DÁIL ÉIREANN

AN COMHCHOISTE UM IOMPAR AGUS CUMARSÁID

JOINT COMMITTEE ON TRANSPORT AND COMMUNICATIONS

Dé Céadaoin, 22 Meán Fómhair 2021

Wednesday, 22 September 2021

Tháinig an Comhchoiste le chéile ag 12.30 p.m.

The Joint Committee met at 12.30 p.m.

Comhaltaí a bhí i láthair / Members present:

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

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

National Cyber Security Centre Review: Discussion

Chairman: Apologies have been received from Deputy Duncan Smith. The purpose of the meeting is to receive an update on the review of the National Cyber Security Centre, NCSC. On behalf of the committee, I welcome the Minister of State at the Department of the Department the Environment, Climate and Communications, Deputy Ossian Smyth, and his officials. I am sorry for the slight delay in the commencement of the meeting.

Witnesses are reminded of the long-standing parliamentary practice that they should not criticise or make charges against any person or entity by name or in such a way as to make him, her or it identifiable or otherwise engage in speech that might be regarded as damaging to the good name of the person or entity. Therefore, if their statements are potentially defamatory in relation to an identifiable person or entity, they will be directed to discontinue their remarks and it is imperative that they comply with any such direction. Witnesses attending remotely outside of the Leinster House campus should note that there are some limitations to parliamentary privilege and, as such, they may not benefit from the same level of immunity from legal proceedings as witnesses who are physically present. Witnesses participating in this committee session from a jurisdiction outside the State are advised that they should also be mindful of their domestic law and how it may apply to 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 any person outside the Houses or an official by name or in such a way as to make him or her identifiable.

For anyone watching this meeting, Oireachtas members and witnesses now have the option of being physically present in the committee or to join the meeting remotely via Microsoft Teams, which is a welcome development. It shows that, like everywhere else in society, the Oireachtas is very much getting back to normal business. I remind members of the constitutional requirement that they must be physically present within the confines of the Leinster House complex in order to participate in public meetings. I will not permit members to participate where they are not adhering to this constitutional requirement. Any member who attempts to participate from outside the precincts will, reluctantly, be asked to leave the meeting. In this regard, I ask any member participating via Microsoft Teams, prior to making a contribution to the meeting, to confirm that they are on the grounds of the Leinster House campus. If attending in the committee room, people are asked to exercise personal responsibility to protect themselves and others from the risk of contracting Covid-19. I strongly advise that people employ good hand hygiene and leave at least one vacant seat between them and the others attending. People should always maintain the appropriate level of social distancing during and after the meeting. Masks should be worn at all times during the meeting except when speaking.

I call on the Minister of State to make his opening statement.

Minister of State at the Department of the Environment, Climate and Communications (Deputy Ossian Smyth): I thank the Chairman and members for inviting me to attend before the committee today and answer questions. I am joined today by Mr. Richard Browne, acting director of the NCSC, and Mr. Peter Hogan, principal officer in the Department's cybersecurity and Internet policy division.

I am delighted to have this opportunity to present to the committee on the capacity review of the NCSC, which was completed last June. When we last met, the Minister for the Environment, Climate and Communications, Deputy Eamon Ryan, and I were awaiting the outcome of

the review. I am pleased to report that the review was completed within the intended timeframe. I know that the committee was keen to hear the recommendations of the capacity review and ensure that the Government took appropriate steps to implement these as early as possible.

As members will be aware, in July the Minister obtained Government agreement to a substantial expansion in the staffing of the NCSC from 25 to 45 staff over the next 18 months, and to at least 70 within five years. The associated budgetary increase for the centre for 2022 is estimated at €2.5 million. The Government also agreed a significant package of other measures to further strengthen the capacity of the NCSC, including the development of legislation to establish the NCSC on a statutory basis with a set of formal powers and a legal mandate. These measures include: that the role of director of the NCSC should be re-advertised at a salary of €184,000, which is the deputy secretary general scale, to reflect the scale and importance of the role, and to attract experienced candidates; that the director will have responsibility for building and leading the NCSC, further developing the operational capacity and expertise of the NCSC and supporting the development of the policy and legislative framework relating to cybersecurity in the State; that a single headquarters for the NCSC will provide the required security infrastructure and capacity, and that the centre will be accommodated within the Department's new headquarters in Beggar's Bush; that we will develop a five-year technology strategy for the NCSC which scopes its internal requirements and its relationship with academia and industry; that there is a measure to recruit people to 20 additional full-time roles; and that a cybersecurity graduate training programme will be initiated by the NCSC in 2021, with four computer science graduates recruited each year on contracts of three years' duration.

I have already shared with committee a redacted version of the executive summary of the capacity review. In respect of the findings of the review and the benchmarking exercise, there are some details that I cannot share due to national security considerations both in Ireland and in those countries with which comparisons were made. I will endeavour to be as open and transparent as possible with the committee, however. Where necessary, I will ask my officials to follow up with written replies to questions.

The capacity review recognises that the NCSC has grown considerably since its establishment in 2011. The consultants acknowledged that the NCSC team had developed significant expertise and capability in a relatively brief timeframe. The consultants found that staff at all levels of the NCSC are knowledgeable and highly motivated and have a clear understanding of the NCSC's role and purpose. The consultants also remarked positively on the progress of implementation of the national cybersecurity strategy and the role that the interdepartmental committee has played in driving this work.

The consultants were tasked with charting a five-year course for the continued development of the NCSC taking into account the evolving threat landscape and the growing body of EU legislation on cybersecurity. The consultants proposed a new organisational structure for the NCSC and recommended that an incremental expansion be pursued over the coming five years. The capacity review recommends, as an initial step, that the headcount of the NCSC's operational team should increase from 25 to 41 full-time equivalent staff, with numbers continuing to grow to in the region of 50 in year 3 and approximately 70 in year 5. In that context, the Government has decided to go further in the initial expansion of the staffing complement.

The capacity review includes more than 40 recommendations which have been categorised as high, medium and low priority and which cover issues from governance to technology to skills development. The capacity review recommendations will not be fully completed for some years and there are many interdependencies within them. For example, much of the rec-

ommended technology development requires a suitably equipped headquarters facility. A clear legislative mandate is necessary for the NCSC's functions to be expanded further.

I would like to provide the committee with an update on the progress of implementing the measures that were agreed by Government in July. Working with the Public Appointments Service, good progress is being made by the Department in progressing the delivery of the increase in headcount that was recommended in the capacity review. I understand that in the coming weeks a number of open recruitment competitions will commence to recruit new staff with cybersecurity skills and experience to complement the existing team. In addition, we are availing of the Civil Service mobility scheme to redeploy staff from across the civil and public service who have an interest in the NCSC's work. We are taking a broad perspective on the skill sets necessary for the NCSC's range of functions, including stakeholder engagement, project management and compliance. The process has already begun and we are currently seeking expressions of interest.

The competition for the NCSC director, run by the Public Appointments Service, will be advertised this Friday. As was the case for the previous recruitment campaign, this will be an open process carried out in line with the established principles for senior recruitment to the civil and public service. I expect to see this competition concluded before year-end and a permanent director appointed as early as possible thereafter. The Public Appointments Service is using the services of an executive search company to assist in identifying suitable candidates. In the interim, we took the decision to appoint Mr. Browne as acting director in order to ensure that the NCSC has a full leadership team in place during this important period of transition. Mr. Browne has previously served in this area since 2014 so he was able to hit the ground running when he returned in July. His focus is in implementing the measures agreed by Government in July, and he and his team are already making good progress.

The development of the NCSC's headquarters will be managed as part of the redevelopment of the Department's offices at Beggar's Bush, Dublin 4, which are expected to be completed in 2023. The acting director and chief technology officer, CTO, have worked closely with the corporate services area of the Department and the Office of Public Works, OPW, over the past two months with a focus on the design and layout of the new headquarters. This will be an important facility for the national response to a major cybersecurity incident and, as a result, we need to ensure that it is fully equipped. There are also international standards for the security of accredited computer security incident response team, CSIRT, which will need to be factored into the design, construction and fit-out of the new facility.

While the new headquarters are being developed, temporary accommodation will be required for the NCSC and the OPW has identified a suitable location for this temporary facility. Under the supervision of the acting director, the NCSC administration and CTO teams are currently working on the design and procurement for the fit-out of this facility. Appropriate measures will be taken to ensure that this temporary facility can accommodate the NCSC as its staffing complement grows through 2022 and 2023. We will ensure that it meets the exacting international security standards for the CSIRT.

The development of a technology strategy for the NCSC is closely linked to the new headquarter project. The acting director and CTO have completed a review of the capacity review's recommendations in respect of technology to inform the development of the new strategy. The CTO has also identified a number of priority investments which are part of the Department's submission for the 2022 Estimates process.

Work has also commenced on the cybersecurity internship scheme which will complement the existing actions in the national cybersecurity strategy on cyber careers and skills. This scheme will be a priority action following the imminent recruitment rounds I referred to earlier.

Finally, in respect of the proposed legislation for the NCSC recognising the need to work in partnership with other Departments and agencies, at the recent meeting of the interdepartmental committee on the national cyber security strategy, a way forward was agreed by all members. To empower the NCSC to carry out its necessary functions, it is inevitable that the proposed legislation will provide for intelligence gathering, which will bring with it certain governance requirements as well as requirements on the legislative process. Officials in my Department are leading a consultation with relevant stakeholders which it is intended to complete before the end of this year. Thereafter, work will begin on drafting heads of a Bill which I hope to see progress through the Oireachtas before the end of 2022.

I recently attended the Estonian Digital Summit, where there was much interest in the Government's response to the HSE cyber incident and the development of our NCSC. The conference theme was trusted connectivity. I was pleased to have the opportunity to engage in constructive conversations with peer Ministers from a number of EU countries, as well as Singapore and the UK, and I also had the opportunity to meet the Estonian Prime Minister. It was clear from the conference and discussions with other Ministers that the global landscape of cyber threats is at the top of the political agenda and that concerted international co-operation will be necessary to secure essential services in the face of these threats. During my visit to Tallinn, I also met with Ireland's secondee to the Cooperative Cyber Defence Centre of Excellence, CCDCOE, and paid the centre a visit. There are great resources in the CCDCOE that we can draw on to inform the further development of our own cyber capacity, both within the NCSC and across Government. I thank the Chairman.

Chairman: I thank the Minister of State. We will now move to members. The first slot of is with Sinn Féin and I call Deputy O'Rourke, who has seven minutes. We will stick with that arrangement, with some degree of latitude, and if people need to come back in then later, they can.

Deputy Darren O'Rourke: I thank the Chairman and the Minister of State. The cyberattack on the HSE on 14 May had and has a very significant impact on services and this needs to be the fore of our thoughts when we discuss these matters and the implications for people engaging with health services. People were asking at the time how this happened, whether it could have been avoided and whether we could have been better prepared. On seeing the report before us, or the bit of it we have available to us, we can be left in absolutely no doubt that we could and should have been better prepared. The report finds that the NCSC is not fit for purpose, is under-resourced, over-tasked and its structural and legislative foundations are wholly inadequate. That is a very damning indictment. It states that the NCSC does not currently have the organisational design or capacity to achieve the objectives of the national cybersecurity strategy which was only published at the end of 2019. It states that the NCSC is under-resourced and over-tasked with regard to wider engagement with critical national infrastructure comprising in the region of 120 operators of essential services or digital service providers.

That raises very fundamental questions on the establishment and resourcing of the NCSC since its establishment. Does the Minister of State accept that previous governments have failed to adequately resource the NCSC?

Deputy Ossian Smyth: I thank the Deputy for his questions. The capacity review was ordered to assess what additional resources were needed by the National Cyber Security Centre in

the face of an escalating level of cybersecurity threats. I am sure that the Deputy is aware that the volume of cybersecurity attacks that are happening around the world greatly increased even before the pandemic but during the pandemic it is estimated that they increased approximately sixfold. In response to that, a capacity review was ordered. This was decided upon, in fact, last summer during the programme for Government negotiations when it was agreed between the Government parties that we would commission a capacity review and see what additional resources were needed by the NCSC.

That was a timely thing to do and was done long before this attack ever happened and the capacity review found that there was an escalating level of threats, that the NCSC was performing well but needed additional resources. The review recommended how those resources should be targeted, how many of each staff should be hired and how much additional money would be needed.

Deputy Darren O'Rourke: My apologies to the Minister of State for interrupting him but I am conscious of time. I hear what the Minister of State is saying but the review also stated that the NCSC is under-resourced and over-tasked and the Minister of State will not actually say those words. Do the Minister of State and the Government accept all of the recommendations, including those on staffing and restructuring? Does the Minister of State believe and can he give a commitment that those resources for staffing and for the fitting of the headquarters will be made available? I have figures here which show that the NCSC has a track record of recruiting one new staff member a year and are to recruit almost 20 extra staff members in the next 18 months. Can I have a commitment from the Minister of State that those resources will be made available and, not only that, but that these positions will be filled within the timeframe committed to and asked for?

Deputy Ossian Smyth: I thank the Deputy again. His first question is whether the Government accepts the recommendations of the report and the answer is we do. He further asks if we accept the recommendations for the additional staffing and the decision was made at Cabinet earlier this year to go beyond that level. I recommended a higher staffing complement and this was accepted. It will be a challenge to recruit additional cybersecurity staff at a time when cybersecurity threats are increasing for all countries and for critical infrastructure providers as there is a great deal of competition in the market but there is a need also for additional training and education. Part of the response to this is to increase the number of people who are being trained up at every level.

Deputy Darren O'Rourke: Is there an estimated cost for the provision of the headquarters for the NCSC for which I appreciate the requirement for specialist equipment and configuration?

Separately, what countries were included in the comparison carried out?

Deputy Ossian Smyth: The first question is how much money is needed for a new cybersecurity headquarters and there are two parts to the answer to this. First, we are building an interim headquarters to move into next year and then there is the permanent building, which will be a brand-new building which is being constructed for the entire Department. One floor of that will be used for the NCSC and will be built to the highest standards possible. On the cost of this, we tripled the capital budget last year for the NCSC, again, before this attack happened. The money provided will be dependent on the spec and what comes in on tender but there will not be a problem in providing for a "best of breed", in other words, a world-class security operation centre to provide-----

Deputy Darren O'Rourke: Does the Minister of State have an estimated cost for this at this stage?

Deputy Ossian Smyth: I do not.

Deputy Darren O'Rourke: Is it too early for that?

Deputy Ossian Smyth: It will probably be in the single-digit millions. The Deputy also asked about comparisons with other countries. There were comparisons with other European countries and with countries outside of Europe. As the Deputy will appreciate, when looking at the weaknesses and strengths of cybersecurity centres in other countries, the details are probably not something that we want to publish to any great degree. However, the purpose of the exercise is to see how we rank on that, the ways in which we need to improve and if we are up to standard in comparison with those other countries.

Deputy Darren O'Rourke: : I thank the Minister of State. It is important that efforts are made to fill those gaps as quickly as possible.

Chairman: We will proceed with the meeting in the normal way. I expect that we will have time for members to come in with follow-up questions. We will now move to the Fianna Fáil slot. I call Senator Horkan, who has seven minutes.

Senator Gerry Horkan: I thank the Minister of State for his opening remarks. It is a fairly sorry state of affairs when one considers the amount of money, time and effort that had to be invested. It would have been much better if the HSE could have spent the money and time doing other, more productive things than trying to firefight the crisis that arose. From the Minister of State's initial review of what happened, were there are gaps in what the HSE was doing and could it have been doing things better? Has it learned lessons in his regard?

Deputy Ossian Smyth: It is early days to say that. Part of the response to this is that two reports have been commissioned. The HSE commissioned a report for its board from consultants. There is also a report into the origins of this and exactly what happened. It is being compiled by an international security company, Mandiant. That will also provide information. At the same time, an investigation by An Garda Síochána is taking place. I am limited in what I can say. An Garda Síochána knows when the network was penetrated and how it happened. Much forensic information has been gathered by An Garda Síochána. I expect those reports to be published shortly. They will be used to inform the HSE of the lessons that should be learned from this attack.

Senator Gerry Horkan: Are there measures in place to share the information in these reports? The Minister of State does not have to tell us everything that happened. The information is obviously sensitive. We do not want people who are carrying out these kinds of attacks to know how they are being stopped from happening. Will that information be shared with other Departments? My concern is that if this can happen to the HSE, then it can happen to the Revenue Commissioners, the ESB or many of the large entities that all of us, as citizens, rely on every day, such as the Department of Social Protection. The health system ground to a halt. The simplest tasks at the HSE had to stop being done. They were being done differently, more slowly and more inefficiently. We talk about energy crisis happening for other reasons, but the last thing we need is for the ESB, the Department of Social Protection or Irish Water to be attacked. Will the NCSC or the Department make sure that all of the other agencies of the State have learned from what has happened in order to ensure that we do not have a similar situation

befall one of those agencies?

Deputy Ossian Smyth: The NCSC has a policy of trying to publish as much information as possible on its website. This is open communication. Most of what is being done is not secret and does not need to be hidden from people. Most of the information about how to protect yourself in terms of cybersecurity is open, public information that everybody can read about. If one goes on the NCSC's website, one will see that it releases information all the time. It has different levels of release. There are releases that are issued to all of the public and there are others that are issued directly to operators of essential services or to people who run critical infrastructure. In general, the things that need to be done to protect oneself against cyberattack are fairly straightforward and well known. There is a set of instructions for what one has to do to protect one's network. Those guidelines for critical infrastructure providers are published on the NCSC website. They were not published in reaction to this attack. They have been there for years. These are 2019 guidelines on how to protect one's critical infrastructure network. Anybody can read them. While an attacker could read them too, they start from simplest things, such as using two-factor authentication, having complex passwords and so on. This is a whole guide on the things that one needs to do to protect oneself. The information about this is to be shared in as public and transparent a way as possible.

Senator Gerry Horkan: I thank the Minister of State for that. It is good to know. We should be publicising the fact that all of that information is available. A question arises in that context, however. If that information is there and it was there before the attack, did nobody in the HSE look at the website? Did nobody in the HSE take on board these published guidelines? The Minister of State says that this is simple, straightforward stuff, but we have had an attack on the HSE that cost us millions of euro, both in outlay and in terms of the lost productivity of people doing things that they would have been able to do more efficiently otherwise. Was nobody in the HSE doing what the NCSC website was telling them to do? Why did it happen?

Deputy Ossian Smyth: There definitely were people in the HSE who were working on cybersecurity. They were in a much stronger position a year ago than they were two years previously. They had been working closely with the NCSC to improve their security. They had been carrying out risk assessments. It is an enormous and complex organisation, however. There are 100,000 staff, one third of whom are contractors. The organisation consists of many independent bodies, health agencies and different levels of private and public medicine, brought together. By its nature, it is a complex organisation.

The healthcare sector is a uniquely difficult sector to protect. Part of the reason for that is that people who are working in healthcare are dealing with life-and-death situations all the time. It is hard to say to somebody who is trying to make a life-and-death decision with a patient that they need to have a better password in order to look at the patient's file. This is a problem with healthcare organisations around the world.

While it would be easy to criticise HSE, you have to look at the organisation at that time. Earlier this year, it was under enormous pressure, and not just from the pandemic. It was trying to get the vaccines out as quickly as possible. Its staff were working from home. Between those factors, it was in a uniquely vulnerable position. I can say that it has made enormous progress.

From the point of view the NCSC telling people about the risk. If one looks at the centre's website, on 30 October 2020, long before any attack like this, it issued a warning about the possibility of ransomware attacks on the Irish healthcare sector. That was based on information from the FBI. Again, that is not a secret. One can find it on the website if one looks at 30

October 2020 to see the release and what is stated. It gives recommendations for what should be done to protect against that kind of situation.

Senator Gerry Horkan: I am not trying to engage in any kind of blame game. I appreciate all of the work being done by the 100,000 people involved in the HSE. However, their lives became far more difficult after this attack than was the case before. We are probably all guilty of not changing passwords as often as we should or of making them more simple than they might otherwise be. I wonder if all of the people in the HSE have changed their passwords at this stage? Have they done the most simple tasks? Is it the case that they are not sharing passwords, that they are not sticking passwords at the top of their screens and that they are not doing all of those things we have all been told not to do? Clearly, the challenges and problems that were presented following the attack far outweigh the complexity of having to change a password, annoying as that may be.

Deputy Ossian Smyth: They have made enormous progress. They had already made enormous progress before the attack. Obviously, the attack has brought into focus the importance of the HSE's IT infrastructure. We saw happened when its information systems were down. Hospitals were able continue to function, but everything was much slower. I understand that, for example, people in accident and emergency departments were frustrated by having to wait ages to get lab test results or look up information about patients. The latter leads to worse patient outcomes. If anything, it was a demonstration of the value of IT and of the importance of having information about patients and the illnesses they are suffering immediately to hand.

Progress had been made up to that point and much more progress will be made into the future. Many of the systems in the HSE have had to be rebuilt from the ground up and a lot of areas of HSE estate that were not thought of very often, such as parts of the 2000 systems that were not very prominent, are now better understood. One of the principles of cybersecurity and of trying to protect any organisation is that there is a complete list of all of the things that need to be protected, that there is a full inventory and that one is familiar with having to build those systems from the ground up whenever that is needed. The HSE is in a much stronger position as a result of that and it is a much more resilient organisation now than it would have been six months ago.

Senator Gerry Horkan: I thank the Minister of State. He is uniquely placed from his previous career in that he probably knows more about the healthcare system and IT systems than anyone else in Parliament. It is good, therefore, that he is the person being tasked with this role. I wish the Minister of State and all of the people in the NCSC the best. Hopefully, when further information is published and made available, we will return to that topic and the Minister of State might be available to discuss it. It is important that parliamentarians and the public are aware of how complex this is and how many people are trying to resolve it. We are all getting text messages about parcels with links and so on lately and it is important that we are all more cyber aware.

Deputy Ossian Smyth: I thank Senator Horkan.

Senator Jerry Buttimer: I thank the Minister of State for being here and for his comprehensive presentation. I would like to make a specific point. I have to give the Minister of State great credit. I have grown to admire him because he has a huge depth of knowledge of his brief, which is refreshing to those of us on the periphery of this debate. Reference has been made to the cyberattack on the HSE and in particular, to the repercussions and knock-on effect it has had on waiting times and on dealing with the backlog of appointments. I know it might

not necessarily be the Minister of State's brief but is there a plan on behalf of the HSE to tackle those waiting times?

Deputy O'Rourke made reference to Government funding for cybersecurity, and it was reported on in the *Irish Independent* last week. There seems to be an issue with funding for and investment in cybersecurity. The Minister of State said there was a sixfold increase in same since the pandemic began. What are our plans to increase capacity in cybersecurity and prevent further attacks?

Deputy Ossian Smyth: I will start with the question about waiting lists. Waiting lists are an operational matter for the HSE and a strategic matter for the Department of Health. They are outside of my remit to some extent. From an IT point of view, a waiting list attaches to a particular consultant and consultants are attached to particular hospitals. This means that there are multiple waiting lists around the country that are not really connected with each other. It is difficult to say, for example, how many people are on multiple waiting lists and how many unique people are on all the waiting lists that are in the country. I know the Sláintecare team and the HSE have been looking at ways of unifying those waiting lists to get some idea of who is on more than one waiting list, whether people should be transferred from one list to another or whether there should be shared lists that go outside of a single consultant. There is an IT aspect to waiting list management and there is also the question of how to keep track of whether the people on waiting lists are still waiting for operations and whether they still require the service. The HSE made great progress in making sure that people who are on waiting lists still intend to have the procedure they are waiting for. The Senator is right that it is outside of my area.

On funding, it is easy to think that money is the solution to all of the problems. That is not the case in this situation. The HSE had its IT funding doubled in recent years. It also had a massive increase in staff. As I said before, the funding for the NCSC had tripled in the previous year. A great deal of money is available. I had no sense when I was speaking to the Minister for Public Expenditure and Reform or when we presented our memorandum to Cabinet that the Government was not willing to spend whatever it took to secure the HSE and national cybersecurity assets. Money is not an issue and we will have the best security operations centre and headquarters for cybersecurity that will be as good as any other country in Europe. It is not a financial thing; it comes down to a cultural approach to the priority that is given to cybersecurity and the seriousness with which it is taken. If one looked over previous meetings of the Joint Committee on Health and saw how much time was spent on discussing cybersecurity, I would imagine it was quite small compared with other issues because there are so many other pressing life and death issues within health. Having political support for cybersecurity might be more important than having a budget and it will not be constrained in any way by a lack of money.

Senator Jerry Buttimer: That is a good point. I know we have been moving towards this point . As the Minister of State indicated, however, it is about unifying waiting lists and having patient identifier numbers for hospitals and consultants. It is important that we learn from this and all of Government must ensure that the waiting lists are tackled. I commend all those who have been involved and who have worked so diligently since the attack, including the members of An Garda Síochána who have been able to mobilise against the people who attacked us. I thank them for that and I thank the Minister of State for being here.

Deputy Ossian Smyth: The Senator is right. There was an enormous patriotic response from security researchers, members of the HSE and medical staff. They assembled in an emergency room in the ballroom of the Citywest Hotel and they worked day and night for weeks on end until they were exhausted to try to fix these systems because they knew it was a life and

death situation. I went to visit them out there with the Minister for Health, Deputy Stephen Donnelly. What they did was heroic and I want to sincerely thank them all for that.

Deputy Ruairí Ó Murchú: I thank the Minister of State. A number of members have already dealt with the fact that the NCSC was under-resourced and overtasked. We have a to-do list and we need to ensure that is completed and that all necessary resources are brought to bear.

I want to deal with the executive summary. Recommendation 5 states:

> Ensure legislation formally and fully embeds NCSC within the wider national security and intelligence machinery of Government as the National Technical Authority for the cyber domain and focuses its mission on the dynamic detection and disruption of sophisticated threat actors.

Could I get some information on exactly what the national technical authority will look like? We all said that the NCSC might not have had the required resources to do its regulatory and preventative work and to deal with critical infrastructure organisations and that there was a need for more. Is that the role the national technical authority would fulfil? The Minister of State already mentioned intelligence gathering but are we also talking about the need for knowledge of disruption and protection and, for the want of a better term, strike or counterstrike capacity?

I refer also to the relationship between the NCSC and the Defence Forces and An Garda Síochána. What is envisaged in that regard.

Deputy Ossian Smyth: This point is about providing a statutory basis for what we do. We have the rule of law. We are dealing with people who are criminals. We want to ensure that what we are doing has a sound legal basis and that we are not descending to their level. The idea is to ensure that we have an absolutely solid legal basis for everything we are doing and that people responding to the NCSC know that the organisation has the right under law to make requests, issue compliance orders, etc. In practice, the NCSC is the national technical authority on cybersecurity and cybercrime. The legislation that will be brought forward will underpin that position. It will provide strategic information to everybody in Government in that regard. If anybody is presented with a decision to make, then he or she will be able to see that the NCSC is clearly and legally the central authority in that regard.

Deputy Ruairí Ó Murchú: Will additional powers be provided?

Deputy Ossian Smyth: The heads of the Bill have not been published yet. There is a reference, however, to whether we need to provide for some intelligence capacity in this regard and some legal underpinning to that. It is not possible to gather information without having some kind of legal basis to do that in the first place. The role of the NCSC is to disrupt attacks. I refer to a situation where a cyberattack may be under way and, in that context, determining what it might be possible to do to disable the attackers. That is the nature of cyber defence as opposed to cybersecurity. We can think of cybersecurity as the measures taken to prevent an attack from happening in the first place and cyberdefence then as what is done when an attack is under way and someone has been identified as an adversary or opponent.

Deputy Ruairí Ó Murchú: That would be where defence meets offence I imagine.

Deputy Ossian Smyth: I do not think there is any recommendation for offensive capacity. There is a line there. I would not, however, rule out the ability to be able to disrupt an attack. It is a different situation when you are being attacked and you need to defend yourself and dis-

able the attacking party. It is a different context from getting up in the morning and attacking somebody else.

Deputy Ruairí Ó Murchú: I accept that. That is why I used the term "counterstrike", which would be carried out in the middle of an attack. I do not mean that we should be engaging in cyberwarfare when it is not necessary. However, we should definitely ensure that we have the full capacity to protect ourselves.

What relationship does the Government see the NCSC having with An Garda Síochána? The Garda is tasked with finding criminals and dealing with international allies when going after people. In addition, what relationship would there be with the Defence Forces, which would or should have a certain capacity concerning cybersecurity as well?

Deputy Ossian Smyth: The role of An Garda Síochána is clear. The members of the force carry out criminal investigations. This is another area where many crimes are now starting to occur and where it will be necessary for the Garda to operate in. My experience is that the members of the force are very skilled in this area. At least one garda is posted in the NCSC. The Garda carried out forensic analysis of the HSE cyberattack, co-operated with other police forces in Europe and globally and managed to get information about the attackers. The force has made progress on this case. It is not going to be a case, though, that one national police agency takes out one criminal gang, especially when gangs are spread throughout multiple jurisdictions. A concerted response will be required, through bodies such as Interpol, etc., to allow the co-operation between different police forces that will be required to enable long-term surveillance of suspects and to prevent potential attackers from being able to carry out their attacks. The function of An Garda Síochána will relate to aspects such as gathering evidence and forensics and then issuing orders to disable bank accounts, for example, or to interrupt the flow of payments, take down websites or deal with anyone in a jurisdiction where members of the force can operate.

Deputy Ruairí Ó Murchú: What will be the interaction between the NCSC and the Defence Forces in future?

Deputy Ossian Smyth: Again, the Defence Forces have one person posted within the NCSC. There is co-operation with other military intelligence people and-or with people working in cyberdefence to protect military installations from being attacked. Cyberattack can, in addition to land, sea and air attacks, be seen as a fourth vector of attack. Any modern military force must have a defensive capacity in this regard. When I was in Estonia, I met one of our soldiers working in that area.

Deputy Ruairí Ó Murchú: The main work is that of a preventative nature that must be done by the NCSC. I refer to ensuring that everyone follows best practice, that we have fireproofing in place and that we no longer have the weaknesses such as those that, for many reasons, existed within the HSE. Regarding this increased capacity, I assume that we are reasonably happy with whatever the interaction is now with critical infrastructure organisations from the perspective of avoiding similar ransomware attacks.

I also appreciate that we are talking about ensuring that there is a decent relationship with academia and industry. I state that because several experts said that there are people with expertise in many colleges, including in Dublin City University, DCU, where I went. Those people have the required expertise and provide specialised courses in respect of cybersecurity, cryptography and all the other aspects and they probably should have been engaged at an earlier

stage. Once we can ensure that will happen in future, however, it will be useful.

Deputy Ossian Smyth: The involvement of people from academia is critical because they are at the cutting edge of knowledge which is constantly changing. We need people who are researchers and keeping up with the changing technology. We also need to have third level institutions educating people who will be the cybersecurity staff of the future. Many academics helped us to deal with the cyberattack on the HSE. Cyber Ireland is a formal organisation which connects the Government, academia and industry. I will be speaking at its conference, which is imminent.

Deputy Ruairí Ó Murchú: Will the Minister of State comment briefly on interaction with the critical infrastructure organisations and how that is going in respect of auditing and providing protection?

Deputy Ossian Smyth: A European directive tells us that we must have a list of critical infrastructure organisations or operators of essential services and keep track of what is included on it. It is not always that obvious. Electricity and water service providers are included, but we might not think about many other essential parts of the economy in the same way. What we do is to provide those organisations with information. We get them to do risk assessments and we can audit those organisations as well. In addition, we have the legal power to request information from those organisations, and we have done that. We can also issue orders for compliance or enter their facilities. Generally, we do not need to invoke those powers. We have a co-operative relationship with those critical infrastructure providers because it is in their interest to ensure that they do not get attacked. The NCSC is there in a supportive capacity to help those providers to protect themselves.

As the Deputy said, 90% to 95% of this work is concerned with prevention. The glamorous end of activity in this area arises when there has been an attack and people come in to help. Situations like that are similar to when there has been a fire and then the fire brigade arrives. To continue the analogy with fire protection, however, the majority of the work must be done at the preventative stage. It is much more effective to spend money on preventing an attack happening than on trying to resolve an attack after it happens. Who is responsible for doing that work? It is the infrastructure providers themselves. In the same way that the fire brigade does not stop people having fires in their houses, it is useful-----

Deputy Ruairí Ó Murchú: I appreciate that, but I am getting the evil eye from the Chair in respect of overstretching my time. I hope that somebody during further questioning will address the issue of the Sensor programme and the point made in the executive summary concerning the development of a baseline security standard.

Chairman: I have had a chance to digest the executive summary and wish to make a couple of comments. I think it would be a fair observation that the FireEye review is very much summarised. On the last page of the executive summary the review states:

> In terms of wider engagement with Critical National Infrastructure (CNI), NCSC is currently under-resourced and over-taxed providing advice to *c.*120 Operators of Essential Services (OES) or Digital Service Providers (DSP), albeit the staff we spoke to were well-informed and highly motivated.

FireEye was generally complimentary of the staff in the current NCSC but the overall view that I got from the report is that the centre is not fit for purpose. The main reason for my com-

ment is that one of the recommendations is the establishment of a cross-government task force with representatives. Has it been formed? Another recommendation is to develop a strategy for NCSC and provide it with a properly established and appropriately scoped mandate. In my view, FireEye basically states that the current strategy may not be fit for purpose. In fairness, the Minister of State stated, of his own volition, that the centre needs to be put on a statutory footing.

The Department will seek to bring in changes over the next year plus. Are we at a point where this work needs to be fast-tracked? I accept that there are issues about drafting legislation. Another recommendation is to provide the NCSC single headquarter facility. I am not certain that one floor within the Department can be categorised as such and ask the Minister of State to comment.

The report further states:

> We recommended consideration is given to separating the Technical Authority and Competent Authority roles as part of this process ... A significant burden rests on NCSC to deliver against the strategy and, based on our review, it does not currently have the organisational design or capacity to achieve all of the objectives. A dedicated budget should also be assigned to achieve the NCSS's objectives.

Finally, the report recommends that the NCSC reduce its reliance on external capabilities and very much prioritise its internal capacity. Has the NCSC lost staff? The Minister of State mentioned boosting retention. Is the NCSC losing top-level staff?

A sum of €100 million was lost due to the cyberattack on the HSE and there was also a cost in terms of the impact on appointments. There is a report in one of today's newspapers that 30,000 of the computers in the HSE still use Windows 7 yet Microsoft came forward and declared that it did not provide security support for Windows 7 from 2015. When will there be a swap over to using more modern software?

I welcome the fact that the post of Firector is being advertised now and has a salary of €184,000, which is very much in keeping with the views of experts in the area who have come before us. The recruitment campaign is being run by the Public Appointments Service. Does the service have the expertise to interview such a person? The cyberattack on the HSE took place in the middle of Covid and, let us be honest, there was a period when things got very hairy. Now that we have reached calm waters do we not need more based on this report?

The report was interesting and never criticised the staff and declared that they are very competent and very good. However, the report is highly critical, stating that the NCSC is not fit for purpose and that it needs its own dedicated budget. How big will the budget be?

The report refers to separating the regulator's post from the advisory one, and having a stand-alone headquarter. What I have in mind is that over the next two years we would see a fit-for-purpose NCSC and have stand-alone legislation in place. To bring the legislation forward would very much concentrate the minds on what should be in the centre.

The executive summary is pretty direct because it says: "However, legislation that gives "statutory legal vires" to the full operation of cyber security capability ... is critical for an effective future operational posture." In fairness, the Minister of State has stated that and I would like him to address my points. The devil is always in the detail and the detail in the report, from

what I can see, states that the current NCSC is not fit for purpose structurally. The staff are very good and performed exceptionally well under difficult circumstances. There appears to be an indication that the NCSC is losing staff. Is that the case? Is it possible, given this work is so important, to make this a two-year plan rather than a five-year plan?

Deputy Ossian Smyth: I thank the Chair. One must look at this in the context of a sixfold increase in cyberattacks in the past two years. Any organisation that faces a sixfold increase in its workload will without doubt be challenged and it cannot magic skilled staff out of nowhere no matter how much money is available. The report absolutely did not say that the NCSC was unfit for purpose but that it needed more resources. Of course, the NCSC needs more resources because the load of work and attacks that it must respond to have increased dramatically and suddenly.

Chairman: The Minister of State may have misinterpreted what I said. The report itself was very complimentary to the staff in the NCSC but certainly pointed out deficiencies in its structure, that the centre did not have legislation to underpin its operations, did not have a single headquarter facility, and had both advisory and regulatory roles. The report said that the staff are fit for purpose but structurally the NCSC, in its current form and in terms of what we will face in the future, was not fit for purpose. Is that a fair comment?

Deputy Ossian Smyth: I do not think that it is fair at all. I have read the report and really do not see it saying that the centre is structurally unfit for purpose but certain recommendations were made. We knew that the NCSC needed more resources in response to an escalating threat and escalating workload. That is why we commissioned the report to see where should the money be spent and where should the resources be directed. I absolutely agree that the centre needs a new headquarter building and new physical facilities to accommodate all of the new staff.

The Chairman asked whether a floor of the Department would be sufficient; he did not say that it is not sufficient. In fact, the space will accommodate 100 staff. We have examined in great detail what a security operations centre for a NCSC looks like in a number of different countries and specified that we wanted the best in class. So there was not a constraint about saying let us get something that is mid-market. We wanted to get the best that we could get and the long-term future is the headquarters facility. In the near future, we will redeploy staff who are there at the moment to a temporary building. I have talked directly to the staff. I have asked them if they feel they are getting what they need, that there is a problem with morale, or there are any issues they wish to address with me. They are saying "No".

The Chair mentioned lost capacity and losing staff. Every organisation has a certain degree of churn, of people who come and go. Sometimes that is an indication of success within an organisation. If you go into an organisation and you develop great skills, you then have that option to move into the private sector or towards some other organisation. You have on your CV that you are somebody who was involved in national security and in protecting your own country at the highest level. Because the centre has such a good reputation, that is something very positive, and it is one of the reasons people want to work at the NCSC and that it does not have difficulty attracting quality staff. Again, from talking directly to the staff, that is the feedback I get from them. The fact some people come and some people go is normal within any organisation. Having fresh people coming in is a good thing. Having the perspectives of people coming from the Army, the Defence Forces, or An Garda Síochána are all positive things that help out.

The Chair also mentioned Windows 7 and the fact there are thousands of computers in the

HSE that are still running Windows 7. If possible, one of the things you should do as part of your security hygiene is to have the most up-to-date patches on your operating system, all the updates that should be on your phone, and, where possible, you should not be using bits of software that are out of date. However, that is just one line of defence. That is part of what you should do. Like with the coronavirus where you should wear a mask, wash your hands, and stay two metres away, none of these things on its own is enough to protect you from an attack, and none of those things on its own is the reason you got attacked. The HSE was not attacked because some computers were running Windows 7, and it would not have been prevented if the computers had all been upgraded. That was not the problem alone. It did not help, but it certainly would not have prevented the attack from taking place. I can tell the Chair that definitively. I can also say the HSE was well aware that this was a risk. Richard Corbet, who was the chief information officer, took useful steps to minimise and mitigate the risk of running Windows 7. For example, he firewalled off those computers to one section of the network and added virus protection software. We do have a-----

Chairman: Are you satisfied with the system in the HSE at the moment? It includes these 30,000 computers running the Windows 7 operating system? Are you satisfied these are fit for purpose in terms of dealing with cybersecurity at this time?

Deputy Ossian Smyth: All of those machines will have to be upgraded at some point. Some of them are connected to very large, expensive legacy pieces of hardware, such as MRI machines or X-ray devices, which cannot cope with the newer versions of Windows software. In a large portion of the cases, perhaps half, that is the reason the Windows 7 computers are there. That involves either the manufacturer of the machinery upgrading its systems or else, when it is time to replace the X-ray or MRI facility, the replacing of the client machines also. However, you can take mitigating actions to prevent against it. Windows 7 is one risk of many. It is not the sole reason this attack happened. Certainly, upgrading software across the network, including Windows, is one of the things that should be done, but there are many things that have to be done-----

Chairman: We have 30,000 computers in the HSE operating Windows 7. Is there a need for a strategy within the HSE to replace those as quickly as possible with new, up-to-date systems?

Deputy Ossian Smyth: I am sure that is something Mr. Paul Reid is looking at. I think that was part of the Estimates, that Mr. Reid mentioned a figure of €100 million for the remediation of his network. Certainly, part of that will refer to Windows 7. They are well capable of doing a strategy and having an upgrade path. However, there is too much focus on upgrading the Windows 7 computers. It is understandable, but this on its own will not prevent a cyberattack. The upgrading certainly should happen in the context of a number of other actions that have to be taken to protect the network. However, it is not the only action and neither is it sufficient on its own.

Chairman: What budgets have you in place for the NCSC? Have you at this stage come up with figures for the annual budget? It is clear in this review, which looks to me to be a very good, comprehensive review, so what funding is required for next year and for the next five years per annum?

Deputy Ossian Smyth: Part of that will be decided in the coming weeks in the budget discussions. There have been estimates of what was needed for this year. There was a large increase in the cybersecurity budget last year. Overall, the NCSC's budget is a small portion of the cybersecurity expenditure to protect the State. All the money that is spent on cybersecurity

to protect Ireland's national infrastructure is being spent in each of the critical infrastructure bodies and by staff who are employed in them. I go back to the analogy of the fire service. If you asked how much money does it cost to prevent buildings in Ireland from catching fire, that is not the budget of the fire brigade. Most - nearly all - of that money is spent on fire prevention. The moneys and budget are spent by the-----

Chairman: I accept all that. Do you accept all the recommendations of this review by FireEye?

Deputy Ossian Smyth: Yes, I do, and the Government accepts them as well.

Chairman: Are you going to implement all of those recommendations?

Deputy Ossian Smyth: Yes, we are.

Chairman: This deals specifically with the NCSC. At the end of the day, I know you are saying it is not all about money, but to a certain extent staff cost money. If I am correct, the budget for 2021 was €2.5 million. What will the budget be for 2022?

Deputy Ossian Smyth: There are two parts to it. There is a capital budget and a current budget. The total budget between capital and current was approaching €7 million. For next year, 2022, that will be the subject of discussion with the Ministers for Public Expenditure and Reform and the Environment, Climate and Communications, Deputies Michael McGrath and Eamon Ryan, respectively, who will agree how much money will be allocated to the NCSC. However, this money in the context of protecting us, whether it is €7 million, €10 million or whatever, will not be an issue up for dispute. What will be allocated for cybersecurity and the NCSC will be what is required, what is needed, and what is capable of being spent. The money is not a constraining factor. I honestly think that money is a red herring at this stage.

Chairman: There is an element of that, but money is still important to run any centre. On that basis alone, do we need a NCSC at all? We do. It is vital. That is why we have this review carried out. It does involve money.

Deputy Cathal Crowe: I apologise for being late, as I was on other duties in the Dáil Chamber. It is great to be back here. We can juggle all of that again, which is great. I would like thank Pádraig, Anthony and all the team here who have allowed this committee to function well on a virtual basis over the past year.

I thank the Minister of State for being here with us today. Many people did not know that there was a NCSC until this year, when we needed to know. We have all been alarmed at what happened with the cyberattack. It had a devastating impact on front-line healthcare delivery because of how it got into the inner bowels of databases held by the HSE. We are talking about capacity to withstand cyberattacks in Ireland, but what led to it in the first place was probably a lack of capacity. We were somewhat akin to a Ford Fiesta chasing a supercharged car down the motorway in a police chase. We were lagging way behind. Now the Minister of State has an important job. He is the right person for that job. We have looked at his CV. He is equipped with skills to lead this out and he now has a review which he has said he will implement, and that is good. It is all very good.

Lack of capacity, is what got us in trouble. I am concerned, without being a cybersecurity expert, that where we are going may still leave us short of capacity. The budget we will spend on cybersecurity is one 1,000th of what is spent in the UK. The UK will spend approximately

£2 billion and has 1,000 staff. We will get ourselves, if I understand the executive report correctly, up to 70 staff over a five-year period. Cybersecurity does not follow international boundaries. We are vulnerable. The fact that we have been attacked this year probably shows the criminal underworld that Ireland has a bit of a soft underbelly insofar as attacks are concerned. I am really concerned. While we are now talking about building capacity and giving the Department money to increase and increase - and the Minister of State has a tough job to do and he will do it right - are we getting far enough? We have counterparts in Europe that have been taking the lead on this for many years. I made the point at this forum just a few months ago that Ireland is militarily neutral - that is a fact - but I do not think cybersecurity necessarily comes into the realm of neutrality. If there is capacity we can have in aligning ourselves with other European nations or indeed the UK to protect ourselves from a cybersecurity point of view, we should do that. Will we have enough capacity? This concerns me hugely. The UK will have 1,000 times more money invested in its system. It will have multiples of staff dedicated to fighting this. I just do not want us to be laggards. I want the Minister of State to say he is in talks with European counterparts on having an alliance in Europe to combat this.

Deputy Ossian Smyth: The Deputy said the attack happened because of a lack of capacity. I want to see the two reports that are coming out before I make a decision on the view I will take on what caused the attack. I will allow that time to see what happened. The Deputy mentioned the UK and its £2 billion spend. There is also the United States. The Deputy has to accept that those countries, with their enormous intelligence-gathering capabilities, Government Communications Headquarters, GCHQ, and so on, were still subject to the same kind of attacks as we were. The Colonial Pipeline attack cut off fuel supply to three US states. There have been huge attacks on the United Kingdom as well. I met with the UK's digital Minister to discuss that a couple of weeks ago. They have not been protected by having this enormous spend. When we compare how much money is spent in Ireland with how much money is spent in the UK on cybersecurity, we have to make sure we are comparing the same thing. The £2 billion is not the budget for the UK's National Cyber Security Centre at all. I do not know what its budget is, but I think the £2 billion figure includes the cybersecurity spend across a range of Departments and on GCHQ. Ireland does not have the equivalent of GCHQ and does not intend to have it. We are not trying to monitor all internet traffic coming in and out of Ireland, to check everybody's emails and to go through everybody's phone calls. We do not have that ambition and that is just not part of our strategy. We have a completely different set-up. We could make comparisons but they would have to be fair comparisons. We would have to compare apples with apples rather than this spend so-----

Deputy Cathal Crowe: Will the Minister of State build capacity with his European partners?

Deputy Ossian Smyth: I do not have the final report stating what caused the attack. Other countries which had a far larger spend or a far broader security apparatus would be subjected to the same kinds of attacks. When the NCSC warned that there could be a ransomware attack on Irish healthcare, that was in response to 16 US hospitals that had been taken down by ransomware attackers, so it is an increasing problem-----

Deputy Cathal Crowe: I do not know if the microphones are working. Will the Minister of State build capacity with other European nations? Ours is a small country. This is not a bottomless pit into which we can keep throwing money. Will he build cybersecurity capacity with other European nations? I do not think we are neutral when it comes to cybersecurity. We are when it comes to our armed forces, but here is a battle we will face every year, and we should

lean heavily on neighbours and other European countries. Will the Minister of State do that?

Deputy Ossian Smyth: Yes, absolutely. This kind of attack is easy to originate. You can originate it from any part of the world and direct it suddenly from one continent to another. You cannot defend against it without co-operation, so it absolutely requires co-operation between like-minded nations to deal with it. During the response to the ransomware attack on the HSE, we were contacted by the Polish authorities, who had been attacked by the same group, and they shared very useful information with us. We worked with the New Zealand authorities. There is a lot of European co-operation and also co-operation between countries that are in NATO and countries that are not NATO members at every level, including police force level. That will continue to happen. We will have the capacity to do it, and that is what the capacity review is all about. It is about saying what resources we will need each year for the coming five years to achieve this. Our response to that report is to go beyond it and say: "Yes, we accept this and we will put in more resources than you recommended."

Deputy Cathal Crowe: I ask for the Chairperson's forbearance. I have just one other minor question to put to the Minister of State. Eighteen months ago, before my election to the Dáil, I was working in an outpost of government, namely, a small rural school - not too small, I should say. We fancied ourselves as a growing school getting a bit bigger. We were growing all the time.

Chairman: The area is urban at this point.

Deputy Cathal Crowe: Small village, big school. What we are talking about here is essential command of cybersecurity, whereby the Government will build resilience, and rightly so. However, when you get out beyond the HSE, the Houses of Parliament and all the Departments based here in Dublin, there are schools dotted right throughout the country, local healthcare centres managed by the HSE and small rural Garda stations. Eighteen months ago, I worked in a classroom in one of those schools. There was a computer with Windows XP installed on it. That computer would sit in a classroom. The teacher might change each year because we could be moved up to sixth class or down to junior infants or anywhere in between, so a different person would come in. Some of the computers in primary schools would not even be password-protected. Our school had a regime for that but many schools would not. Those computers in some ways are probably not too different from what the HSE has. There would be a whole plethora of reports relating to a child's abilities or psychological needs. There could be comments relating to discipline, their attainment in tests, standardised and non-standardised - a whole litany of information that is relevant to the teacher but which, if it got beyond the realm of the classroom and out into the public domain, would be pretty upsetting to students and parents, who would take huge offence at the school. What I am getting to - and our Chairperson alluded to this just a moment ago - is that if the HSE has 30,000 PCs that have Windows 7 as their operating system. I am in a position to tell the Minister of State anecdotally that the schools around Ireland have antiquated laptops and computers, a lot of them not properly protected whatsoever. That is a matter of real concern for me. It concerns me that we will have essential command of robust cybersecurity but then, when you go down to the tentacles and go out of the spokes of the wheel to all those small schools, Garda stations and health centres, there just is not that protection. It is fine having "mothership government" protected, but I do not think that protection will be there. I am not convinced that 70 staff working centrally for cybersecurity across a five-year period will have the capacity either. The arms and the tentacles of government invested very heavily in freedom of information, and there is a freedom of information officer in pretty much every public body and they are robustly protected. However, we really

need to see this capacity built not just centrally but to all those schools. How will the Department do that? That is what I would like to know.

Deputy Ossian Smyth: The Deputy is absolutely right. There is no intention to try to provide a central protection for all State bodies from 70 people working in Dublin who will offer some kind of centralised support across all these organisations. It has to be distributed. Most of the effort and work to protect people will have to happen in a distributed way at the site where people are trying to protect themselves, that is, at the hospital or at the school. That requires information, education and so on. To give the Deputy a concrete example, next month is European Cybersecurity Month and a programme of events has been planned, targeted at schools. A new transition year module on cybersecurity has been developed and is being piloted this year in order that students in their fourth year of secondary school will learn those skills. The Garda also provides information to the public on protecting themselves from a basic cyber-hygiene point of view and on learning how to protect themselves from that kind of attack. The Deputy is correct that it has to be distributed and it cannot be done in a centralised way. It cannot work that way. There will not be somebody sitting in an office in Dublin protecting you from being attacked. It has to go out to the furthest leaves on the tree.

In my other role, I am extending broadband to every primary school in Ireland by the end of next year. I am well aware that Internet access for schools is a critical part of education and that schools need to be protected. They are educational facilities and are capable of upskilling and learning what they need to do to protect themselves from a cyberattack in the same way they learn to protect themselves from a fire or other natural disaster.

Chairman: I will move to Senator Craughwell of the Independent Group. He has approximately seven minutes.

Senator Gerard P. Craughwell: I compliment the Minister of State on taking board the issue of cybersecurity, but we need to start seeing it from a much more macro perspective. We should compliment the Garda on reversing at least some of the damage done to the HSE. The Minister of State said a few moments ago that money was a bit of a red herring. I am appalled to hear him say that. Malta, one of the smallest countries in the EU, is scheduled to spend €1.9 billion on cybersecurity over the next six years. I am afraid it does not go down well with me to say that money is a red herring.

I compliment the Chairman and my colleagues on agreeing to bring a human resources expert in front of the committee because the money the Department offered for the director of cybersecurity role was a joke. No serious professional would come anywhere near this country for that money, which suggests to me, and I have said this many times, security, whether it is cybersecurity, internal security or external attacks, is treated as a joke. We do not take it seriously. The Minister of State is trying to change that, but if he is going to do so he will have to see a budget that will support him. Some €13.8 million was spent on cybersecurity from 2017 to 2021. Where are we going? At the end of the day, it is a joke.

As we move forward, and I have said this a hundred times, we need an integrated intelligence agency under a director of intelligence that will bring together all the different intelligence-gathering agencies of the State. That includes the Garda, Defence Forces and the Departments of Social Protection and the Environment, Climate and Communications. We need them all under one umbrella whereby they can share information and we will know what is happening. We take issues like cybersecurity with a grain of salt. In the past few weeks, we had word of a Minister's phone being hacked. It just sort of breezes past everybody as nothing to get too ex-

cited about. Maybe the Minister of State cannot answer this today, but are his phones protected properly? Does he have encrypted telephones? If he does not, then he should.

Ireland is a central location for foreign direct investment. We control some of the largest volumes of data in Europe and we are talking about having 30 people working in cybersecurity. There should be hundreds of people working in cybersecurity, particularly when you look at the United States, which has almost 1 million people working in cybersecurity, and Estonia, a country we looked down our noses at a few years ago because it was much poorer than us, and its reputation in this area. My colleague, Deputy Ó Murchú, spoke about the issues of the Defence Forces and legislation. Last night, we saw on television how the Graham Dwyer case may limit the capacity of the Garda to get involved in counter-espionage, or counterintelligence, which is outrageous. It is outrageous that that might happen. We see ships sailing up and down the Atlantic coast, coming very close to the 12-mile limit where they are capable of intercepting data travelling from the United States into Ireland.

There are 3.5 million cybersecurity positions open in the world. With that many positions open, Ireland will have to compete. To do so, we will have to put billions into cybersecurity. We will not have foreign direct investment here in a few years' time if we start seeing cybersecurity attacks. I cannot understand it, but my belief is that since we all started to register on our mobile phones during the Covid-19 pandemic, we are being inundated with all sorts of crazy attacks. I get a dozen phone calls a week from the Department of Social Protection that I no longer answer. I will not answer any number now if I do not recognise the caller because I am sick to the teeth of it.

The Minister of State will be going in front of the Minister for Public Expenditure and Reform and the Cabinet in the next few days. Do they fully understand the impact there will be on foreign direct investment if they do not invest in cybersecurity? There is clearly a lack of understanding of what is required. In fairness to the Minister of State, after he saw the HR expert, Bláthnaid Carolan, talk to the committee about a salary structure of €220,000, he clearly fought the battle and got as close to that figure as he possibly could. We will, hopefully, get somebody very good for the role. The problem we have, with 3.5 million vacancies in the world, is if we will become a training centre for people who are paid poor money and who will move to higher-paying economies as soon as they are trained.

I am very concerned about this issue. This committee has taken a huge amount of time to debate these matters. I thank the Chairman for that and I thank the Minister of State for being here but is cybersecurity, and security in general, treated as a joke? Does he agree we need a director of intelligence and one single intelligence agency? I am shocked to hear that we have only one Defence Force member posted with the NCSC. It should be run by the military, like most cybersecurity organisations in the world. I will throw that over to the Minister of State and I might come back with one or two supplementary questions.

Deputy Ossian Smyth: I am not aware of any cybersecurity centre in the world that is run by the military. Ours is not run by the military, although it has military assistance and that is a very valuable input.

On the director's salary and whether there is enough money to pay that person, the job of the director who will be appointed on a salary of €184,000 is not directly equivalent to a chief information security officer working for a big tech company. It is a different job because it has different responsibilities and will have different day-to-day working arrangements. They are not directly equivalent. There are different benefits and responsibilities in respect of that job.

There is a lot of diplomacy, organisational skills----

Chairman: On that point, will the Department bring in experts in recruiting people for cybersecurity roles to assist in the recruitment process? It is such a specialised post. While the Public Appointments Service does its work well, for this particular role will the Department bring expertise in for the recruitment process?

Deputy Ossian Smyth: In short, we will bring in experts. It was the plan to bring in experts for this process. The board also has expertise but we will bring in external experts in this area.

I will go back to Senator Craughwell's question. He mentioned the idea that we should have some kind of overall head of all the different parts of cybersecurity and cyberdefence across the different branches of the Government, military, policing and so on, in some kind of co-ordinating role. In fact, we have that. It is called the national security analysis centre and it is based in the Department of the Taoiseach.

The Senator also asked if my phone was encrypted; it is. It is a basic security measure to make sure phones are encrypted so that if they are stolen the data can be-----

Senator Gerard P. Craughwell: I will interrupt the Minister of State. If Cabinet members' phones are encrypted, yet one has been hacked, does that raise a massive national security question? We have been talking about the HSE incident and the impact that has had for the past half hour. If people can hack a Cabinet Minister's phone, off the top of our heads we can think of the number of telephone numbers they would have, not just nationally but internationally, and the text messages that would be exchanged between Cabinet members and between Ministers across the EU. I find it beyond belief that we have had a Minister's phone hacked and that absolutely nobody seems to mind about it. It is a case of "Sure it is grand; it is all fine." We treat security as a joke.

Deputy Ossian Smyth: In terms of the security incident with the Minister for Foreign Affairs, Deputy Coveney, his phone was encrypted and the security incident was reported to the NCSC. I assure the Senator that the centre took it extremely seriously and as a matter of national security because of his position as Minister for Foreign Affairs. In no regard was this treated as a trivial matter. All of the correct statutory things were done to respond to that incident. That is all I have to say about it.

I will move on to the question about the Graham Dwyer case and the legal implications for intelligence gathering and the rules about-----

Chairman: I ask the Minister of State to be careful in his comments about any live legal case.

Deputy Ossian Smyth: I thank the Chairman for the reminder. In fact, what I was going to say was that it is a live case. It has not yet been decided and the implications of it are unknown as yet. Scenario planning is done, of course, but it is a live case and I cannot comment. I do not know how it is going to turn out, and that is the reality.

Senator Gerard P. Craughwell: In fairness, I was not asking the Minister of State to comment on the Dwyer case. It was the concept. When we are talking about security, for example, in regard to the development of anti-virus software, as the Minister of State will know, we are always chasing the criminal.

Chairman: In the interests of consistency, I also ask the Senator to be guided by the fact it is a live legal case.

Senator Gerard P. Craughwell: I was not going to go there. We are always chasing the criminal when it comes to virus software and we are always chasing the criminal when it comes to any sort of criminal behaviour, just as we are chasing the hardware when we are trying to develop the latest software. These are serious issues. Things like ethical hacking need to be proactive in the country if we are to be sure and safe. That would also apply to the schools, as noted by my colleague, Deputy Cathal Crowe. In the college where I worked in Blackrock, which the Minister of State knows well, we spent anything up to €100,000 a year on computer hardware, anti-virus software and cybersecurity systems. I know every school would not have that advantage. By the way, my school was a VEC, not a private school. In any case, I have taken enough time.

Chairman: Has the Minister of State concluding remarks in response to the Senator's questions?

Deputy Ossian Smyth: One of the questions the Senator asked was whether the members of the Cabinet understand the seriousness of cybersecurity with reference to foreign direct investment. They do. This is an issue the American Chamber of Commerce and other lobby groups for multinationals bring up because they want to have a secure environment in which to locate their data and do business. That is completely understood.

In general, the gist of what Senator Craughwell had to say is that he is concerned that cybersecurity is not being taken seriously, that adequate resources are not being given to it and that it is not understood within the Government how important it is. I would like to reassure him that none of that is true, that everybody understands how incredibly important it is to protect our national assets and critical infrastructure and that there are huge costs to being attacked, and that we have to do everything we need to do to be the best in class for cybersecurity.

Chairman: I have a question. The first recommendation from the capacity review is to form a cross-government task force with representatives from the Taoiseach's office, the Minister of State's Department, the Departments of Defence, Justice and Foreign Affairs and other key Departments to develop an action plan for this report and sponsor its implementation. Has that task force been established?

Deputy Ossian Smyth: In fact, a task force with all those members was set up in 2011. We will review it in light of this capacity review and any specific recommendations they have about it. We actually have that in place. If there is some way in which it needs to be-----

Chairman: Might I suggest that the Minister of State speaks to the consultants because they clearly do not appear to have been aware of it? They have put it as the first recommendation.

Deputy Ossian Smyth: Their recommendation is to develop an action plan for this report and to sponsor its implementation. The task force is in place.

Chairman: Is the action plan in train?

Deputy Ossian Smyth: Their recommendation is to develop the action plan, which I will remind the task force to carry out.

Chairman: In terms of getting down to do the action plan for this report, that is something

the task force will now take up. Am I correct?

Deputy Ossian Smyth: The Chairman is correct. I will remind them of that.

Chairman: Thank you. That is hugely important. I call Deputy James O'Connor.

Deputy James O'Connor: I thank the Minister of State and the officials who are here to discuss this very important topic. It would be remiss of me and any other public representative not to say, first and foremost, that we are grateful for the extremely hard work that was done by some of the officials in response to the attack on the State that happened in regard to the HSE software and IT systems recently. I am by no means an expert in IT and I will disclose that to the committee. However, I have grown up with technology and perhaps have more familiarity with it than some other Members of the Houses of the Oireachtas. I have done a bit of research and homework on this, and I am worried.

I do not want to go into an in-depth speech and would rather ask a couple of questions of the Minister of State. With the goodwill of the Chair, I would appreciate some rapid responses. What is the gross annual budget of the NCSC?

Deputy Ossian Smyth: The gross annual budget in terms of current and capital expenditure is approximately €7 million for 2021.

Chairman: What is the breakdown between capital and current?

Deputy James O'Connor: The important question I have is that the gross resourcing on an annual basis that the centre has for a country of 5 million people is €7 million.

Deputy Ossian Smyth: This angle has been raised by a number of Deputies and in the media, namely, the idea that the entire country's cybersecurity is being protected by 29 people and €7 million. That is absolutely not the case.

Deputy James O'Connor: I must ask for the protection of the Chair.

Chairman: Deputy O'Connor has his own direction on this. I will just hand back to him to allow him to develop the point.

Deputy James O'Connor: It is a clean question. I just want to know how much money the State is spending annually on cybersecurity. Given that he has responsibility in this area, will the Minister of State tell me that?

Deputy Ossian Smyth: I would love to be able to tell the Deputy that. What I need for that is the accounting to support that, in other words, that every Department, every State organisation and every public sector body would report back to me as to what its spend is and what its manpower is for cybersecurity. Without that information, I cannot give the Deputy a clear answer as to what the total expenditure is. I know it is two orders of magnitude higher than €7 million, and we are looking into the hundreds of millions of euro.

Deputy James O'Connor: Above all else, what happened in regard to the HSE was shocking. I am not going to lay the blame at the feet of the Minister of State. He is relatively to the Department and many of these problems are historic. However, the country and the Oireachtas need to have a better understanding of the existential risks relating to Ireland's cybersecurity. It all comes down to why we were targeted, and it is very clear that we were. It is because those involved saw an open goal. They saw this country as an easy place to come into and phish for

people's personal data, by means of a ransomware attack, in the hope of securing a financial reward from the State to get our data back.

I am concerned by some of the Minister of State's remarks. I was listening to his earlier contributions on putting things into a degree of perspective in comparison with what other countries can do. The reality is that the Republic of Ireland is Europe's leading country for foreign direct investment in tech. We have tens of thousands of highly skilled individuals working in multinational tech companies - I will not go through them because there are too many to mention - that offer particular services, including in the area of cybersecurity. Quite a few of them are located in Cork, where I am from. Have the Minister of State or the Government engaged with some of our major fintech companies, especially those with expertise in encryption and cybersecurity, to ask for their advice and input in strengthening the State's ability to defend itself from foreign cyberattacks?

Deputy Ossian Smyth: The Deputy 's first question was on why Ireland was targeted. The truth is that Ireland was not especially targeted. Hospitals around the world have been randomly attacked. It is just as easy, if one is a criminal sitting at a computer, to attack a hospital in New Zealand as it is to attack one in the United States, where 16 hospitals were taken down, Ireland, France or wherever. The truth is that every country can be a target for these people. They attack indiscriminately across countries around the world. Even those with the greatest cyberdefence systems can be victims. What was the Deputy's next question?

Deputy James O'Connor: My next question was on the role of tech multinationals, which is crucial. If we are not in a position to defend ourselves, particularly in comparison with other countries that began resourcing this area at a far earlier stage than we did, we need to try to reach out to organisations in the private sector in order to find the best expertise possible to allow us to build the team that is necessary to protect our country. I say this in terms of the ongoing review being done on the NCSC and the support staff who are to be recruited soon. I hope progress will be made in the two years to which reference was made. Can the Minister of State comment on that crucial point?

Deputy Ossian Smyth: We regularly meet with the tech giants. I had a meeting with Apple, which is based in the Deputy's constituency, not that long ago. Cybersecurity is discussed, but, in addition to that, we received support from third-party international cybersecurity consultants who provide us with a subscription service. We do not just rely on our own staff in Ireland. We also use third-party companies that are specialists in this area and we work with major multinational tech companies to get their advice. The truth is, however, that they rely-----

Deputy James O'Connor: Is the Minister of State in a position to give us the feedback from that engagement? What are they saying to the Government about our set-up and the steps we are undertaking to improve our cybersecurity?

Deputy Ossian Smyth: They have said to me that they need Government involvement as well and that cannot defend themselves purely on a commercial basis. Through our co-operation-----

Deputy James O'Connor: I am asking the Minister of State specifically about the State's defences. Is he in a position to inform the committee of what the members of the private sector with whom he has engaged are telling the Government? What is the feedback he is getting on what happened with the attack on the HSE? Is he in a position to disclose any details in that regard?

Deputy Ossian Smyth: None of the tech giants has contacted me, either directly or indirectly, to comment on the attack on the HSE attack or to express their concerns about it. We have a co-operative relationship with those companies. I have no sense they are suffering from dissatisfaction with the State in any way. They need us and we need them. There is a relationship there whereby we hire third-party and private companies to help us with work, but they need the State's assistance as well.

Deputy James O'Connor: I will come back in the additional round of questioning if there is available time.

Chairman: We have an executive summary of the redacted version of the FireEye capacity review. Would it be possible for the committee to get a copy of the full document, even if it also had to be redacted? We understand the confidentiality aspect.

My second point is on a recurring theme here. We accept all the work done by the NCSC and the Minister of State, but we had an expert in here who said that if one was to base the €7 million - of which approximately €2 million is capital spending and €5 million current, if I am correct - *per capita* relative to the UK, we should be spending approximately ten times that figure, or in the region of €50 million per year. We are spending €5 million, which will probably go up next year, because, extra staff will be coming in. We appreciate that. How does the Minister of State respond to in that regard? We want to assist him in getting the maximum amount of money from the Government. The HSE attack was certainly a wake-up call and everyone will accept that. How does the Minister of State address the fact that it is being said that it should be ten times the €5 million being spent per annum on national cybersecurity and current operational expenditure?

Deputy Ossian Smyth: The €7 million is split differently from the way the Chair said. It is €5 million for capital spending and €2 million for current.

Chairman: Only €2 million is current spending. It was stated that €50 million should be spent and, based on that, it should be 25 times the current level of operational expenditure.

Deputy Ossian Smyth: I appreciate that the committee is trying to help me. We are all on the same page. We all want fantastic cybersecurity defences for our nation and we want them to be properly resourced. That is absolutely fine. What would help this discussion, however - this has been brought up by a number of Deputies and Senators - would be to have a broader accounting in respect of how much money is being spent in different sections of the State public sector bodies on cybersecurity, rather than focusing on the NCSC all the time and then making comparisons with other countries which are counting other parts of their expenditure that are different from ours. The Garda and the Army are spending money. I would love to come back to the Chair with more information in order that a fair comparison can be made.

Chairman: Will the Minister of State do a body of work on that? Everything costs money. One can speak about it, but, ultimately, it is taxpayer's money and we want to put it to good use. If the Minister of State does a body of work on what is being done by all public bodies, then maybe when we come back again, we will look at that aspect. Will the Minister of State be forthcoming with the full redacted report?

Deputy Ossian Smyth: I am happy to do that work. I am interested. My thoughts over the past few months, when people were saying the money is wrong, were that I needed more information. I will do that work and come back to the committee with it. I will also come back

to the committee in the coming weeks with the full report, again redacted. That will take a number of weeks.

Deputy Darren O'Rourke: I thank the Minister of State for sticking with us. Why a five-year rather than a two-year plan? What are the considerations involved? Why is the scale of investment not more compressed and front-loaded? Is it because the money is not there? Is it because the recruitment criteria cannot be met? Is it feasible to condense this into two years? The Minister of State rightly said that the NCSC is one small part of a far bigger operation. To what degree will there be a renewed focus on cybersecurity across all Departments, sectors and critical infrastructure interests? Will the NCSC and Government bring that focus to the table in order to ensure that we are better prepared for future eventualities?

Deputy Ossian Smyth: On the Deputy's point about whether there should be cybersecurity investment across all of Government and so on, I am looking to have that included as an objective within the national development plan, which is due to come out shortly.

The Deputy also asked why it is not going to grow faster and why it is a five-year plan rather than a two-year one. The NCSC has been growing since 2018. There is a limit to how fast you can organically grow an organisation, do it well and recruit the right people. This is a highly specialist area. We are doing it as quickly as our external consultants recommended was possible. Thus it is a five-year plan rather than a two-year one. It would be great to suddenly be able to explode it in size overnight but that is what it is. What was the Deputy's other point?

Chairman: The point was on the process whereby there would be a direction with all Departments about investing in cybersecurity. I would add that the Estimates process is ongoing. The Minister of State is at the Department of Public Expenditure and Reform as well as the Department of the Environment, Climate and Communications. I would have thought it would have been relatively straightforward to insist each Department put what it is spending on cybersecurity in as a specific item. That might enable the Minister of State to gather that information and come back to us.

Deputy Ossian Smyth: I completely agree with the Chairman. I will also mention that the NCSC has developed standards in cybersecurity for public bodies. It is due to publish that within weeks. That will address the matter in question.

Chairman: The Estimates process could be a way of capturing that data. It is something the Minister of State might take on board, even at this stage. He could instruct Departments to include cybersecurity spending within their Estimates when they come to his Department. I call Deputy Ó Murchú.

Deputy Ruairí Ó Murchú: It is absolutely necessary that we have that information, namely, the moneys that are going to be spent across the board and the actions that will be taken in every part of critical infrastructure.

On something the Minister of State said earlier, the buck stops with the national security analysis centre in the Department of the Taoiseach in the context of intelligence. To a degree, it is the lead on all of this. Is this so?

Very quickly, will the Minister of State provide an update on what he foresees under Sensor as to the increased capacity?

Our relationship with the CCDCOE, which, I believe, is a NATO operation, was mentioned.

Are we involved with the EU on this sort of co-operation, at any level?

Deputy Ossian Smyth: The CCDCOE in Tallinn is not a NATO facility. It is not under the NATO command structure but it is accredited by NATO. It has people in it from Sweden, Finland, Austria and Switzerland. It involves a number of nations co-operating, but it is not run by NATO. We have somebody out there. It is mostly a research facility. Due to the fact that international co-operation is so critical to making progress against cybercriminals, it is a place where experts in the field can work together and develop techniques and skills to be able to fight the criminals. I think that is all I can say about it. Nearly everything it does is published so it is not, in any sense, a secret facility or anything like that.

There was a question then about Sensor, was that it?

Deputy Ruairí Ó Murchú: It was about Sensor and also the national security analysis centre.

Deputy Ossian Smyth: The national security analysis centre is a co-ordinating body. The Deputy asked whether it is the place where the buck stops. The statutory responsibility still lies with the Garda, the Defence Forces or the NCSC, which is under the Department of the Environment, Climate and Communications, in each case. The national security analysis centre is a co-ordinating body.

Deputy Ruairí Ó Murchú: It is responsible for co-ordination.

Deputy Ossian Smyth: Correct.

Deputy Ruairí Ó Murchú: All right.

Deputy Ossian Smyth: It is under the Taoiseach's Department.

Chairman: What about Sensor?

Deputy Ruairí Ó Murchú: Point 8 in the executive summary states: "Enhance the technical monitoring capability under Sensor, improve the analytical and intelligence technologies that underpin it, and expand its use across the Public Sector."

Chairman: The Minister of State must be brief.

Deputy Ossian Smyth: The Sensor platform is actually in full operation across Government. It needs legislation to be developed and that legislation is being drawn up. It is not as if there is no legislation underpinning cybersecurity in Ireland. We have the network and information systems directive, which is being transposed into Irish law, but we are bringing in additional legislation to provide a better statutory basis.

Chairman: Is the legislation the overall primary legislation on the NCSC? Is it included in it? When does the Minister anticipate we will have pre-legislative scrutiny in this committee on that legislation giving the NCSC a statutory footing?

Deputy Ossian Smyth: I expect it will be next year.

Chairman: That is great. I call Senator Craughwell.

Senator Gerard P. Craughwell: There was a ransomware attack on the UK health system on 12 May 2017. It beggars belief that our health service was still operating with machines and

software that were so out of date that they were an easy target. This brings me back to the point I have been trying to make all along, namely, that we do not do security seriously. The Minister of State outlined the various different agencies that are involved under the security umbrella. There are too many goddamn cooks. There must be a director of cybersecurity who has his or her staff placed in every Government agency. They should be reporting directly to him or her, not to the Secretary General of the Department or some principal officer in a Department, who might write a report at some stage which might finish up in the Department of the Taoiseach. There is a terribly lax attitude to security here.

The Minister of State said he engaged with the high-tech companies. I have met people from high-tech companies at various functions around town. They tell me they have been screaming for years about the state of security and cybersecurity in this country. I would like to have an audit, if we could, of the current state of all State agencies with respect to cybersecurity, including what steps they have taken to protect their own systems since the HSE was attacked and whether they reporting directly to the Minister of State so we know where we are on this. I am deeply concerned that with all the cooks who are involved in the organisation of security in this State, we will find ourselves attacked time and time again.

Deputy Ossian Smyth: The 2017 attack on the NHS was the WannaCry virus ,which was not a ransomware attack. It did cause great damage to NHS systems. It also attacked the HSE and luckily the HSE was protected to the extent that much less damage was caused.

On the question of centralised cybersecurity, the Senator was suggesting that every cybersecurity lead in every Department should report to the NCSC director. This is a centralised model, and the opposite of the model we were discussing with Deputy Cathal Crowe, whereby we have a distributed model as people need to be able to control their own cybersecurity in their own organisations. We are not proposing, and the review of our cybersecurity capacity does not suggest, that we should centralise all our cybersecurity and have it run by the Department with responsibility for communications and that everyone should report to it.

Senator Craughwell also raised the question of the reporting of cybersecurity events and the transparency around those. I agree with him on this. Usually, not every cybersecurity attack and incident that happens is reported and becomes well-known to the public. The assumption is then that staff are doing nothing or that nothing is happening and there is nothing to defend. I would like to see in the future a framework for better reporting to the Oireachtas and to the public of the cyberattacks that are happening and how they are being defended against.

Chairman: On that point, if there is a cyberattack on a business, school or public service, to whom is it currently recommended that should be reported? Do people know about that? Can the Minister of State come up with a framework that can be put in place, including a structured approach so that people are able to report attacks, which allows for transparency in the publication of the numbers of incidents that are reported and a signals map of our general state of being? To whom do people report incidents at the moment?

Deputy Ruairí Ó Murchú: I would add that we have heard a number of anecdotal reports of many companies that are not declaring incidents and are just paying the money, getting the key and telling nobody anything because of a fear of reputational damage.

Chairman: The Minister can take on board that people are unwilling to report, for whatever reason. What can we put in place? Who do such people currently report to? Are they supposed to report to the NCSC?

Deputy Ossian Smyth: They are supposed to report to the NCSC. I would tell any organisation that is attacked to look at the website of the NCSC where there is information on how to report an incident. To give the committee an idea of the volume, 3,000 such incidents were reported last year. That is to give the committee an idea of what is going on. What was Deputy Ó Murchú's question?

Chairman: The Deputy made the point that people are paying ransoms rather than reporting incidents. What is the Minister of State's perspective on that?

Deputy Ossian Smyth: We do want people to report what happens. We do not want them to pay ransoms because doing so only creates more attacks. That is the business model of the people conducting the attacks. I would ask anybody who is attacked to contact the NCSC for assistance. The staff at that centre have great experience dealing with people who have been attacked. The actions a company takes when it is attacked are critical to what happens later on and to that company's success in protecting itself from these people. Even if the ransom is paid, the data may be published and a key may never be forthcoming to unlock the data. In the case of the HSE attack, we did not pay a ransom, got the key back and no data were published. I would advise any organisation that is attacked to contact the NCSC.

Deputy James O'Connor: We are hearing a lot about reviews and reports. Time is against us on this issue. It is only a matter of time before we have another ransomware attack in the State. There is an onus everybody, including us on the committee, to try to assist in any way we can with our suggestions. I want to use the remainder of my time to be very clear that I think it is imperative as part of this review and report that the Minister of State engages directly with all of the available tech expertise in the private sector located in Ireland. They are here for many reasons, including for corporation tax in terms of their own enterprise and the business they do. That is their own business and that is fine. There is a service they could provide our State and surely there is sense in bringing them in now and asking them for their input to this review. That is important. I know the Minister of State said he has been engaging with the tech companies when I asked a couple of questions in that regard. That is a must.

Above all else is the encryption of people's personal data. This might seem boring to some but what happened is incredibly serious. Hackers were able to get access to people's personal data and intimate details relating to their personal health. They got people's addresses and other matters relating to their personal lives. That is extremely concerning and should be treated more seriously at the highest levels of Government, including in the Civil Service. I am not putting direct political blame on the Minister of State in that respect. He inherited this state of affairs. However, we do need to take proactive and urgent measures now.

I am asking the Minister of State to bring in the private sector leaders in encryption and cybersecurity. It would be no harm talking to tech multinationals and social media companies that have vast experience around coding and the encryption expertise required for improving the State's cybersecurity. Will the Minister of State please respond on those points?

Deputy Ossian Smyth: I can assure the Deputy that we regularly talk to all of the major tech companies. We are in contact with them all the time. I will make sure cybersecurity is on the agenda for those meetings, but there is no lack of communication. Neither is there a lack of communication with small businesses. I meet all their representative bodies every quarter. Engagement is essential. We are the centre of European tech and it would be crazy for us to ignore the expertise we have onshore. We would never do that. I assure the Deputy we have constant engagement at the highest levels with those organisations.

Deputy James O'Connor: The point of my contribution was to ensure those tech companies would have a role in the review of the NCSC we are here to discuss. That is what I am trying to stress to the Minister of State, to be totally clear.

Deputy Ossian Smyth: When we have public consultations on cybersecurity, they are the bodies that respond. There are often only one or two individuals who respond and all of the others are large corporate bodies, tech giants or whatever. They have a particular interest in this area. We have a co-operative, not a fractious or confrontational, relationship. We work with those companies because we have the same goal, which is to protect Ireland, our assets and infrastructure from attack to ensure peace and continuity on the island. We are absolutely aligned and in clear communication with those companies at all times.

I appreciate the opportunity to appear before the committee. It gives me food for thought. The committee's questions were insightful and useful and came from different perspectives. I now have a couple of things on my to-do list. I hope my civil servants are happy to work with me on that and I think they are. I appreciate the committee's constructive approach to working with me. I thank committee members for attending.

Chairman: We will write formally to the Minister of State. We think that in the short term he should request that all Departments incorporate cybersecurity spending in their Estimates. That should be possible and it would enable the Minister of State to gather that information very quickly. We spoke about the framework the Minister of State is looking at in terms of the reporting. A structured framework should be put in place so that when people are attacked, instead of immediately taking the default position and paying the ransom, they will instead engage with authorities such as the HSE. That is how we can ensure these pirates do not come knocking on the door all the time. We must let it be known that Ireland is not a haven for cyber pirates. We will write to the Minster of State formally in that regard, if that is okay.

Deputy Ossian Smyth: That would be great. Thank you.

The joint committee adjourned at 2.48 p.m. until 9.30 a.m. on Tuesday, 28 September 2021.