Opening Address – Oireachtas Committee on Foreign Affairs and Defence

23rd May 2023

Good afternoon Chair and thank you for the opportunity to speak to the committee this afternoon

My name is Richard Browne. I am the Director of the National Cyber Security Center and I am accompanied by my colleague Kerri-Ann Woods, Head of the Project Management Team in the NCSC.

The mission of the National Cyber Security Centre is to lead in enhancing the security of essential network and information systems in the State against cyber threats, facilitating a free, open, secure, and stable digital ecosystem for the people of Ireland.

We achieve this mission by a number of means, including by actively detecting and defeating cyber threats targeting critical infrastructure and critical networks in the State, leading the national cyber security incident response process and reducing risks to the States' critical infrastructure by strengthening its resilience. The NCSC also has a series of new roles around capacity building in the cyber security sector in Ireland, and in setting certification standards.

I'd like to speak to you today about three things. I'd like to talk about current global state of affairs in cyber security and the risk level that it presents to this State. Then, I'd like to talk to you about the work of the NCSC, and how our capability is continuing to develop, and our evolving role in the defending the state against risks and threats in the cyber security domain. Lastly, I'd like to talk to you about the future, including future European legislation and the future political, economic and security challenges that we will almost certainly face.

To begin with, and reflecting on more than a year of the most recent Russian invasion of Ukraine, a number of things have become evident. The first of , as was widely predicted before the event is, that cyber remains a key tool in the armoury of any State wishing to conduct offensive military action.

The second thing is that these attacks have been largely inconsequential in terms of the overall Russian military effort. There are three primary reasons for this. The first of these relates to an innate characteristic of cyber as a means of force projection; it is simply less effective as a destructive tool than many commentators have allowed for in recent years. The second reason is that the Ukrainians were ready; ready because they had endured years of similar offensive actions and ready because they expected an attack. They have taken and continues to take very significant measures to protect themselves from the consequences of these activities. Lastly, the Ukrainians have also benefited from massive external support from public and private sector organisations on a global basis, including from NCSC.

There have been some notable implications for cybersecurity in the rest of Europe as a consequence of the conflict in Ukraine also of course. Some of this relates to the ongoing risk of spillover in the cyber security domain, as has already happened to a limited extent in the ViaSat incident. There has also been an ongoing and persistent series of so called 'hacktivist' attacks which have extended over the vast majority of EU Member States including Ireland.

These attacks have primarily been distributed denial of service, or ‘DDOS’, attacks and have caused little to no disruption to services. They do however indicate the existence of an organised campaign to harass service providers in Europe, and a willingness to at least tacitly threaten further action against European infrastructure operators.

As ever of course, the most pressing risk to services, businesses and infrastructure remains ransomware. This is now a highly evolved vertically integrated industry with a significant number of well capitalised and well organised criminal groups conducting attacks on an ongoing global basis. Furthermore, this criminal ecosystem, which also includes a vast amount of cyber enabled fraud, is evolving extremely quickly, developing and sharing new tools and techniques very rapidly.

There are however some reasons for guarded optimism at this point. Better international cooperation particularly around intercepting these groups revenue, and targeting their core infrastructure, has seen some of the major groups fracture in the last few months. Also it appears that the percentage of victims who were paying ransoms continues to fall, at least partially due to the fact that victims are now more resilient.

Critically and this cannot be overstated chair, none of these groups despite their capabilities, are unbeatable. Sensible resilience measures can dramatically reduce likelihood of being targeted can reduce the seriousness of the impact if you are targeted, or can make it far easier to recover even if you are hit.

Moving on to the work of the National Cybersecurity Center; I think it's worth reflecting on the July 2021 Government Decision on the future of the NCSC, which was based on a very detailed Capacity Review of the organisation, including setting a trajectory on staffing and technology development. The contents of that Decision continue to be delivered and in fact exceeded, with a Technology Strategy developed last year and the very significant evolution of the outputs of the organisation.

In terms of people, in the last 12 months, the NCSC has gone from 25 staff to 52 staff today, with sanction to grow to 62 staff this year. The organisation now has three directorates, each led by a Director level post, and each with a team led by staff at Principal Officer grade. Furthermore, this far more robust management structure has allowed for a far greater specialisation of function within the organisation, and for the addition of entirely new functions, including the National Coordination Centre role, and the Certification Team.

The Operations Team is the team responsible for incident response, and in detecting and defeating incidents before they occur. Previously led by a Principal Officer, now has three Principal Officers led teams, overseen by a Director. The organisation now has a dramatically increased ability to defend against incidents at a national level and to collect, manage and analyse cyber intelligence material.

The Resilience Directorate has five teams, covering Engagement, Compliance, Capacity Building, Certification and Project Management, also led by a Director. The range of work accomplished includes ensuring the compliance of critical infrastructure with binding security requirements, building and maintaining information sharing networks, and working with industry and academia to support the development of the cyber security sector here.

The Technology Directorate is awaiting the appointment of our new CTO, which will happen later this year, but this team already builds and maintains the systems, networks and tools we use, and are instrumental to the process of building our new permanent headquarters.

Quite aside from our capability developments, we have also made significant strides in both operational and resilience realms. For example, we fully revised the national cyber emergency response plan on the basis of After Action Reviews of previous experiences, and conducted a full scale national exercise to test this, using the energy sector as a basis.

We also commenced the process of revising and deepening our longstanding information sharing structures, starting with a new Government Cyber Security Coordination and Response Network (GovCORE), which also acts as our point of contact for the Baseline Standard. This is being followed by augmented cyber security information sharing, coordination and response networks, or COREs in the Local Government, Energy and Digital Infrastructure sectors.

The NCSC is now housed in an interim facility that is secured to international best practice and has the appropriate infrastructure for full international sharing of cyber security intelligence, as well as a full incident response suite. In turn, this has augmented our ability to conduct faster and more complete analysis and response to cybersecurity incidents and risks, and allows us to share information with colleagues globally on a real time basis.

Our permanent facility, in Beggars Bush, is on track for handover to us at the start of Q4; we are in the process of procuring the hardware and equipment for that facility at the moment. That new facility will allow us space to continue to grow and develop, and perhaps most importantly, allow us to build out our new National-Level Security Operations Centre.

Lastly, chair, to the future.

By the 18th of October next year, the revised Network and Information Security Directive will come into effect in Ireland. This will result in a dramatic expansion of the number of entities subject to the Directive here, from just over 100 to at least 2,000. Unsurprisingly, this will have some implications for the NCSC, and for a great number of other entities in the State and will take up a very significant amount of the next 18 months.

Also, in the coming weeks a Mid Term Review of the National Cyber Security Strategy will be brought to Government for approval. This will contain a series of new roles of the NCSC also, which will be framed in new primary legislation, with the general scheme to be published by year end. This legislation will also reframe the roles and powers of the NCSC, as well as make provision for the transposition of several other pieces of EU legislation.

In addition to all of this, the technological underpinnings of the world we live in are beginning to change very significantly. Were I sitting here a year ago, I would have spoken about the shift to cloud computing, the challenges associated with post quantum cryptography, or perhaps the need for security by design to be implemented at every level of the supply chain. All of these are still factors today, but are entirely overshadowed by the first public outings of generally available Artificial Intelligence.

This technology has been much heralded, and has seen a vast amount of investment in the last decade. It is not an overstatement to suggest that this is at least the single most important technological development since the internet, and it may well likely turn out to be more important than that.

Like any such technological revolution, the full effects of this will take years to play out, and perhaps even more than that. Already, it is clear that these tools will be extremely powerful, with applications and implications across the full range of human behaviour and activity, including in security. We have already published a blog on the matter, and will have a piece of guidance available for public servants in the coming weeks.