Roinn Cumarsáide, Gníomhaithe
ar son na hAeráide & Comhshaoil
Department of Communications,
Climate Action & Environment

National Cyber Security Strategy
Draft Public Consultation
March 2019

1 Introduction

1.1 Cyber Security has become a central issue for government globally in the last number of years, owing both to the increasingly pervasive nature of network and information systems and the growing awareness of the potential for incidents affecting these systems to threaten social and economic wellbeing. However, the decentralised and global nature of the technology means that there are limited direct levers that States can bring to bear to ensure the security of networks and devices, while those same tools are exposed on a global network, and to a diverse range of actors seeking to compromise them, and the data they contain or the systems they manage.

1.2 Ireland ranks 6th in the 2018 EU Digital Economy and Society Index (DESI), meaning that it is among the leading ranks of EU Member States in terms of the uptake and use of digital technologies. This is reflective of the general strengths of the Irish economy and of Irish citizens, but it also reflects an underpinning set of vulnerabilities. Furthermore, it also shows that the security of network and information systems is both ever more important and is rendered more complex and challenging as systems become more embedded and complex.

1.3 The increasing centrality of network connected devices to the operations of business and critical infrastructure in turn means that the consequences of cyber enabled attacks are far more serious than in the past. Government responses to these issues have developed significantly over the last number of years, and the European Union, for example, has taken a particularly coherent and comprehensive approach. However, the challenges for policy are such that continued evolution is critical; the next National Cyber Security Strategy marks an opportunity to adapt and implement national policy responses across Government to meet these emerging challenges.

1.4 The pervasive nature of these issues has a number of implications. Firstly, every sector of society is involved to some extent; a very wide range of services, products and industries depend on Network and Information Systems. This means that any response to these emerging challenges has to be very broadly based and capable of ongoing flexibility and evolution. Secondly, the diverse nature of these sectors, with different ownership models and technologies, means that there is no single model or solution, technical or otherwise.

1.5 The next National Cyber Security Strategy will mark an important step in securing Ireland's digital future by setting out a series of initiatives, building on the work completed since the 2015 Strategy, that focus on the key challenges facing us all with regard to the security of our Network and Information Systems. These measures include some that focus on improving the resilience of Public Sector IT systems, and other that set out how we will improve those measures already in place around Critical Infrastructure, and to support businesses and individuals in securing their own systems.

2 National Developments since 2015

2.1 The first National Cyber Security Strategy, agreed by Government in 2015, set out a series of measures that would be taken to build the capability of the National Cyber Security Centre (NCSC) and to achieve a high level of security for computer networks and critical infrastructure in the State. These measures included steadily increasing the capacity of the NCSC and the Computer Security Incident Response Team (CSIRT) which is part of the NCSC and a series of measures around improving the network and information security of Public Bodies. The Strategy also established how the resilience of critical national infrastructure would be improved, in part by the transposition of the EU Network and Information Security Directive, and how the national incident response process would be developed through ongoing participation in the National Emergency Management System.

2.2 The aims of the 2015 strategy were exceeded in practically all respects. The NCSC has developed significantly in terms of capacity and resources, and its roles have been formally established in law including responsibilities around critical infrastructure protection and dealing with EU requirements around the security of some Digital Service Providers. The responsibilities of the CSIRT itself with regard to risk and incident handling have been defined in law as requiring it to;

> "(a) monitor incidents within the State,
>
> (b) provide early warnings, alerts, announcements and dissemination of information about risk and incidents to relevant stakeholders,
>
> (c) respond to incidents notified to it under Regulation 18 or 22,
>
> (d) provide dynamic risk and incident analysis and situational awareness,
>
> (e) participate and co-operate in the CSIRTs network,
>
> (f) establish relationships with persons in the private sector to facilitate co-operation with that sector[1]".

[1] Regulation 10 of S.I. 360 of 2018

2.2 The NCSC has developed a threat intelligence database that is being used to assist Agencies and Departments in protecting their networks. There has also been a comprehensive expansion of the NCSC constituent base with over 130 members including Government Departments and Agencies, the Financial Sector, Critical National Infrastructure (CNI) providers and other Operators of Essential Services (OES), which is augmented by the development of a more robust Alert and Advisory Service and the rolling out of a text alerting system.

2.3 The CSIRT has also received Trusted Introducer accreditation, signifying that the team had reached a defined level of best practice and maturity. The CSIRT team has continually sought to develop new processes and means to detect and manage potential cyber security threats, and has built an automated incident management and response system, fully integrated with the threat intelligence database.

2.5 The NCSC has worked, on an ongoing basis, with utility operators and with similar bodies in other jurisdictions to ensure that risks to infrastructure in Ireland are managed appropriately, including the active management of ongoing issues. This includes North-South and East-West consultation in relation to the implementation of the NIS regulations and incident response. The NCSC maintains close cooperation with the Defence Forces and the Gardaí on national security issues, and has a secondment arrangement with both entities. The NCSC and Garda National Cyber Crime Bureau have developed a positive co-operative relationship with ongoing shared training and secondment opportunities for staff.

2.6 The NCSC has also developed a Malware Information Sharing Platform (or MISP), which is offered to constituents free of charge, with the main objective being to stimulate sharing practices among public and private actors and ultimately to improve malware detection. By using such a platform organisations can benefit from the shared knowledge about existing malware or threats which can help them to improve their counter measures to prevent such attacks.

2.7 The 2015 strategy was written in anticipation of the EU Network and Information Systems Directive (NIS Directive) which would introduce new measures to better secure critical national infrastructure against cyber related incidents. The Directive was transposed in September 2018 by S.I, 360 of 2018, which has resulted in the introduction of a set of new legal tools for the NCSC and a formal role with regard to the security of critical national infrastructure. Enforcement powers under the regulations allow authorised officers of the NCSC to conduct security assessments, require the provision of information and issue

binding instructions to remedy any deficiencies. Furthermore, the NCSC has prepared a guidance documents relating to security measures, compliance and incident reporting to provide additional support to the OES, which was published for public consultation in January 2019.

2.8 In October 2018, a new Cyber Security Skills Initiative was launched by Skillnet Ireland in partnership with the NCSC, Garda National Cyber Crime Bureau, and other agencies and third level institutions. The core aims of the initiative are to develop awareness, bridge the skills gap and to set standards for skills and competencies for Cyber Security roles. The three year plan will focus on building training and accreditation in the field to address skills gaps, attracting more young people, and in particular women into the sector and promoting Continuous Professional Development. Skillnet Ireland estimates that the initiative will deliver Cyber Security training to in excess of 5,000 people in the industry over the next three years.

2.9 The Gardai also have responsibility for preventing and investigating criminal offences – to that end they have recently created a National Cyber Crime Bureau (originally established as the Cyber Crime Investigation Unit in 1991, and re-established as the Garda National Cyber Crime Bureau (GNCCB) in 2017). The Bureau is the national Garda unit tasked with the forensic examination of computer media seized during the course of any criminal investigations. These include murders, cybercrime, online harassment, computer intrusions, child exploitation offences and any criminal investigation in which computers are seized or may contain evidential data.

2.10 The 2015 Defence White Paper notes that "*… the Department of Communications, Energy and Natural Resources has lead responsibilities relating to cyber security*" and explained that "The primary focus of the Department of Defence and the Defence Forces will remain the protection of Defence networks" but that "*as in any emergency/crisis situation, once Defence systems are supported, the Department of Defence and the Defence Forces will provide support to the CSIRT-IE team in so far as resources allow*".

2.11 Cork Institute of Technology (CIT), supported by the IDA, have established a programme to establish and grow a Cyber Security Cluster in Ireland. The cluster will include stakeholders from industry, academia and government and will seek to encourage co-operation, raise awareness of education and career opportunities, drive innovation and stimulate new business in the Cyber Security field.

CIT has secured 2 years funding from the IDA to develop the cluster and has drafted a 7 phased structured program to achieve this aim.

As a Government partner the NCSC will support CIT in building and managing the cluster from inception providing guidance through programmes, workshops and national policy.

3 Challenges for the Future/Risk Assessment

3.1 The internet and its supporting technologies are now truly global in nature and have become integral to the way we live, do business, and socialise. They provide open and free communications across a network governed by a set of simple and open technological rules. Over time, this network has grown to become a platform for a vast range of products and services, including many of those services essential for the continued functioning of our society and economy, including sectors like financial services, healthcare, energy supply and the media.

3.2 As such, the flexibility and openness of this platform has brought some profound benefits. However, it has also introduced a series of new and confounding vulnerabilities; the very openness of the network and of the protocols that have facilitated this transformation have enabled a series of different threats. Some of these are simply new manifestations of age old activities, and involve the mere theft of data or money. Others are entirely new, and include the remote destruction of data or critical infrastructure. Determining the optimal response measures for any State will depend on the nature and extent of the risks it faces.

3.3 At a high level, these risks extend to the security of the State. This can include the theft or destruction of sensitive Government or private sector data, or the damage or destruction of critical infrastructure. Examples of all of these have been seen and demonstrated internationally in recent years, with the threat actors varying. In some cases other States are responsible; in others the source is criminal. Of course, one of the confounding characteristics of the sector is the fact that a malware premised attack on the infrastructure of one country can swiftly become a global issue, due to the spread of malware (as was the case with the NotPetya incident in 2017). Similarly, once used and known, these same tools often find their way into the hands of criminals.

3.4 Cyber tools are often a key component of so called 'Hybrid Threats'. These threats *"combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives*[2]".

[2] https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en

In practical terms, threat actors seeking to use these means can use cyber enabled techniques to steal information from political parties, Governments or private organisations for subsequent release, sometimes in edited form, at an opportune time or to support a general campaign of misinformation or to subvert some genuine political or judicial process. As such, this represents both a data protection challenge, and a risk to the proper function of democracy.

3.5 One of the more common and more damaging outcomes of the rise of malicious online activity relates to attacks on businesses, often for financial gain. Cyber Crime is widely estimated to cost businesses globally a very significant amount of money annually and often builds on long standing methods of fraud, like Invoice Fraud (or 'CEO Fraud').

3.6 An ever present and real risk arises as to the confidentiality, availability, integrity and authenticity of data, regardless of whether they are owned by citizens or businesses, or where the data are stored.

3.7 Historically, States could hope to secure key infrastructure by securing a very small number of key installations. They could make laws to prohibit parties using their territories for illicit purposes or activities, and they could use physical borders as a means of defending against external threats. None of these measures work in the same way in the digital age. Because of the nature of the network, borders no longer have the same effect. Moreover, for practical and legal reasons, Governments generally do not have visibility of, or cannot secure, the vast range of devices or the traffic flowing to and from them. This is because networks are privately owned, as are both connected devices and a very large proportion of critical national infrastructure. This dependence on digital infrastructure has implications for both services, and for the physical infrastructure that these services rely upon.

3.8 The fact that these devices rely on software provided by a relatively small number of vendors adds further risk. This is because any identified vulnerability can be used to rapidly compromise the data or systems of millions of people, on a global basis. Moreover, software has to be kept up to date, and in some cases is no longer supported by a vendor once a given period of time has passed. Lastly, the ongoing development of internet connected tools has led to the decline of the older systems, with the effect that the internet itself is now critical, meaning that the physical infrastructure and software that allows it to function is has become a source of risk in and of itself.

3.9 The threats to individuals, businesses and the State arise from a wide range of actors. Traditionally, these have been divided into three broad groups, escalating in terms of access to resources and capability.

Firstly, there are individuals acting alone or in small groups, or so called 'script kiddies'. These actors have traditionally engaged in nuisance type attacks, ranging from website defacement to small scale denial of service attacks. At the upper end, these segue into the next category, that of criminal actors. This category covers a very wide range of people, ranging from small scale criminals engaged in cyber enabled fraud, through to organised large scale criminal gangs, with access to high end tools and capable of running organised and large scale operations. Lastly, at the top of this pyramid, are State entities, usually military or security organisations, seeking to use network and information systems to conduct operations ranging from the exfiltration of data to the destruction of physical infrastructure. In the recent past, there have been multiple examples to suggest that this simple typology may no longer be particularly relevant. For example, criminal gangs have allegedly been operating under contract to some States, and there is evidence to suggest also that lone actors have been organised to act collectively by Governments.

3.10 The response by States, particularly in Europe, has gone through several readily identifiable phases. The first of these was to establish expert support and response organisations, usually by means of the creation of Computer Security Incident Response Teams (or CSIRTs). These organisations were generally tasked with gathering and sharing information around threats and risks, and organising and coordinating incident response capacity. The second response has been to focus on the resilience of critical infrastructure, first by working with operators, and more recently by beginning to legally compel these operators to meet certain standards. This later response has been further developed at EU level, and forms the basis for the NIS Directive, along with formal information sharing and cooperation between Member States.

3.11 In December 2017, the Government decided to establish the first Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation. This group is tasked with assessing the risks to Ireland's electoral process, taking into account the substantive issues arising from recent experiences in other democratic countries with regard to the use of social media by external, anonymous or hidden third parties. The Department of Communications, Climate Action and Environment is a member of this group and the NCSC provides input in relation to the Cyber Security Aspects. The Group published its first report in July 2018 which overall found that while the risks to the electoral process in Ireland are relatively low at present there is potential for future risks due to the spread of disinformation

online and the risk of cyber-attacks on the electoral system. The group has proposed a number of measures to protect against these risks, including establishing an Electoral Commission, modernising voter registration, regulating online political advertising and supporting EU efforts to tackle disinformation.

The group has also proposed enhanced cyber security measures around the electoral process including the NCSC safeguarding of the electronic aspects of the electoral register, increasing awareness of cyber security risks and the NCSC providing advice to political parties on cyber security.

4 Questions

Question 1

> *"Having regard to the developing challenges and risks arising in cyber security, and the progress made as outlined above, what should be the focus and key objectives of this Strategy?"*

A successful cyber security model must be the sum of joint efforts between Government, business, and citizens. The next National Cyber Security Strategy must be both inward and outward looking, focusing on improving Government ICT Networks, developing Cyber Security Skills and addressing the concerns of businesses and citizens. One way of establishing the key issues to be addressed is to do so in a thematic manner. As such, the key themes selected to shape our strategic approach to Cyber Security in Ireland are 'Protect', 'Develop' and 'Engage'.

Protect

Protecting the State, its citizens and critical infrastructure must be at the forefront of any Cyber Security Strategy. Advances in technology will continue to present both opportunities and threats. Ireland, like most of Europe, has a highly developed infrastructure that is, in most cases, almost entirely dependent on information and communication technologies (ICT). There are two key themes at issue here, critical infrastructure protection and Government ICT. Critical infrastructure such as energy, water, social welfare, telecommunications, banking and healthcare are all dependent on ICT to operate effectively. Equally, Government networks are exposed to high risks and the capacity across the networks to respond effectively is mixed. Given the criticality of the services provided by Government and the threats posed to these, it is clear that a comprehensive programme of activity is required in this area.

The NIS Directive has introduced many requirements for the protection of network and information systems of critical infrastructure. As per the Directive, the NCSC has created a register of all Operators of Essential Services in the State. Many of these Operators will require support and assistance as they navigate the implementation of the security requirements set out in Article 14 of the Directive. With this in mind the NCSC has drafted security guidelines to assist OES in identifying the necessary measures to be taken to protect their information infrastructure from threats, risks and vulnerabilities.

Every Government Department and Agency is responsible for the security of its own networks and data, with the Office of the Government Chief Information Officer (OGCIO) providing network connectivity to all of Government, as well as steering cross Government policy on some aspects of IT Governance. The NCSC has assisted and supported public sector bodies by (a) providing timely and accurate information, (b) providing an expert analytical service, and (c) providing an incident response and coordination capacity. The NCSC has also begun to take a more engaged approach as its capacity has developed. Along with the Monitor Programme, which is being rolled out to a number of Departments in a pilot phase, the NCSC has also issued a 'Five Point Guide' to all Departments setting out a baseline for the security of Government ICT, and offering training and assistance to Departments. Other objectives have been introduced by the EU eGovernment Action Plan 2016-2020 and Irelands Public Service ICT Strategy 2015 to ensure that appropriate governance is in place to create integrated service while allowing openness and transparency between the Government and the public.

Question 2

> *"Are further steps/measures required to protect critical national infrastructure, including those sectors outside of those covered by the NIS Directive?"*

Question 3

> "*In relation to meeting the threats posed to integrity of the electoral process, what are the key Cyber Security measures that should be taken, and how might these contribute to the national response to hybrid threats?*"

Question 4

> *"Government IT systems are owned and operated by a wide range of operators; what measures should be taken to ensure that public services and data are secured to a uniform and high degree, with reference to governance, staffing, organisation and training?"*

Question 5

"Are public information campaigns focused on general messages around online fraud and phishing attacks aimed at individuals useful, or should the focus of public information campaigns be on measures designed to assist small and medium businesses in mitigating risks to their businesses and data, or are both issues equally important?"

Develop

For many years Cyber Security has operated in the background but with the rise of the Internet of Things cyber security has become a real issue for every citizen. The growth of digital technology means the need for a skilled cyber security workforce is of critical importance. To develop, we need to enlarge the pool of cyber security experts and enhance user proficiency. Ireland must therefore focus on developing skills and raising awareness and understanding of Cyber Security. As mentioned above there is an ongoing shortage of cyber security skills with less young people seeing cyber security as a valuable career path. Our next strategy intends to place an increased focus on developing skills and raising awareness among citizens, businesses and government bodies.

The Cyber Security Skills Initiative was launched in October 2018 and is a three year plan focused on building training and accreditation in the field to address skills gaps. The NCSC will continue its partnership in this initiative and proactively promote it.

Question 6

"What are the key challenges initiatives and measures are required to develop the Irish cyber security industry, with particular regard to supporting the research and development agenda"

Question 7

"What kind of measures could be undertaken by Government to improve the availability of skilled workers in this field?"

Question 8

"How might the relationship between academia and industry be facilitated to ensure that third level institutions are providing and developing the skills that industry require?"

Engage

Increased engagement in the national and international arenas is critical to better understand and respond to a constantly changing threat environment. The Cyber Security community in Ireland has a considerable amount of technical and procedural knowledge which should be tapped into to refine our strategic approach and future objectives.

Developments globally have also brought focus and increased attention to the field of Cyber Security in terms of its implications for international relations and for peace and security. How States and citizens engage on these critical issues, and how norms of responsible State and non-State behaviour can be established and maintained is a key challenge.

Question 9

> *"What concrete structures can be put in place so that developments in Cyber Security community (industry, academia and prospective workers in the area) are clearly understood by Government, and vice versa?*

Question 10

> *"What role should the State play in the international discussion around Cyber Security, responsible State and non-State behaviour, and the responsibilities of private industry?*