Rialtas na hÉireann
Government of Ireland

National Cyber Security Strategy

2019-2024

Table of Contents

Executive Summary

Ireland ranks among the leading EU Member States in terms of the uptake and use of digital technologies. Like the rest of the developed world, these technologies have come to play a central role in supporting and facilitating economic and social life. Ireland has also gained very significantly in economic terms from development of a global data ecosystem; our geographic position, open economy and EU membership have ensured that we have become host to a significant amount of data and economic activity.

However the progressive development and deployment of the internet and its constellation of connected devices has been accompanied by an increasing dependence on these systems. This dependence has created a complex and evolving set of risks, some of which flow from flaws in the design or operation of systems, leading to unexpected loss of service. Others exist as a consequence of deliberate actions by organised groups, including Nation States, seeking to subvert or compromise these systems for a range of reasons. These compromises can take the form of theft or destruction of data or money and the physical disruption or destruction of services or infrastructure. In turn, these risks have a complex and interrelated set of consequences for States, ranging from the protection of citizens data, to the protection of key infrastructure and services.

Cyber Security is often defined as the means of ensuring the confidentiality, integrity, authenticity and availability of networks, devices and data. However, as network and information systems become more embedded and complex, securing these becomes simultaneously more important and difficult. While these responses have evolved quickly in an attempt to keep pace with technological and market developments, this process is made vastly more challenging by the extremely dynamic nature of developments, both in terms of technology and in terms of the global strategic environment.

Ireland's first National Cyber Security Strategy was agreed by Government and published in July 2015. It set out a road map for the development of the National Cyber Security Centre (NCSC) and a series of measures to better protect Government data and networks, and critical national infrastructure. This period since that time has seen the NCSC grow significantly in scale and capacity, and the introduction of EU Network and Information Security Directive 2016/1148 (NIS Directive), a significant set of measures to support Government Departments and Agencies in managing their systems.

Furthermore, approximately 70 critical national infrastructure operators have been legally designated as such, and have been made subject to binding security requirements and to a binding incident notification requirement. Together, these mean that the State and critical

national infrastructure operators are far better prepared to deal with cyber security related risks than before.

The technology sector is characterised by its extreme dynamism however, and it appears likely that a fresh wave of developments are about to emerge, centred around virtualised networks using advanced communications protocols (such as 5G), Artificial Intelligence and the Internet of Things. In turn, these recursively linked developments will likely have a vast range of use cases, meaning that they will penetrate further into the lives of citizens and the key infrastructure that services depend on. Moreover, the software based nature of this technology is such that new regulatory and governance tools are likely to be required to ensure that both data and services are resilient and secure.

These developments have been accompanied by the rapid growth of a global industry providing products and services aimed at securing digital systems and infrastructure. With over 6,500 people employed in the cyber security sector in Ireland, the industry is already a key part of the technology sector here, both in its own right and as an enabler for investment in related sectors here. Sustaining and building on this success is an essential part of ensuring future economic growth and high value jobs, and also ensuring that a cyber security ecosystem with adequate critical mass exists in the State.

The integration of digital technologies at a national level remains an ongoing process also, and one that has seen considerable Government action. The 2015 Public Service ICT Strategy has been augmented by ‘Our Public Service 2020’, a new policy framework designed to build on these previous reforms while expanding the scope of reform to focus on collaboration, innovation and evaluation. At a national level, the National Broadband Plan will ensure that more than half a million people will have access to high speed broadband for the first time, and the forthcoming National Digital Strategy will set out how Government intends to ensure that the benefits of digitisation are available for all. Taken together, these will continue to have positive effects on economic growth, regional balance and individual opportunity; however this digitisation also brings a degree of risk.

This Strategy sets out how Ireland will embrace these challenges, and also how we plan to take advantage of the enterprise and job creation opportunities flowing from these global technological developments. This Strategy sets out a series of measures designed to address some of the complex challenges associated with sustaining and growing the number of people employed in this sector.

Lastly, the development of network and information security as a key policy theme has important international dimensions also, both in terms of the centrality of internet governance and, critically, in the general diplomatic sphere. Cyber Security is a first tier international relations issue; this Strategy establishes how Ireland will continue to play a role in shaping this environment at a global level.

Measures

Government will, over the period 2019-2024, implement the following systematic measures to protect our nation, to develop our cyber security sector, and to deepen our international engagement on the future of the internet.

1	The National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents and developing threats in the State.
2	Threat intelligence and analysis prepared by the National Cyber Security Centre will be integrated into the work of the National Security Analysis Centre.
3	The existing Critical National Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programmes to mitigate risks to key services.
4	The NCSC, with the assistance of the Defence Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber attack.
5	The existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system.
6	The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of Critical National Infrastructure.
7	Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.
8	The NCSC will develop a baseline security standard to be applied by all

	Government Departments and key agencies.
9	The existing 'Sensor' Programme will be expanded to all Government Departments, and an assessment will be conducted as to the feasibility of expanding Sensor to cover all of Government networks.
10	A Government IT Security Forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.
11	The NCSC will be tasked by Government to issue recommendations with regard to the use of specific software and hardware on Government IT and telecommunications infrastructure.
12	Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.
13	Science Foundation Ireland (SFI) will promote cyber security as a career option in schools and colleges by means of their Smart Futures Programme.
14	Science Foundation Ireland, along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes, to fund a significant initiative in Cyber Security Research.
15	Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/Government cyber security collaboration.
16	Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community that leads to the practical application of research in business.
17	We will reinforce Ireland's diplomatic commitment to cyber security, including by stationing cyber attaches in key diplomatic missions and by engaging in sustainable

	capacity building in third countries.
18	We will create an interdepartmental group (IDG) on internet governance and international cyber policy to coordinate national positions across Departments.
19	We will deepen our existing engagement in international organisations, including by joining the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia.
20	Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision.

A detailed implementation plan of actions relating to these measures, including timelines and responsible organisations, are set out in the accompanying Annex.

1 Introduction

Ireland is among the leading ranks of EU Member States in terms of the uptake and use of digital technologies (7th out of the 28 EU Member States in the European Commission Digital Economy and Society Index (DESI) 2019). In practical terms, this means that the internet and the vast array of technology and devices connected to it have played a central role in delivering and enabling our economic success. Moreover, they have also allowed for considerable improvements in productivity and quality of life, and for greater efficiency and sustainability in the use of resources. However, these same technologies also bring with them an embedded set of risks and vulnerabilities. This is a dynamic issue; it is rendered more complex and challenging as systems become more embedded, connected to the internet and integrated into virtually every aspect of our lives.

Meeting this challenge, both in terms of the resilience of key infrastructure and services and the ability of the State to manage and respond to incidents is already critical to the social and economic wellbeing of the State and its people. It is not a simple task. Cyber security brings with it a complex web of issues to be dealt with. Internet enabled and connected technologies already permeate every aspect of our lives, both at a personal level and in providing the services that we rely upon. The diverse nature of these various sectors, with different ownership models and technologies, means that there is no single model or solution, technical or otherwise, that will suit every sector. In formulating a national response, a dynamic and flexible approach is required, one in which different solutions are applied according to the nature of the sector and to the risk posed to society, to human life, and to the economy.

The global nature of the internet has significant geopolitical implications also - infrastructure of any kind attached to the internet is vulnerable to threats from anywhere on the planet. As such, the geography of national security has changed, posing some profound national security policy questions for Ireland. In the first instance, the global management of the Internet, how it is governed and how States and others behave and act, is now a key national concern. Secondly, the security of every process, service and piece of infrastructure in Ireland, from the electoral process through to military infrastructure and the security of public sector data has to be approached in a different way, because they are all, to some extent, dependent on connected devices and can now be targeted directly from anywhere on the planet.

Lastly, the nature of our economy has changed radically. Ireland is home, according to some estimates, to over 30% of all EU data, and to the European Headquarters of many of the

world's largest technology companies. Our economic success is therefore closely bound up with our ongoing ability to provide a secure environment for these companies to operate here.

The security of our network and information systems is therefore crucial for the continued economic and social development of Irish society. The first National Cyber Security Strategy, published in 2015, has resulted in the establishment of a functional and evolving National Cyber Security Centre, and the development of a comprehensive set of measures around protecting key critical national infrastructure and the security of Government systems and data. Given the expanding nature of the threat and the evolving complexity of systems, this Strategy takes a broader perspective and sets out a series of measures that go well beyond those in the 2015 Strategy. These measures also embrace a broader set of issues than before; there are challenges around skills, enterprise development and research that require specific actions.

The process for drawing up this Strategy was managed by a High Level Steering Group, chaired by the Department of Communications, Climate Action and Environment, with representation from the Department of the Taoiseach, the Department of Foreign Affairs and Trade, the Department of Employment and Social Protection, the Department of Defence, the Office of the Chief Government Information Officer, the Department of Justice and Equality and the Department of Business, Enterprise and Innovation.

The process was also guided by a set of consultation mechanisms. Firstly, a set of five sector specific engagement groups were drawn together, comprising of stakeholders from across the public and private sector. These groups covered National Security and Policing, Enterprise Development, Skills and Research, Public Sector ICT Security and Critical National Infrastructure Protection, and were designed to ensure that the Strategy was comprehensive and accurately reflected the diverse range of issues to be tackled. These groups were each convened twice, once before the public consultation to ensure that the consultation document and questions were appropriate, and to identify those fundamental concerns affecting each sector. The second meeting occurred after the public consultation was closed, and the groups were provided with the outcome of this, and with the proposed outcome of the Strategy. These groups provided a forum in which participants could freely voice opinions, concerns and ideas, and were extremely valuable in framing and contextualising the Strategy, and in identifying solutions to some of the challenges faced.

A public consultation was run between March and May 2019, in which a brief draft of the strategy was published as part of a public consultation process to gather the views of the public and wider industry. Members of the public had 30 working days to make submissions

of the draft brief of the strategy, and a total of 47 submissions were received. These submissions were then assessed by the Steering Group and the five sector specific engagement groups, and the suggested measures from each were extracted and tabulated for further analysis. This analysis also involved an assessment of more than 30 national strategies from across Europe and beyond, as well as best practice documents from bodies like the OECD and ENISA.

2 Vision

Our vision is of an Irish society that can continue to safely enjoy the benefits of the digital revolution and can play a full part in shaping the future of the internet. To that end, we will;

Protect the State, its people and critical national infrastructure from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs.

Develop the capacity of the State, research institutions, businesses, the public sector and of the people to both better understand and manage the nature of the challenges we face in this space and to ensure that businesses and individuals can continue to benefit from economic and employment opportunities in information technology, and in particular in cyber security.

Engage nationally and internationally in a strategic manner, supporting a free, open, peaceful and secure cyber space, and ensuring that cyber security is a key component of our diplomatic posture across the full range of engagement.

3 Objectives

- To continue to improve the ability of the State to respond to and manage cyber security incidents, including those with a national security component
- To identify and protect critical national infrastructure by increasing its resilience to cyber attack and by ensuring that operators of essential services have appropriate incident response plans in place to reduce and manage any disruption to services
- To improve the resilience and security of public sector IT systems to better protect data and the services that our people rely upon
- To invest in educational initiatives to prepare the workforce for advanced IT and cybersecurity careers
- To raise awareness of the responsibilities of businesses around securing their networks, devices and information and to drive research and development in cyber security in Ireland, including by facilitating investment in new technology
- To continue to engage with international partners and international organisations to ensure that cyber space remains open, secure, unitary, free and able to facilitate economic and social development
- To increase the general level of skills and awareness among private individuals around basic cyber hygiene practices and to support them in this by means of information and training

4 Risk and the Information Society

From its very origins as ‘Arpanet’ in the United States in the 1960s, the internet was designed to be an open system that allowed any one point on a network to receive messages from any other point, and to allow information find multiple routes from one point to the other. Despite the fact that there are now billions of connected devices connected to a network that spans the globe, that fundamental principal persists, and in fact has been central to the rapid growth of the internet and its utility to humanity.

However this openness and ease of connection also facilitates the use of the network for malicious activities. Over time, and as the internet has grown in importance, the potential range and impact of such actions have grown, bringing with them a wide range of new risks to critical social and economic functions. This Section outlines those key risks for Ireland.

4.1 Strategic Risks

At a very high level, developments in cyber security pose two fundamental challenges for Ireland. Firstly, the a-spatial nature of the internet exposes the State to new and rapidly developing global threats, including those developed and deployed by threat actors with very significant resources and expertise. These threats manifest at a national level in a variety of ways that make detecting and mitigating the associated risks difficult. The fact that the global security environment is in a particularly dynamic phase is also pertinent; the apparent return of ‘great power’ politics in international relations, accompanied by tensions over trade and technology vendors, pose particular challenges for small, open economies like Ireland.

Secondly, the technological base of the Irish economy has developed significantly in recent years; the State is now home to a large proportion of Europe’s data (upwards of 30% according to some industry assessments) and the European headquarters of a number of the world’s largest technology firms. Critically also, the conceptual evolution of cloud computing has had profound implications for Ireland. In many cases, rather than being passive repositories of data, these centres are now home to live operational software environments; an outage or incident affecting one of those facilities could therefore have immediate disruptive effects on infrastructure or business across the EU or globally.

In turn, this means that the infrastructure supporting these centres, public and private, now has an elevated security and economic risk associated with it.

Recent years have seen the development and regular use of very advanced tools for cyber enabled attacks and espionage, and, likely for the first time, the physical destruction of Critical National Infrastructure by cyber enabled means. As such, the field of cyber security

is characterised by an ongoing and high stakes technological arms race, between attack and defence.

The nature of network connected infrastructure adds a further complexity. Firstly, these are ultimately global systems, both in terms of the supply chains for devices and software and in terms of the network that links them together; this means that any single State can only exercise a degree of control over the operation of the network in its territory. Also, and critically, these devices and systems are owned by a very wide range of types of businesses and organisations. In fact, many private homes already have several connected devices, something that is likely to become more prevalent with the ongoing rise of the Internet of Things ('IoT'). This means that coordinating protective measures or responses to incidents or attacks across this very wide range of potential targets is a very complex challenge. Moreover, unless Governments are willing to insist on an intrusive system of monitoring, they have limited options available to them to predict or prevent all attacks or incidents on their territory or against their citizens or infrastructure. The challenges in this space extend to the most fundamental; the nature of cyber-attacks have often been such that many of them have traditionally not been reported or publicised, posing an obvious issue for Governments in understanding and responding to the underlying question.

The increasingly complex and dynamic nature of the security challenges facing the State have already been recognised by Government with the establishment of a Cabinet Committee dealing with national security matters. The Government has also established the National Security Analysis Centre (NSAC) which will work across Government to support a coherent approach to assessing, understanding and addressing national security challenges, resulting in enhanced strategic advice for Government.

4.2 Hybrid Threats

One of the more challenging issues to emerge in recent years has been the active use and refinement of hybrid threats. These threats are defined by the EU as being "*multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary* ", and have arisen in a number of EU countries in the recent past. Many of these threats have had a cyber component, the most common of which has been the use of cyber tools to steal information for subsequent use in disinformation campaigns (so called 'hack and leak'). By their nature, these campaigns are designed to be difficult to detect, and because of their explicitly political goals, even more difficult for public authorities to counteract.

As an open liberal democracy, Ireland is vulnerable to campaigns of this type in much the same way as other EU Member States. In December 2017, the Government established the first 'Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation', which is coordinated by the Department of the Taoiseach. The 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 third parties. 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. At a European level also, there has been significant work, including the creation of the Hybrid Fusion Cell, set up in the European External Action Service to facilitate the rapid sharing of information relating to the potential hybrid type actions affecting multiple EU Member States.

4.3 Risks to Critical National Infrastructure and Public Sector Systems and Data

While general risks arise for society as a consequence of developments in cyber space, there are particular sectors in which these incidents have potentially far greater implications. In broad terms, these include those infrastructure sectors that are critical for societal and economic functions, often termed Critical National Infrastructure (CNI), and Public Sector Systems and Data.

The traditional conceptualisation of CNI has encompassed the energy and transport sectors, the financial services sector, healthcare and the telecommunications system itself. Government IT systems, in turn, are central to the delivery of many functions that are essential to allow a modern society to function, including social services and payment systems, tax collection and the functioning of democracy.

Recent decades have seen the development and use of tools to compromise, disrupt and even destroy these systems. These threats have emanated from a wide range of actors, varying in terms of access to resources and capability. These range from individuals acting alone or in small groups engaged in nuisance type attacks, such as website defacement and small scale denial of service attacks, through to 'hacktivists', criminals of various scales, and Nation States. Among the higher level threats, organised criminal gangs are often

indistinguishable from Nation States in that they sometimes deploy advanced techniques to infect and compromise networks and data.

Lastly, at the top of this pyramid, are those State sponsored 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. These threat actors, usually referred to as ‘advanced persistent threats’ (or APTs) have been shown to be involved in attacks across a wide range of sectors, but with a particular focus on Government IT systems, telecommunications networks, financial services and technology companies. The resources at their disposal, their persistence and their expertise mean that that these entities pose a very particular challenge, they are difficult to detect and difficult to remove and therefore pose a serious and ongoing challenge to the security of network and information systems.

Historically, States could hope to secure both Critical National Infrastructure and public sector systems and data 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 are as effective in the digital age. Moreover, for practical and legal reasons, Governments generally do not have visibility of, or cannot secure, the vast range of devices in their territory 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.

For much of the period until 2016, the approach taken by many National Governments has been to support organisations by providing information as to threats and to risk mitigation measures, and by providing an incident response function. In Ireland, the signing into law of the 2018 Network and Information Security Regulations (S.I. 360 of 2018) has resulted in a far more proactive approach to the protection of Critical National Infrastructure, including the formal identification of operators, and the commencement of a programme of security measures that include assessments and audits of compliance, in line with measures being taken across Europe. These will, over time, result in an increase in the resilience of these key services against attack or incident. Risks remain however, both in those sectors covered by the NIS Regulations and outside of these.

In the first instance, the adherence to the security measures in the NIS Regulations is a risk reduction methodology, not a guarantee of absolute security. Secondly, the NIS Directive and Regulations are explicitly limited to seven named sectors. Both the assessment of Critical National Infrastructure carried out by the NCSC during the designation process and

the application of the security measures after designation have shown that some of the infrastructure in the State outside of the scope of the NIS Regulations is in fact also critical, and that there are a number of interdependencies between Critical National Infrastructure sectors that are likely to give rise to particular risks.

Although the security of public sector ICT has seen considerable investment and attention, not least due to the advent of the General Data Protection Regulation, the nature of the sector poses some particular challenges. Some Departments and Agencies can readily demonstrate compliance with international best practice (and international standards like ISO27001) but challenges remain in ensuring a consistently high level of security across Government Departments and agencies. Particular issues remain around the formal governance of ICT security, both in general and in the context of national classified information and classified information of other States and international bodies. Similar issues exist in obtaining Facilities Security Clearance for companies engaged in the handling and storage of confidential information. Some measures are being developed to deal with these challenges, including the growing use of (and plans for) shared IT infrastructure between Departments, but some fundamental challenges remain.

Critically, ongoing technological developments, including revolutions in telecommunications are likely to render this situation even more complex. In allowing for low latency and high bandwidth transmission of information, the deployment of 5G technologies will likely serve as a key enabling infrastructure for a series of other technologies and use cases.

These potentially include customer facing services like autonomous vehicles, eHealth services and entertainment, and industry oriented services. On that basis, it seems likely that 5G networks will form the backbone of a new set of services critical to the operation of vital societal and economic functions. The nature of these networks and technology is relevant also; being software defined and virtualised means that new types of security measures will likely be required in this sector to ensure the security of both the 5G network and of the services dependent on it.

4.4 Citizen and Business

For private citizens, of all ages, many of the issues associated with cyber security are closely related to online safety and the prevention of cyber crime. These matters usually refer to the online behaviour of individuals, or the manner in which they maintain or use their personal or home devices. These risks involve the potential loss of data to cryptoware attacks, or the loss or theft of personal information including credentials or bank details.

For businesses, one of the more common and more damaging outcomes of the rise of malicious online activity relates to attacks on businesses for financial gain. Despite an increased level of awareness, Cyber Crime incidents in Ireland are increasing with 61% of Irish organisations reported to have suffered cybercrime such as Fraud in the last two years with an estimated loss on average of €3.1m.

5 National Capacity Development

5.1 State of Play

Until 2011, governmental responsibility for cybersecurity in Ireland was spread across a number of different organisations, including both military and civilian authorities. In July 2011, the Government decided to establish the National Cyber Security Centre (NCSC) in what is now the Department of Communications, Climate Action and Environment, bringing responsibility for all cyber security matters into one operational unit. This decision was based on a detailed analysis of the evolving threats to security, and an assessment of the most appropriate type of organisation to respond to issues and to proactively improve the resilience of key infrastructure and services. This organisational concept has since come to represent best practice in Europe, primarily because it allows for the creation of a single critical mass of experience and operational expertise, and for the end to end management of incidents of all types.

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 National Infrastructure in the State. These measures focusing capacity development within the NCSC on the Computer Security Incident Response Team (or 'CSIRT'), and a parallel series of measures aimed at 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 NIS Directive, and how the national incident response process would be developed through ongoing participation in the National Emergency Management System.

The initial focus of the NCSC was to be in the creation of a Computer Security Incident Response Team, within the organisation. CSIRTs are an internationally recognised organisation type with a set of formal roles around cyber security incident response and information sharing. At their most basic, they are designed to act as focal points for information; by taking in and anonymising incident reports from victims, and then sharing the technical details of both incidents and mitigation strategies with their constituents (those bodies they have been assigned to assist), they can ensure that the broader constituent group has a higher degree of situational awareness as to what is occurring.

In this way, CSIRTs are expressly designed to obviate some of the structural challenges emanating from the fragmented ownership of IT systems.

The CSIRT in the NCSC, called CSIRT-IE, went through an extended phase of capacity building and upskilling. In the early stages, the focus was first on the primary tasks of being able to securely and professionally manage and track incidents and share information with constituents. To do so requires both a pool of trained and experienced staff, and a secure stand-alone IT infrastructure. These have been very significantly developed since 2015, and have resulted in the creation of an expert unit with significant capacity in the full range of cyber security incident response functions. The Defence Forces and An Garda Síochána were central to the early stages of this process, providing both seconded staff and expertise in security, process development and threat intelligence assessment. Also, the UCD Centre for Cybercrime Investigation has been critical in the development of cyber security skills in Ireland; much of the knowledge base that established the NCSC flowed from students and staff of UCD.

The development of the CSIRT's operational capacity was designed to lead to a point where the unit would have a high degree of situational awareness as to cyber security activity in the State, and would have a network of 'constituents' with which it could securely share the technical details of incidents, in an anonymised fashion, to allow them take measures to protect their systems and services. These constituents include Government Departments and agencies, and Critical National Infrastructure operators, and number in excess of 130 entities. However, the NCSC was involved in a number of serious cyber security incidents in 2016 and 2017 which pointed both to issues not comprehended in the Strategy. The analysis of these incidents pointed to the need to evolve some of the tools of the NCSC to better respond to future incidents. As such, the NCSC took a series of initiatives during this period to support both critical national infrastructure operators and Government stakeholders. Examples of this include: (i) formalising and augmenting the system of advisories and alerts (which flowed from lessons learned in the incident management process for WannaCry2 and NotPetya), and (ii) the formation in 2017 of the Threat Sharing Group, which acts both as a forum for critical national infrastructure operators, and a means for State Actors (including Gardaí and Defence Forces) to share information with these operators and to engage with cyber security professionals. These same incidents also reinforced the centrality of cyber security to the key security challenges facing the State, and of the need for ongoing and close cooperation with the State's security services on operational matters.

The NCSC has developed significantly in terms of capacity and resources, and its roles have been formally established in law, including responsibilities around Critical National 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 NIS 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]".

The CSIRT received its first international accreditation in late 2017, (Trusted Introducer accreditation), signifying that the team had reached a defined level of best practice and maturity. 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 to over 130 members. This base now includes Government Departments and Agencies, and key entities across the Financial Sector, Critical National Infrastructure (CNI) providers and other Operators of Essential Services (OES).

Since that period, the CSIRT has further developed its incident response capacity by means of an integrated incident response and analytics platform, and a highly augmented system of advisories to constituents across Government and Critical National Infrastructure. Furthermore, the CSIRT has pivoted from a solely reactive stance to a more proactive position. This includes the deployment and use of MISPs (Malware Information Sharing Platform) to share threat intelligence directly with Critical National Infrastructure Providers, and the evolution and use of a series of tools to identify, parse and analyse open source intelligence (OSINT). The CSIRT has also developed, tested and deployed the 'Sensor' platform, now operational on the infrastructure of a number of Government Departments, to detect and warn of certain types of threat.

The evolution of the NCSC was accompanied by developments in related areas. 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*

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

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*". As such, the role of Defence Forces with regard to cyber security is explicitly a supporting one, with their primary responsibilities in this area relating to the protection of their own systems. This supporting role has evolved over time, and the Defence Forces continue to play a central role in facilitating the operations of the NCSC. The NCSC maintains close cooperation with the Defence Forces and the Gardaí on national security issues, and has a secondment arrangement with both entities.

An Garda Síochána also have a set of responsibilities in the sector, both in preventing, investigating and prosecuting cyber-crime and as a consequence of their national security roles. Their capacity and organisation has evolved somewhat in recent years, as the Computer Crime Investigation Unit (established in 1991) was 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. In addition, the bureau conducts investigation into cyber dependent crime including network intrusions, data interference and attacks on websites belonging to Government Departments, institutions and corporate entities, An Garda Síochána has invested heavily in the area, with a particular focus on developing capacity in the regions. The NCSC and Garda National Cyber Crime Bureau have developed a positive co-operative relationship with ongoing shared training and secondment opportunities for staff.

Key Developments

1. The CSIRT has been made fully operational and internationally accredited.
2. The information sharing and outreach programmes operated by the NCSC have very significantly developed, including by means of the deployment of Malware Information Sharing Platforms (MISPs).
3. The CSIRT has developed, tested and deployed the Sensor platform.
4. The Garda National Cyber Crime Bureau has been established, and the capacity of the organisation significantly augmented.
5. The National Security Assessment Centre has been established in the Department of the Taoiseach.

5.2 Objective

To continue to improve the ability of the State to respond to and manage cyber security incidents, including those with a national security component.

5.3 Measures

The National Cyber Security Centre (NCSC) will remain the primary Cyber Security authority in the State, and will further develop its capacity to deliver on its two key roles; leading the national response to cyber security incidents and building the resilience of key networks and devices across the State. The core response element of the NCSC will continue to grow, and its pivot from a reactive stance towards a proactive one will be maintained, including by means of new ways of detecting threats before they impact on services and citizens. By the end of 2022 the NCSC will also have a number of new and expanded roles in protecting Government networks and data, and will continue to work with the Office of the Government Chief Information Officer to develop and implement policies and practices relating specifically to Government and public services.

1. **The National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents and developing threats in the State.**

   The CSIRT within the NCSC will be developed into a 'Joint Security Operations Centre' (or JSOC) by the end of 2020 to better support the security of both Government ICT, and Critical National Infrastructure. Separate specialist teams will be formed within the JSOC, including Threat Intelligence, Incident Response and Network Monitoring. This will facilitate the ongoing development of the response team while allowing for the maintenance and progressive development of the capacity of the NCSC to monitor network activity across Government and Critical National Infrastructure. This unit will continue to function as the national point of contact for all cyber security incidents, and will continue to lead the response to cyber security incidents of all scales.

2. **Threat intelligence and analysis prepared by the National Cyber Security Centre will be integrated into the work of the National Security Analysis Centre.**

   The National Security Analysis Centre (NSAC) in the Department of the Taoiseach will play a central role in coordinating the strategic analysis of threats to National Security,

and in providing improved situational awareness to Government. The NCSC will assist in ensuring that new and emerging cyber security challenges that have a national security impact are fully reflected in the work of the NSAC, including in the development a new National Security Strategy.

Measure 1: The National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents and developing threats in the State.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Develop detailed technical and organisational plan for the JSOC.	Q4 2020	NCSC	DCCAE
2	Receive sanction for resourcing and staffing for NCSC expansion.	Q2 2021	NCSC	DCCAE, D/PER
3	Build prototype JSOC in interim facility	Q4 2021	NCSC	OPW, DCCAE
4	Commission Final JSOC Facility in NCSC HQ	Q2 2023	NCSC	OPW, DCCAE

Measure 2: Threat intelligence and analysis prepared by the National Cyber Security Centre will be integrated into the work of the National Security Analysis Centre.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish Formal Reporting and Information Sharing arrangements with NSAC	Q1 2020	NCSC	NSAC

6 Critical National Infrastructure Protection

6.1 State of Play

Until relatively recently, accepted best practice in Europe for the protection of critical national infrastructure and services against cyber-attack involved two types of actions, (1) the creation of a national incident response function such as the NCSC, and (2) instituting formal information sharing arrangements whereby information relating to threats to this infrastructure could be shared with owners and operators, including urgent information relating to imminent threats. The NCSC established and still runs precisely these services and has worked, on an ongoing basis, with utility operators and with similar bodies in other jurisdictions to manage risks to Critical National Infrastructure in Ireland, including the active management of ongoing incidents.

However, experience over time across Europe and elsewhere has made it clear that there is a risk asymmetry between the public interest and that of many operators of this type of infrastructure. In many cases, critical services remained vulnerable despite comprehensive attempts by Government to provide information and support to operators. As such, and building on work underway in some EU Member States and on previous Directives in Telecommunications, the European Commission published a draft of the 'Network and Information Security Directive' in 2013. This NIS Directive, which was formally agreed in 2016, included a series of measures aimed at improving the resilience of Critical National Infrastructure across 7 different sectors (including energy, transport, drinking water, banking, financial markets, healthcare and digital infrastructure). These measures include requiring Member States to formally assess their infrastructure, and legally designate so called 'Operators of Essential Services' – those entities that are critical to the provision of these services in each State. Moreover, these entities are required to be made subject to a formal set of security requirements, and to a binding incident reporting requirement. As such, the NIS Directive aims to (a) compel improvements in the security and resilience of Critical National Infrastructure, and (b) improve State awareness of cyber security incidents across Europe, and (c) allow for greater consistency and coordination of response at an EU level.

The 2015 strategy was written in anticipation of the NIS Directive, and detailed work was underway from before the Strategy was complete on a detailed assessment of Critical National Infrastructure in Ireland, which included an Infrastructure Interdependency Study with the UK (completed mid in 2017). These assessments were then used to derive a national list of Operators of Essential Services (OES), which were formally designated following the transposition of the NIS Directive in Ireland in September 2018 by S.I. 360 of

2018. Enforcement powers under the NIS Regulations allow Authorised Officers of the NCSC to conduct security assessments and audits in 5 of the 7 sectors (the Central Bank of Ireland retains responsibility for the application of security measure to the Financial Services sectors), and require the provision of information and issue binding instructions to remedy any deficiencies. The NCSC has also prepared detailed guidance documents relating to security measures, compliance and incident reporting to provide additional support to the OES, which were published for public consultation in January 2019.

For the purposes of this document Critical National Infrastructure is defined as "… *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of failure to maintain those functions*." The aim of Government is to secure our CNI from attack by mandating that measures are taken by operators to manage risks to this infrastructure, including by having appropriate incident response plans in place to cope with any disruption to services.

The progressive dependence of Critical National Infrastructure and services on network connected devices has led to the State taking a series of measures to ensure the resilience of certain categories of critical national infrastructure. However, given the nature and extent of the risk, and because of developing technologies, this system needs to be further developed and expanded. To that end, Government will take the following measures to further protect Critical National Infrastructure and services;

Key Developments

1. The Critical Infrastructure Protection methodology set out in the EU NIS Directive has been implemented.
2. This has resulted in the designation of Operators of Essential Services across 7 key sectors, and the commencement of a series of formal assessments of readiness by Operators.
3. The introduction of tailored information sharing mechanisms to share sensitive information with key Operators.

6.2 Objective

To identify and protect critical national infrastructure by increasing its resilience to cyber attack and by ensuring that operators of essential services have appropriate incident response plans in place to reduce and manage any disruption to services.

6.3 Measures

The NCSC will also continue to implement its existing Critical National Infrastructure protection programme, premised on the already implemented NIS Directive process, but will significantly evolve this, based on a broad ranging piece of analysis. It will be supported in this in particular effort by the Defence Forces and An Garda Síochána, and will engage across Government to ensure that cyber security concerns are integrated into all relevant policy matters.

3. **The existing Critical National Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programmes to mitigate risks to key services.**

   The main objective of the NIS Directive is to ensure that there is a high common level of cyber security across Member States. The NCSC is the national competent authority charged with providing guidance on the security of Critical National Infrastructure, and with auditing the application of security controls for many of these sectors. The NCSC will continue to develop and apply these measures to ensure that the NIS Directive is fully applied in Ireland, and that this application keeps pace with changes in technology and best practice.

4. **The NCSC, with the assistance of the Defence Forces and An Garda Síochána will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber attack.**

   Building on the existing assessment process conducted under the NIS Directive, the NCSC will conduct a detailed risk assessment of the vulnerability of all Critical National Infrastructure and services to cyber attack. This will include an assessment of the criticality of a wide variety of services and a mapping of interdependencies between these. The output from this process will inform the expanded scope of the existing cyber security Critical National Infrastructure protection process.

5. **The existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system.**

We will broaden and deepen the existing regulatory system for the cyber security of CNI to include a wider range of operators across a broader range of sectors and to allow for the closer monitoring of compliance. This expanded system is likely to include aspects of higher education and electoral systems and will build upon the work already in place as a consequence of the NIS Directive.

6. **The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of Critical National Infrastructure.**

The existing cyber security information sharing forums, such as the 'Threat Sharing Group' (TSG) and the 'All Island Information Exchange' (AIIE) will be substantially developed.

7. **Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.**

We will introduce a new and specific set of security requirements for the telecommunications sector, with detailed risk mitigation measures to be developed by the NCSC to assist Comreg in fulfilling their statutory functions under existing EU Security Regulations (transposed by S.I. 333 of 2011), and the forthcoming EU Telecommunications Code (Directive 2018/1972)

Measure 3: The existing Critical Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programmes to mitigate risks to key services.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Complete first phase of Operators of Essential Services (OES) Self-Assessment against Security Control Framework	Q1 2020	NCSC	Designated OES
2	Commence Security Control Testing of Operators of Essential Services (OES)	Q3 2020	NCSC	Designated OES
3	Reassess Register of Designated OES	Q3 2020	NCSC	

	and Security Guidelines			
4	Security Control testing post incidents, and ongoing audits of OES compliance	Ongoing	NCSC	Designated OES

Measure 4: The NCSC, with the assistance of the Defence Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber attack.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Steering Group formed and terms of reference for the review agreed	Q1 2020	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA
2	Information gathering phase complete, and methodology agreed	Q3 2020	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA
3	Complete Assessment Process, including international consultation and detailed assessment of cross sectoral interdependencies.	Q2 2021	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA
4	Final Report and Recommendations Complete	Q4 2021	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA

Measure 5: The existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Draft Heads of Bill for Agreement by Government	Q4 2021	DCCAE	AGO
2	Drafting Process with AGO	Q1 2022	DCCAE	AGO

3	Oireachtas Process	Q2 2022	DCCAE	AGO, Oireachtas

Measure 6: The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of critical national infrastructure.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Expand the current Threat Sharing Group (TSG) representatives to include CNI, with new Terms of Reference.	Q2 2020	NCSC	AGS, DF, CNI
2	Refine existing arrangements with the UK on information sharing and incident response, with particular reference to North-South critical infrastructure protection.	Q4 2020	NCSC	OEP, CPNI UK

Measure 7: Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Transposition of Directive 2018/1972	Q4 2020	DCCAE	NCSC, Comreg
2	Provision of Technical Support to Comreg	Q4 2020	NCSC	Comreg
3	Application of revised security measures	Q1 2021	Comreg	DCCAE, NCSC, Telecoms Operators

7 Public Sector Data and Networks

7.1 State of Play

Responsibility for the operation and security of public sector IT systems sits with individual Departments and Agencies, with the Office of the Government Chief Information Officer having an overarching role in leading the implementation of the Public Service ICT Strategy and managing the network which Departments and Agencies use to connect with each other and the wider internet. The primary role of the CSIRT within the NCSC in its early years involved establishing an incident response function to support these Departments and agencies when they reported incidents to the NCSC, and to build an Advisory system to allow for the rapid dissemination of specific information relating to threats and incidents, and best practice with regard to cyber security. The NCSC had no direct insight into activities on Government networks however, and no formal or precise means of determining what security measures might be in place in individual Departments or agencies.

On this basis, and in tandem with the ongoing development of the CSIRT and the expanding toolset that are available to all constituents, the NCSC began to rollout a project titled 'Sensor'; this is essentially an additional layer of boundary protection for Government Departments that alerts the NCSC when particular types of activity are observed transiting Government networks. Also, the NCSC issued a '5 Point Guide' for Departments in late 2018, setting out a recommended baseline of security measures that Departments might take, based on some of the common incidents that the CSIRT had reported to it over the previous period.

Key Developments

1. The Advisory system operated by the NCSC has been augmented substantially to allow for the rapid dissemination of information.
2. The NCSC has developed, tested and deployed the Sensor platform across a number of Government Departments, improving the security of IT systems and data against high level threats.
3. Government Departments and agencies have invested heavily in security, supported by guidance from the NCSC.

7.2 Objective

To improve the resilience and security of public sector IT systems to better protect services that our people rely upon, and their data.

7.3 Measures

The Public Sector relies heavily on Information Technology to deliver practically all of the services it provides; these services therefore need to be secure, resilient and capable of ensuring that personal information remains private. To that end, Government will take the following specific initiatives;

8. **The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies.**

   The NCSC, in conjunction with the OGCIO, will formulate a minimum cyber security baseline standard for Government ICT. This will be aligned with international standards and phased in across all Government bodies, beginning with Government Departments. These standards typically include measures and controls in relation to staff training, identity and access management. It is envisaged that the standard will be audited at a local Departmental level with support and guidance provided by the NCSC.

9. **The existing 'Sensor' Programme will be expanded to cover all Government Departments, and an assessment will be conducted as to the feasibility of expanding Sensor to cover all of Government networks.**

   The NCSC Sensor Programme will be rolled out across all Government Departments with a view to improving the early detection and removal of threats. The NCSC will support its application across the public sector, and the Joint Security Operations Centre will be developed to support and operationalise this system. It is envisaged that every significant Government Department and Agency will be monitored by the Joint SOC managed by the NCSC.

10. **A Government IT Security forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.**

The NCSC will lead in creating, chairing and implementing a new Public Sector IT Security forum, with Heads of IT security from across Government Departments and Agencies. The forum will meet quarterly to exchange and share information around best practice, inter organisational processes, cyber security threats and measures to comply with the new public sector cyber security baseline standard.

11. The NCSC will be tasked by Government to issue recommendations with regard to the use of specific software and hardware on Government IT and telecommunications infrastructure.

The NCSC will be tasked to issue recommendations with regard to the procurement and use of certain types of IT infrastructure and software in securing Government data and services, and to recommend the prohibition or removal of certain infrastructure from Government IT networks and communications if the NCSC determines that its presence poses an unacceptable risk to the security of Government data.

Measure 8: The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Design suitable minimum standard for Government IT, in conjunction with Government IT Security Forum.	Q4 2021	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
2	Develop detailed measures, controls and implementation procedures.	Q1 2022	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
3	Draft guidance and support materials for IT teams and Internal Audit Units on compliance assessment.	Q2 2022	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
4	Support Government Departments and Key Agencies in implementation of the baseline	Ongoing	NCSC/OGCIO/Govt IT Forum	Government Departments and key

	standard.			agencies
5	Conduct assessment of the implementation of the baseline standard	Q4 2023	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies

Measure 9 The existing 'Sensor' Programme will be expanded to all Government Departments, and an assessment will be conducted by the same date as to the feasibility of expanding Sensor to cover all of Government networks.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Deploy Sensor on the IT infrastructure of all 15 Government Departments.	Q4 2020	NCSC	All Government Departments, Gov IT Security Forum
2	Review costs and legal issues associated with the application of Sensor on Government Networks, covering all of public sector ICT, and bring outcome to Government for decision.	Q4 2021	NCSC	OGCIO, AGO, D/PER

Measure 10: A Government IT Security forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Resource the creation of Public Sector IT Team in the NCSC, and establish Terms of Reference for the Forum	Q1 2020	NCSC	OGCIO, All Government Departments
2	Plan a briefing session for all Heads of IT Security to outline the purpose of the	Q1 2020	NCSC	OGCIO, All Government

	Security Forum			Departments
3	Establish quarterly meetings of the Forum and appoint a Chairperson and Secretary	Q4 2020	NCSC	OGCIO, All Government Departments

Measure 11: The NCSC will be tasked by Government to issue Recommendations with regard to the use of specific software and hardware on Government IT and telecommunications infrastructure.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Rationale and Terms of Reference Prepared and brought to Government for Agreement	Q3 2020	NCSC	OGCIO, AGS, DF, NSAC
2	Entry into effect of NCSC Recommendation Process	Q4 2020	NCSC	OGCIO, AGS, DF, NSAC

8 Skills

8.1 State of Play

A number of substantial skills gaps have emerged in cyber security, largely as a consequence of its rapid development as a societal challenge. This skills gap is a global issue, with upwards of 2 million unfilled cyber security vacancies worldwide in 2019. At a national level, ensuring a ready supply of staff is critical to both preserving the ability to secure our own infrastructure, and to be able to continue to attract and retain data heavy investment. In turn, meeting this demand requires not only the training of new entrants but the encouragement of cross training and upskilling from professionals in ICT and other relevant sectors. In recent years Ireland has made important strides towards addressing and improving skills, developing research capabilities and raising awareness of cyber security as a career. However there remains a time lag between industry and academia in fast moving sectors like this, and a need to ensure that graduates are leaving third level institutions with the requisite skills for the employment requirements in industry.

The Government is seeking to address the growing demand for cyber security skills through the implementation of Technology Skills 2022, the third ICT Skills Action Plan. Cyber security was identified in the underlying research for the plan, undertaken by the Expert Group on Future Skills Needs, as one of the key emerging fields that will drive the demand for high level ICT skills in Ireland in the coming years. The cyber security skills agenda is being advanced in the context of Technology Skills 2022 through a number of channels, including Skillnet Ireland, the expansion of provision in higher education and the promotion of ICT apprenticeships through SOLAS, the Further Education and Training Authority.

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 is focused 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. Also, the third level sector in Ireland has also begun to offer a significant number of courses in cyber security, with at least 8 Masters level courses now on offer.

Developed by industry led consortia, apprenticeships combine both work-based and off the job training while in employment. Approved by the Apprenticeship Council and funded under the National Training Fund, apprenticeships provide a pathway to careers for school leavers, jobseekers and those looking to change career. A 2 year Associate Professional in CyberSecurity apprenticeship at QQI level 6 was launched in February 2019 with SAP as the industry lead and Fastrack to Information Technology (FIT) as the coordinating provider.

Also, the third level sector in Ireland has also begun to offer a significant number of courses in cyber security, with at least 8 Masters level courses now on offer. Cyber security programmes are also being supported through the Springboard+ programme, which is increasingly facilitating those already in employment to reskill into alternative roles or occupations. This will be important with the rising demand for cyber security skillsets.

The Department of Business Enterprise and Innovation with the Department of the Taoiseach launched Future Jobs Ireland in March 2019, a new multi-annual framework to ensure our enterprises and workers are resilient and prepared for future challenges and opportunities. Future Jobs Ireland will also ensure our enterprises and workers are well positioned to adapt to the technological and other transformational changes our economy and society will face in the years ahead. Although wide ranging in scope, one of the five Pillars within Future Jobs Ireland is “Embracing Innovation and Technological Change”. The framework recognises the need for new and diverse skillsets to meet our changing economy and “exploit cutting edge technological areas such as Artificial Intelligence, Data Analytics, the Internet of Things and Blockchain to facilitate and help companies co-innovate and develop solutions”.

A series of ambitions and deliverables have been identified to achieve these aims including increasing the capacity of SMEs to engage in research & development, providing high quality education and training, encouraging lifelong learning, and enhancing participation in apprenticeship programmes. A number of initiatives have already commenced under the medium-term ambitions outlined in Future Jobs Ireland 2019. Each year Future Jobs Ireland will set out new steps to deliver on these ambitions.

Key Developments

1. Technology Skills 2022 has been published and implemented.
2. Skillnet Ireland launched their Cyber Security Skills Initiative to deliver a broad programme of initiatives in the field.
3. Fastrack to Information Technology have launched a Cyber Security Programme for apprentices.

4. Government has launched Future Jobs Ireland, a multiannual framework for skills and enterprise development, including the technology sector.

8.2 Objectives

To invest in educational initiatives to prepare the workforce for advanced IT and cybersecurity careers.

8.3 Measures

Through the implementation of Technology Skills 2022, Future Jobs Ireland, and this Strategy Government aims to ensure that the employment market has sufficient skilled and trained staff to meet demands from employers.

12. **Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.**

    Government will continue to support the work of Skillnets Ireland in developing and delivering training to private industry aimed to promote cyber workforce participation, upskilling and general career development. The NCSC will provide assistance in developing initiatives which encourage women into the cyber security field and encourage participants from other disciplines to cross train.

13. **Science Foundation Ireland (SFI) will promote cyber security as a career option in schools and colleges by means of their Smart Futures Programme.**

    Smart Futures is a collaborative education programme run by Science Foundation Ireland that provides second-level students in Ireland with information about careers in Science, Technology, Engineering and Maths (STEM). SFI will develop a Cyber Security component, using input from industry professionals, for inclusion in Smart Futures so students remain aware of the wide range of career opportunities available in the field.

14. **Science Foundation Ireland along with DBEI and DCCAE, will explore the feasibility through the SFI Research Programme, the Research Centre Spoke**

programme or other enterprise partnership programmes to fund a significant initiative in Cyber Security Research.

This research centre would link scientists and engineers in partnership across academia and industry to address crucial research questions.

Measure 12: Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Provide support to initiatives under Technology Skills 2022 including development of Skillnets and ICT apprenticeship initiatives	Ongoing	DCCAE	Skillnets, SOLAS, DES
2	Add education and upskilling as a standing item on the agenda of the Gov IT Security Forum	Q2 2020	NCSC	Gov IT Security Forum
3	Support the development of a Junior Cycle short course in cyber security, which will provide for the inclusion of cyber security education in second level	Q4 2020	NCSC	NCCA
4	Support initiatives which encourage women into the cyber security field	Ongoing	NCSC/DES	Industry

Measure 13: Science Foundation Ireland (SFI) will promote cyber security as a career option in schools and colleges by means of their Smart Futures Programme.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	NCSC to seek industry partners to participate in Smart Futures	Q1 2020	NCSC	SFI,Industry
2	NCSC will work with Smart Futures to support initiatives which encourage	Q1-Q4	NCSC	SFI

	female students into the cyber security field			

Measure 14: Science Foundation Ireland along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes to fund a significant initiative in Cyber Security Research.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Issue calls to which cyber security community can respond	Q4 2020	SFI	NCSC,DBEI, SFI
2	Assess proposals based on independent international peer review.	Q1 2021	SFI	NCSC,DBEI, SFI

9 Enterprise Development

9.1 State of Play

IDA Ireland has supported the establishment of the 'Cyber Ireland' Programme by Cork Institute of Technology (CIT), to establish and grow an Irish Cyber Security Cluster in Ireland. Cyber Ireland was officially launched on 20th May 2019 and is hosted by Cork Institute of Technology (CIT). This national cluster aims to represent the needs of the sector in Ireland and includes stakeholders from industry, academia and government. It will 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 facilitate the establishment of developing the cluster and has drafted a 7 phase structured programme to achieve this aim. The development of Cyber Ireland is included in Future Jobs Ireland 2019 underscoring the Government's commitment to developing the sector.

Key Developments

1. The Cyber Ireland Initiative has been launched, funded by the IDA, to assist in the development of the sector in Ireland.

9.2 Objectives

To raise awareness of the responsibilities of businesses around securing their networks, devices and information and to drive research and development in cyber security in Ireland, including by facilitating investment in new technology.

9.3 Measures

15. Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/ Government cyber security collaboration.

The NCSC, along with the IDA and Enterprise Ireland, will participate as active inaugural board members of Cyber Ireland supporting their initiative of bringing together industry, academia and government to enhance the cyber security environment in Ireland. Cyber

Ireland are actively involved in promoting education and skills, forums for communications, attracting foreign direct investment and research and development.

16. Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community that lead to the practical application of research in business.

Consistent with Enterprise Ireland's mission, Enterprise Ireland will leverage its sectoral knowledge and experience of industrial-academic collaborative initiatives and engage with the NCSC to explore opportunities to support economically beneficial cyber security collaborative links between enterprise and the research community.

Measure 15: Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/Government cyber security collaboration.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Support given to Cyber Ireland in developing a Cyber Security Cluster of Industry, Academia and Government	Ongoing	IDA	Cyber Ireland, EI, NCSC, DBEI

Measure 16: Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community that lead to the practical application of research in business.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish a National Cyber Security Competence Centre	Q1 2021	NCSC	NCSC, EI, DBEI.

10 Engagement

10.1 State of Play

Cyber security is inherently an international field, and has multiple implications for many aspects of the State's international engagement. We recognise the importance of cyber security as a priority for foreign policy. Developments in this field have been an integral part of foreign policy making in Ireland for some time already but there is a clear need to evolve and develop that engagement, both in general and specifically across the European Union.

At a global level the last 10 years have been marked by a number of increasingly high profile attacks and incidents, including attacks on electricity infrastructure in Ukraine in 2015 and the 'Wannacry2' and 'NotPetya' incidents in 2017. These have brought with them a reinvigorated debate about the role of States and the international community in moderating State behaviour online, and as to the appropriate set of measures for countries to use within their own territory to ensure the integrity and resilience of key systems.

A number of international organisations have brought forward initiatives to try and frame these issues within existing international relations frameworks. The most notable of these has been the UN Group of General Government Experts (or GGE). This was established in 2004 on the basis of discussions that had been underway since 1998, on the basis of Resolution 53/70. In the period since 2004, there have been five separate iterations of the GGE, with three agreeing on substantive reports, and two, including the most recent one in 2017 failing to reach agreement.

In late 2018, the UN adopted two new resolutions on cyber security matters. The first established an open-ended working group, which convened initially in June 2019 and will focus on raising awareness, building common understanding and advancing implementation of previously agreed norms and principles of responsible State behaviour. The second underlined the three successful GGE reports and called for the establishment of another GGE, with a focus on the application of international law to cyberspace and advancing the consensus on responsible State behaviour in cyberspace.

At a regional level, both the Organisation for Security and Cooperation in Europe (OSCE) and the European Union has also played an increasingly progressive role in the area of Cybersecurity. The OSCE has produced two sets set of draft confidence-building measures (CBMs) in 2013 and 2016 to "enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs".

Key Developments

1. The UN adopted two new resolutions focusing on co-operation and building awareness of cyber security matters.
2. The OSCE produced two sets of confidence building measures enhancing co-operation and stability.

10.2 Objective

To continue to engage with international partners and international organisations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development.

10.3 Measures

17. We will reinforce Ireland's diplomatic commitment to cyber security, including by stationing cyber attachés in key diplomatic missions and by engaging in sustainable capacity building in third countries.

Ireland will reinforce its diplomatic commitment to cyber security as part of the 'Global Ireland' initiative, by assigning designated Cyber Attachés to key diplomatic missions. Based on our support for an open, free, peaceful and secure cyberspace, we will advocate for preventative diplomacy in our international engagement. We will support international cooperation to combat cybercrime and promote formal and informal cooperation in cyberspace, including by engaging in sustainable capacity building in third countries. As part of our commitment to combatting cybercrime, we will ratify the Budapest convention as early as practicable. The applicability of international law, including international humanitarian law, and respect for human rights will guide our international commitment to cybersecurity. We will provide sustainable capacity-building support to developing countries and civil society actors and ensure we are fully aware of potential human rights abuses, targeting of human rights defenders, and monitoring/controlling ethnic minorities through technology.

18. We will create an interdepartmental group (IDG) on internet governance and international cyber policy to coordinate national positions across Departments.

We will create an Interdepartmental Group (IDG) on international cyber policy matters to coordinate engagement on issues with a geopolitical dimension and to develop a coordinated position on internet governance and cyber security matters.

19. We will deepen our existing engagement in international organisations, including by joining the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia.

We will deepen our engagement in International Organisations in dealing with the full range of issues arising under this Strategy. As such, Ireland will join and play a full part in the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia. This will include the secondment, initially, of a member of the Defence Forces[2] to the Centre in due course. We will also fully support the UN processes in seeking to develop and implement a framework for stability in cyberspace.

Measure 17: We will reinforce Ireland's diplomatic commitment to cyber security, including by stationing cyber attachés in key diplomatic missions and by engaging in sustainable capacity building in third countries.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Appoint Cyber Attachés to key Diplomatic Missions.	Q3 2020	DFAT	NCSC
2	Ratify the Budapest Convention	Q2 2021	D/Justice	NCSC, D/Taoiseach
3	Develop a sustainable capacity building programme for developing countries	Q2 2021	DFAT, NCSC	NCSC

Measure 18: We will create an interdepartmental group (IDG) on internet governance and international cyber policy to coordinate national positions across Departments.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish a IDG to coordinate on cyber policy matters	Q2 2020	DFAT	NCSC, All Govt

[2] While the initial deployment to the CCD-COE will be from the Defence Forces, the persons deployed thereafter may be either civilian or military in accordance with the Government approval.

				Departments

Measure 19: We will deepen our existing engagement in international organisations, including by joining the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Secondment of a member of DF to CCD-COE	Q4 2020	NCSC	DF, D/Defence, DFAT

11 Citizens

11.1 State of Play

In terms of cyber security awareness, there have been a number of important national initiatives over the last number of years, particularly in the educational system. To begin with, Webwise, an internet safety initiative co-funded by the Department of Education and Skills and operated by the Professional Development Service for Teachers (PDST) Technology in Education, promotes the autonomous, effective, and safer use of the internet by young people through a sustained information and awareness strategy targeting parents, teachers, and children themselves with consistent and relevant messages including guidance on acceptable usage in schools.

A range of resources have been developed including “UP2US”, “My Selfie and the wider world” and “Lockers”; the online Parenting Hub: Webwise Parents; and ‘Be in Ctrl’, which supports teachers to address the topic of online sexual coercion and extortion with their students. In mid 2019, the ‘HTML Heroes’ resource was launched, which aims to assist and support educators when teaching children aged 7–10 years about the safe and responsible use of the Internet, including social media.

Smart Futures is coordinated by Science Foundation Ireland in partnership with organisations and academia. The programme provides second-level school students in Ireland with information about careers in science, technology, engineering and maths (STEM). Smart Futures engages with guidance counsellors, teachers and industry to develop resources and activities to stimulate interest in students. The Smart Futures website provides information on the wide range of opportunities available such as courses, apprenticeships, festival and events. In February 2019, Smart Futures launched a new national campaign titled “I get paid to do this” in partnership with the Department of Education and Skills. The campaign centres around an online resource of profiles on professionals working in STEM related industries to give students insight into what they can expect from a career in STEM and the diverse opportunities open to them.

The programme is currently being implemented by a Sponsors Group under the Chair of the Department of Education & Skills. Enactment of the Online Safety Act which will set out how we can ensure the further safety of children online has been brought forward. This will involve, for the first time, setting a clear expectation for service providers to take reasonable steps to ensure the safety of the users of their service.

Key Developments

1. Through a sustained information and awareness programme Webwise has provided parents, teachers, and children with guidance on the safe use of the internet.
2. Smart Futures has been launched to provide second-level students with information about careers in science, technology, engineering and maths related disciplines.

11.2 Objective

To increase the general level of skills and awareness among private individuals around basic cyber hygiene practices and to support them by means of information and training.

11.3 Measures

By developing good cyber hygiene practices in the wider population we can create a more secure society. Awareness of cyber risks is of particular importance in vulnerable parts of the population.

20. Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision.

A National Cyber awareness campaign will be developed and delivered to the public. This programme will harness the experience of the NCSC and the Garda National Cyber Crime Bureau, and will be developed as a collaborative effort between multiple partners, to include PDST and the Online Safety Commissioner. The aim of this campaign will be to improve societal awareness around common cyber risks such as basic cyber hygiene and social engineering. It will also facilitate more targeted awareness campaigns aimed at vulnerable groups such as children and the elderly, including by the provision of information to Webwise.

Measure 20: Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Support the continued inclusion of cyber security elements in Webwise programmes	Q4 2020	DCCAE	AGS, DES
2	Develop a public awareness campaign to include information on cyber security and cyber crime prevention.	Q1 2021	NCSC, Online Safety Commissioner	DCCAE, AGS, DJE, DES

12 Governance Framework and Responsibilities

12.1 Governance Structure

Delivering the National Cyber Security Strategy will require a governance framework and structure, both in terms of operational response and the overarching components of the Strategy itself.

12.2 Delivery of the National Cyber Security Strategy

The Cabinet Committee on Security will be the primary means of coordinating responses to national security matters. However, a High Level Interdepartmental Committee will be created, meeting twice a year, tasked with assessing and reporting on progress towards meeting the Measures under this Strategy, and with agreeing any amendments to the actions to be taken to meet these.

Appendix 1 List of Actions

National Capacity Development

Measure 1: The National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents and developing threats in the State.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Develop detailed technical and organisational plan for the JSOC.	Q4 2020	NCSC	DCCAE
2	Receive sanction for resourcing and staffing for NCSC expansion	Q2 2021	NCSC	DCCAE, D/PER
3	Build prototype JSOC in interim facility	Q4 2021	NCSC	OPW, DCCAE
4	Commission Final JSOC Facility in NCSC HQ	Q2 2023	NCSC	OPW, DCCAE

Measure 2: Threat intelligence and analysis prepared by the National Cyber Security Centre will be integrated into the work of the National Security Analysis Centre.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish Formal Reporting and Information Sharing arrangements with NSAC	Q1 2020	NCSC	NSAC

Critical National Infrastructure Protection

Measure 3: The existing Critical Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programmes to mitigate risks to key services.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Complete first phase of Operators of Essential Services (OES) Self-Assessment against Security Control Framework	Q1 2020	NCSC	Designated OES
2	Commence Security Control Testing of Operators of Essential Services (OES)	Q3 2020	NCSC	Designated OES
3	Reassess Register of Designated OES and Security Guidelines	Q3 2020	NCSC	
4	Security Control testing post incidents, and ongoing audits of OES compliance	Ongoing	NCSC	Designated OES

Measure 4: The NCSC, with the assistance of the Defence Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber attack.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Steering Group formed and terms of reference for the review agreed	Q1 2020	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA
2	Information gathering phase complete, and methodology agreed	Q3 2020	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA
3	Complete Assessment Process, including international consultation and detailed	Q2 2021	NCSC	AGS, DF, NSAC, CBI,

	assessment of cross sectoral interdependencies.			COMREG, CRU, IAA
4	Final Report and Recommendations Complete	Q4 2021	NCSC	AGS, DF, NSAC, CBI, COMREG, CRU, IAA

Measure 5: The existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Draft Heads of Bill for Agreement by Government	Q4 2021	DCCAE	AGO
2	Drafting Process with AGO	Q1 2022	DCCAE	AGO
3	Oireachtas Process	Q2 2022	DCCAE	AGO, Oireachtas

Measure 6: The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of critical national infrastructure.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Expand the current Threat Sharing Group (TSG) representatives to include CNI, with new Terms of Reference.	Q2 2020	NCSC	AGS, DF, CNI
2	Refine existing arrangements with the UK on information sharing and incident response, with particular reference to North-South critical infrastructure protection	Q4 2020	NCSC	OEP, CPNI UK

Measure 7: Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Transposition of Directive 2018/1972	Q4 2020	DCCAE	NCSC, Comreg
2	Provision of Technical Support to Comreg	Q4 2020	NCSC	Comreg
3	Application of revised security measures	Q1 2021	Comreg	DCCAE, NCSC, Telecoms Operators

Public Sector Data and Networks

Measure 8: The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Design suitable minimum standard for Government IT, in conjunction with Government IT Security Forum.	Q4 2021	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
2	Develop detailed measures, controls and implementation procedures.	Q1 2022	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
3	Draft guidance and support materials for IT teams and Internal Audit Units on compliance assessment.	Q2 2022	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies
4	Support Government Departments and Key Agencies in implementation of the baseline standard.	Ongoing	NCSC/OGCIO/Govt IT Forum	Government Departments and key

				agencies
5	Conduct assessment of the implementation of the baseline standard	Q4 2023	NCSC/OGCIO/Govt IT Forum	Government Departments and key agencies

Measure 9: The existing 'Sensor' Programme will be expanded to all Government Departments, and an assessment will be conducted by the same date as to the feasibility of expanding Sensor to cover all of Government networks.

Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Deploy Sensor on the IT infrastructure of all 15 Government Departments.	Q4 2020	NCSC	All Government Departments, Gov IT Security Forum
2	Review costs and legal issues associated with the application of Sensor on Government Networks, covering all of public sector ICT, and bring outcome to Government for decision.	Q4 2021	NCSC	OGCIO, AGO, D/PER

Measure 10: A Government IT Security forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.

Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Resource the creation of Public Sector IT Team in the NCSC, and establish Terms of Reference for the Forum	Q1 2020	NCSC	OGCIO, All Government Departments
2	Plan a briefing session for all Heads of IT	Q1 2020	NCSC	OGCIO, All

	Security to outline the purpose of the Security Forum			Government Departments
3	Establish quarterly meetings of the Forum and appoint a Chairperson and Secretary	Q4 2020	NCSC	OGCIO, All Government Departments

Measure 11: The NCSC will be tasked by Government to issue Recommendations with regard to the use of specific software and hardware on Government IT and telecommunications infrastructure.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Rationale and Terms of Reference Prepared and brought to Government for Agreement	Q3 2020	NCSC	OGCIO, AGS, DF, NSAC
2	Entry into effect of NCSC Recommendation Process	Q4 2020	NCSC	OGCIO, AGS, DF, NSAC

Skills

Measure 12: Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Provide support to initiatives under Technology Skills 2022 including development of Skillnets and ICT apprenticeship initiatives	Ongoing	DCCAE	Skillnets, SOLAS, DES
2	Add education and upskilling as a standing item on the agenda of the Gov IT Security Forum	Q2 2020	NCSC	Gov IT Security Forum

3	Support the development of a Junior Cycle short course in cyber security, which will provide for the inclusion of cyber security education in second level	Q4 2020	NCSC	NCCA
4	Support initiatives which encourage women into the cyber security field	Ongoing	NCSC/DES/	Industry

Measure 13: Science Foundation Ireland (SFI) will promote cyber security as a career option in schools and colleges by means of their Smart Futures Programme.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	NCSC to seek industry partners to participate in Smart Futures	Q1 2020	NCSC	SFI, Industry
2	NCSC will work with Smart Futures to support initiative which encourage female students into the cyber security field	Q1- Q4	NCSC	SFI

Measure 14: Science Foundation Ireland along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes to fund a significant initiative in Cyber Security Research.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Issue calls to which cyber security community can respond	Q4 2020	SFI	NCSC,DBEI, SFI
2	Assess proposals based on independent international peer review.	Q1 2021	SFI	NCSC,DBEI,SFI

Enterprise Development

Measure 15: Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/Government cyber security collaboration.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Support given to Cyber Ireland in developing a Cyber Security Cluster of Industry, Academia and Government	Ongoing	IDA	Cyber Ireland, NCSC, EI, DBEI

Measure 16: Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community the leads to practical application of research in business.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish a National Cyber Security Competence Centre	Q1 2021	NCSC	NCSC, DBEI, EI

Engagement

Measure 17: We will reinforce Ireland's diplomatic commitment to cyber security, including by stationing cyber attachés in key diplomatic missions and by engaging in sustainable capacity building in third countries.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Appoint Cyber Attachés to Key Diplomatic Missions.	Q3 2020	DFAT	NCSC
2	Ratify the Budapest Convention	Q2 2021	D/Justice	NCSC, D/Taoiseach
3	Develop a sustainable capacity building programme for developing countries	Q2 2021	DFAT, NCSC	NCSC

Measure 18: We will create an interdepartmental group (IDG) on internet governance and international cyber policy to coordinate national positions across Departments.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Establish a IDG to coordinate on cyber policy matters.	Q2 2020	DFAT	NCSC,, All Gov Departments

Measure 19: We will deepen our existing engagement in international organisations, including by joining the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Secondment of a member of DF to CCD-COE	Q4 2020	NCSC	DF, D/Defence, DFAT

Citizens

Measure 20: Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision.				
Actions for Delivery		Timeline by Quarter	Lead	Key Stakeholders
1	Support the continued inclusion of cyber security elements in Webwise programmes	Q4 2020	DCCAE	AGS, DES
2	Develop a public awareness campaign to include information on cyber security and cyber crime prevention.	Q1 2021	NCSC, Online Safety Commissioner	DCCAE, AGS, DJE, DES