk management. The problem will not be solved if it is just addressed by putting a finger in the dyke and deploying stopgap measures. It must be considered from the top down from the point of view of the governance structures. Resourcing is absolutely essential. The function of governance is to resource solutions to these problems.

Dr. Michael Scott: I will add some short, final words. This issue is not going to go away. It is going to get worse before it gets better and we need to do something. One thing I would like to see happen is a change of culture at the NCSC. That is something we can do in the short term. The NCSC needs to come out from behind its walls, interact and take on a much more public role. During the pandemic, there were many people we could talk to who were more than willing to come out and talk about viruses, vaccines and all the rest of it. We need the NCSC to come out to interact with and educate the public, which would allow us to feel comfortable and not to panic or overreact. The NCSC should be telling us calmly and seriously that we have these issues under control, that we have the expertise, and that anyone with a problem should call X, Y or Z. A change of culture at the NCSC would be a great starting point.

Mr. Pat Larkin: The State should be leader, co-ordinator, enabler, incubator and accelerator. That is the role of the State, whether it falls to the NCSC, the Taoiseach or whoever else. On Mr. O'Reilly's point, we must be highly innovative on cybersecurity. We must produce a mainstream of core cybersecurity professionals. There is a simple model that would build cybersecurity knowledge, which is simply to embed a relevant cyber-related module in all professional and academic courses. I am formerly of the Defence Forces and my former colleagues tell me they run 2,000 or 3,000 people through a career course every year. If we added a cyber module to that course, we would produce 2,000 or 3,000 cybersoldiers every year. Culturally, the organisation is asking what to do with them. They will leave. We can tell the Defence Forces that they are producing people who can defend the cyber realm, no matter the role they are in, for the Defence Forces. The same applies to lawyers, teachers, academics and public servants. Including those modules in courses would build a cybersavvy workforce and citizenry. The fundamental point is that cybersecurity needs to be a national and economic priority.

Chairman: I thank our guests. This is a matter we are going to continue to do work on. It is something that falls under our remit, although I take Dr. Scott's point about how it evolved to fall under the remit of the Department. As a committee, we have been proactive in enhancing the NCSC. It needs further enhancement and a rounded role. I thank our guests again for attending and engaging with the committee. I thank Mr. Larkin, Mr. O'Reilly and Dr. Scott for their engagement and no doubt we will be following up with them again at a later stage.

The joint committee adjourned at 4.56 p.m. until 1.30 p.m. on Wednesday, 6 April 2022.