Rialtas na hÉireann
Government of Ireland

National Cyber Risk Assessment

TLP:CLEAR

2022

Prepared by the National Cyber Security Centre
gov.ie

Table of Contents

Table of Contents i
1 Introduction 3
2 Threat landscape overview 5
2.1 Nation State / State affiliated 5
2.1.1 Disruption and sabotage 6
2.1.2 Espionage 6
2.1.3 Financially motivated 7
2.1.4 Hybrid warfare 7
2.1.5 Foreign Information Manipulation and Interference (FIMI) 8
2.2 Criminals 9
2.3 Terrorists / Hacktivists /script kiddies 11
2.4 Unintentional acts 11
2.5 Threat landscape summary 13
3 Supply chain attacks on the rise 16
4 Understanding Systemic Cyber Risk 17
4.1 Sectoral overview of Systemic Cyber Risks 19
4.1.1 Financial Services sector 20
4.1.2 Transport Sector 20
4.1.3 Healthcare Sector 21
4.1.4 Energy Sector 22
5 Undersea fibre cables 24
6 National Cyber Risk Assessment methodology 26
7 Survey results 28
7.1 Electricity and Communications critical 29
7.2 More focus on supply chain security required 30
7.3 C-suite appreciation for cyber risks is high 30

7.4 High dependency on a small number of non-EU companies 31
7.5 Novel technologies on the rise 32
8 Recommendations 33
Appendix A – Survey Results 36
Appendix B – Online Survey 42

1 Introduction

The National Cyber Security Strategy 2019-2024 describes two fundamental challenges for Ireland in relation to cyber security. 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 Irish society has developed significantly in recent years; not only is the State now home to a large proportion of Europe's data and the European headquarters of a number of the worlds largest technology firms, but also the vast majority of the critical services in the State are wholly or partially dependent on technology, in both the information system and industrial control system realms.

An outage or incident affecting this critical technology could therefore have immediate disruptive effects on the critical services they underpin across the State, the EU or even globally. While entities which provide vital societal or economic functions in the State, often termed Critical National Infrastructure (CNI), are in the first instance responsible for identifying and managing the risks to their own organisation and services, the cross cutting and interconnected nature of technology-based services and dependency on global supply chains in which issues of technological sovereignty are increasingly pertinent, means that entities are also exposed to 'systemic' cyber risks outside of their direct control.

Systemic Cyber Risk (WEF Definition)

> Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security. Systemic cyber risks have the following characteristics:
>
> - Widespread consequences
> - Can affect entire systems, not just individual parts or components

- Dependencies and interdependencies result in cascading, often unexpected consequences
- Can build up over time, e.g., common threat vectors across enterprises and ecosystems can result in large aggregate effects

In order to address cyber security risks at State level, the second National Cyber Security Strategy, under the 'Critical National Infrastructure Protection' theme, requires a detailed Cyber Security focused Risk Assessment of all Critical National Infrastructure in the State to identify any pathways which could lead to systemic cyber risks and to recommend measures to address these.

The National Cyber Security Centre (NCSC) led this measure with the assistance of a Steering Group which consisted of specialist members and staff from An Garda Síochána, the Defence Forces, the National Security Analysis Centre in the Department of the Taoiseach, the Central Bank of Ireland, the Commission for Regulation of Utilities (CRU), and the Commission for Communications Regulation (Comreg).

2 Threat landscape overview

Digital threats are a permanent fixture in today's society. The threat posed by criminals, including ransomware operators as was seen in the 2021 ransomware attack against the HSE, has escalated in recent years and Nation-state actors continue to pose a threat to national security through their ability to conduct disruptive cyber-attacks and espionage operations. The threat from other actors such as hacktivists, terrorists, so called script kiddies and insiders has also remained virtually the same. Even unintentional acts such as mistakes, errors or environmental factors can cause significant disruption to the cyber realm and resulting in impacts to critical services.

While we have seen first-hand the harm that can be caused by high profile cybersecurity incidents, more often threats in the cyber realm are chronic and pernicious in nature and mostly never make the headlines, while always having the potential to disrupt businesses, public confidence and public services.

Finally, the threat that an actor poses to the security of (information) systems is determined by the combination of the degree of capability, intent, and activity. Capability comprises the necessary knowledge and access to resources that can facilitate a cyber-attack. Intent relates to whether the actor has a specific objective (e.g., geopolitical or financial) and is willing to impair the confidentiality, integrity and availability of a system. Activity relates to the level of evidence that a particular actor has been detected engaging in or has concrete opportunities to engage in malicious cyber activities which compromise the confidentiality, integrity or availability of information systems. It is possible for an actor to pose a threat if the actor has intent and capacity, even if little to no activity has been detected.

2.1 Nation State / State affiliated

Geopolitical tension between the major world powers is on the rise and this tension has manifested itself in increasingly malign assertiveness in the cyber realm. State actors are increasingly engaged in cyber espionage and disruptive action to achieve geopolitical objectives. Russia's illegal and unprovoked attack on Ukraine in particular has reshaped the threat landscape, and has seen the deployment of destructive cyber-attacks in concert with kinetic military action.

Major State-sponsored actor trends include increased exploitation of zero-day and other critical vulnerabilities; the growing interest of State actors in targeting critical infrastructure and operational technology; and increased focus on supply chain compromises. The EU Agency for Cybersecurity (ENISA) has warned of an increased interest of threat actor

groups, and predominantly those coming from Russia and China, and to a lesser extent North Korea, in supply chain attacks[1].

In response, the EU and its Members States have continued to publicly attribute[2], to denounce malicious State-sponsored cyber activities[3], to urge States to adhere to the norms of responsible state behaviour as endorsed by all UN member states, and to not allow their territory to be used for malicious cyber activities by non-state actors[4].

2.1.1 Disruption and sabotage

State-sponsored groups are increasingly testing and exhibiting their capabilities for disruptive operations. For example, in the lead up to Russia's attack on Ukraine in early 2022 threat actors deployed destructive malware such as WhisperGate and HermeticWiper against organisations in Ukraine to destroy computer systems and render them inoperable. Russia was also responsible for the attack on the Viasat[5] satellite network which caused indiscriminate communication outages and disruptions across several public authorities, businesses and users in Ukraine, as well as affecting several EU Member States. In July 2022, the Government of Albania was subject to malicious cyber-attacks that destroyed data and disrupted essential government services, including paying utilities, booking medical appointments and enrolling schoolchildren. The websites of the Albanian Parliament and the Prime Minister's office, as well as 'e-Albania', a portal that Albanians use to access a number of public services, were attacked and subject to a shut down. The attackers also leaked Albanian government data, including details of emails from the Prime Minister and Ministry of Foreign Affairs[6] [7].

Pro-Russian Hacktivist groups continue to claim to be threatening, preparing for, or participating in more sophisticated disruptive and destructive attacks. In addition to established groups such as KillNet and XakNet, other threat actors which claim to be enhancing their capabilities include Legion, Beregini, RaHDIt, Zarya, FRwL (From Russia with Love group) and Deadnet. Whilst the frequency of hacktivist attacks has increased markedly they have tended to be low-sophistication and low-impact attacks such as Distributed Denial of Service (DDoS) attacks and website defacements.

2.1.2 Espionage

In addition to the threat of digital disruption and sabotage, espionage by nation-state actors also constitutes a significant threat to Western economies. States conduct spying activities to gain information for the benefit of their geopolitical, military and economic interests.

In this context, in February 2023 ENISA and CERT-EU drew attention to the Advanced Persistent Threats (APTs) of threat actors APT27, APT30, APT31, Ke3chang, GALLIUM and Mustang Panda noting that these threat actors have recently conducted malicious cyber activities against business and governments in the European Union[8] [9]. On 19 July 2021, the European Union urged the Chinese authorities to take actions against malicious cyber activities undertaken from their territory, and linked to APT31. These malicious cyber activities, which had significant effects, targeted government institutions and political organisations in the European Union and Member States, as well as key European industries.

2.1.3 Financially motivated

Certain State-backed groups and their operators have been observed engaging in cybercrime as a revenue generation activity. In July 2020 the EU imposed sanctions against six individuals and three entities responsible for or involved in various cyber-attacks[10]. This included sanctions against Chosun Expo for providing support for and facilitating a series of cyber-attacks with a significant effect originating from outside the Union which included cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank[11]. Chosun Expo can be linked to APT38 / the Lazarus Group, which according to the Electronic Transaction Development Agency are believed to be run by the North Korean government, motivated primarily by financial gain as a method of circumventing long-standing sanctions against the regime[12].

2.1.4 Hybrid warfare

Cyber operations can also occur in tandem with kinetic actions on the ground during so called hybrid warfare, as was observed in February 2022 just an hour before Russia's attack on Ukraine, when cyberattacks on the VIASAT satellite infrastructure caused widespread disruption when they brought down communications networks used by Ukrainian public and private organisations. State-backed actors are expected to continue to pursue their strategic objectives via cyber operations for intelligence gathering for advantages in decision-making, stealing intellectual property, and pre-positioning of military and critical infrastructure (preparation of the operational environment) for future conflicts. During the last 5-10 years, adversaries have increasingly invested resources to target ICS (Industrial Control System) networks. The number of threat groups targeting ICS networks is growing at a rate three times faster than they are going dormant Historically, organisations have had less visibility in their ICS networks as compared to their IT networks. Moreover, digital transformation initiatives, the rise of Industrial IoT, the cloud connectivity of ICS devices, as well as the

remote access services for ICS networks provide opportunities for the threat actors to exploit.

2.1.5 Foreign Information Manipulation and Interference (FIMI)

Foreign Information Manipulation and Interference in the information domain (FIMI), including disinformation, describes a mostly non-illegal pattern of behaviour in the information domain that threatens or has the potential to negatively impact universal values and integrity of government procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, often in relation to other hybrid activities. Actors of such type can be state or non-state actors, including their proxies inside and outside of their own territory.

According to the joint analysis by ENISA (EU Agency for Cybersecurity and the EEAS (European External Action Service) one of the most important parameters in defining the manipulation of information is the notion of "intent" [13]:

- Misinformation is an unintentional attack, where sharing of information is done inadvertently. Inaccuracy carried by the information is unintentional and could happen for example when a journalist reports wrong information in good faith or reports information by mistake.
- Disinformation the intentional spread of false and/or misleading information for a specific purpose

Information operations dominated the news headlines during the 2016 US elections, and in 2021 the European Union issued a declaration condemning malicious cyber activities collectively designated as GhostWriter, which targeted numerous members of Parliaments, government officials, politicians and members of the press and civil society in the EU by stealing data in computer systems and personal accounts. Currently, several states are leveraging information operations as a tool for hybrid conflicts exploiting societal divisions, undermining trust, and polarising societies over issues that are sensitive and important in certain countries. Also, threat actors are conducting more targeted information operations as compared to the "noisy" ones in the past. Moreover, currently there are commercial actors that sell Information-Operations-as-a-Service, providing plausible deniability for their sponsors, and threat actors have also adapted their TTPs and exhibit better operational security as well as platform diversification to survive takedowns.

Hack-and-leak operations are now an established tactic. Hack-and-leak operations include activities where a threat actor has unlawfully accessed information via a cyberattack and

then leaks this information. This information is usually leaked in a specific context– sometimes the information is manipulated–and at a time that serves the threat actor's objectives to achieve the desired effect and influence public debate. Targets for these operations can be businesses, politicians, as well as governmental organisations, and they are information operations impacting the confidentiality and integrity of the information leaked.

2.2 Criminals

The threat from criminals has escalated in recent years, particularly with the rise in the level of organisation and sophistication of Ransomware groups, many of whom have focussed on so-called 'Big Game Hunting'[14], consequently they can cause real damage to society particularly when they attack Operators of Essential Services. Cybercriminals are catching up to some nation-states' hacking capabilities and are making attribution more difficult[15]. Although the pernicious nature of cybercrime attacks can potentially erode trust in digital society in the long term, cybercrime attacks can also have societal and economic impacts which reach the level of national security incidents – in April 2022 the Costa Rican government declared a national emergency when 27 different government ministries were attacked by the Conti Ransomware group[16], in April 2021 President Joe Biden declared a state of emergency when Colonial Pipeline was the victim of a ransomware attack which resulted in the shutdown of a pipeline which moves oil from refineries to meet the demands of nearly half of the fuel requirements of customers along the eastern seaboard[17].

During the pandemic, organisations were forced to change their strategies and quickly adopt technologies that would support the new reality of remote working. This allowed cybercrime adversaries to take advantage of the rapid deployment of these teleworking technologies and exploit them for initial access. As organisations come to permanently rely on remote working services as they adapt to new hybrid working models, cybercriminals are expected to continue adopting their tactics, for example to gain unauthorised access by bypassing MFA (Multi Factor Authentication) through the use of SMS phishing campaigns to steal passwords and one time codes in real-time[18].

Social engineering also remains a prevalent attack technique[19]. During the pandemic, cybercriminals have been exploiting people's interest, concern, curiosity, and fear by using phishing lures related to current events such as COVID-19 and the Russian invasion of Ukraine for financial gain. Cybercriminals will also cynically exploit events to exert maximum pressure on victims, as was seen when cybercriminals leveraged COVID-19 to create

opportunities for targeted ransomware against organisations within the healthcare and public health sector.

The frequency and the complexity of ransomware is on an upward trajectory[20] and has become one of the greatest threats that organisations face today regardless of the sector to which they belong. Some commentators call this the golden era of ransomware, and it has become a national security priority[21] which may yet not have reached the peak of its impact. The successful business model of human-operated ransomware (aka Big Game Hunting) has been increasingly attracting cyber-criminal threat actors and it is also having an impact on their targeting, with cybercriminals performing active research and reconnaissance to carefully select their targets to maximise their successes[22]. Moreover, the Ransomware-as-a-Service (RaaS) business model is booming[23], two-thirds of ransomware campaigns were attributed to operators using RaaS during 2020. This trend sets a relatively low barrier for conducting this type of cybercrime and allows inexperienced cybercriminals to conduct ransomware attacks.

Threat actors are constantly evolving their techniques, and in fact the evolution of tactics and techniques by threat actors in pursuit of their objectives is what sets adversarial threats apart from other threats such as those resulting from errors, environmental factors or system failures, where such threats tend to be more static and better understood. For example, the effects of a storm are well documented and therefore the methods to defend against it are well understood, notwithstanding the unpredictability of its path or intensity on the ground. Likewise, system and component failures can be predicted with relative accuracy at various stages of a devices lifecycle. Adversarial threats however are not static, and defenders and attackers are in a constant 'arms race' to get the upper hand. In late 2019 ransomware groups further evolved their tactics by deploying so called 'multiple extortion techniques'[24] whereby they not only deny access to a victim's data by encryption, but also put additional pressure on victims by exfiltrating sensitive data and threatening to release it unless a ransom is paid.

Cybercriminals have also become more 'professional' with different cybercrime groups providing specialist services. This 'Cybercrime as a services' further lowers the barriers for threat actors to conduct cybercrime activities by building relationships and selecting services they require within the cybercrime ecosystem. For example, such services include phishing kits, credit/debit card testing services, 'bulletproof' hosting services, DDoS attack tools, distribution services for delivering malicious emails and monetisation services such as money mules, money laundering and wire fraud cryptocurrency services.

It is expected that cybercrime will continue to be a problem for years to come due to the widespread availability of sophisticated hacking tools and services and relatively low level of knowledge required to deploy and operate the tools.

2.3 Terrorists / Hacktivists /script kiddies

Following its peak during the period 2010-2015[25], the threat from this group of actors fell off in the following years when these actors were seen operating in small groups or as individuals, protesting against regional events and targeting specific organisations. Their capabilities and tactics in the main lacked sophistication and typically focused on DDoS attacks, defacements, releasing sensitive data and account takeovers. This fall off was likely due to the success of prosecutions which may have acted as a deterrent[26], in combination with their limited resources, with their real-world operations kept in in check by law enforcement agencies.

However, the last 2 years have witnessed a rise in hacktivism once more, with hacktivists seen targeting US institutions over the Supreme Court's revocation of the legal right to abortions, a hacking group called Predatory Sparrow claimed they were behind an attack against an Iranian steel factory which caused a serious fire in the production machinery in response to unspecified acts of aggression carried out by the Islamic Republic of Iran[27]. The Russian war against Ukraine has spawned several potent new hacktivist groups on both sides of the conflict, such as Killnet, Legion, DeaDNet which support the Russian cause, and supporting the Ukrainian cause are groups such as the IT Army of Ukraine, NB65 and Against-the-West. They now deploy the full spectrum of offensive cyber capabilities such as deploying large botnets in widespread DDoS attacks[28], ransomware attacks[29] and successful exploitation of zero-day vulnerabilities.

Apart from the obvious risks of hacktivist attacks spilling over and impacting non intended targets, this resurgences of hacktivism and cyber-activism in 2021/2022 may have other long-term consequences, in particular cyber-activism may be used as a pretext to lure individuals into potentially unlawful activities. Such a trajectory has been observed in the early 2010s, when sophisticated spinoffs and hacking groups broke away from the wider *Anonymous* brand umbrella.

2.4 Unintentional acts

Systems failures and breakdowns remain a significant threat, albeit a threat that does not involve any intent or malicious activity. Due to the interconnectedness of systems and the increasing degree of complexity, unintentional acts such as human errors, hardware and

software failures and natural hazards are the most frequent root causes for critical service outages, as illustrated in Fig 1 and Fig 2 below[30]. The failure of one individual system or network can cause breakdowns or failures in other areas. This is especially the case if basic cyber security 'availability' measures have not been sufficiently implemented and if no underlying systems are in place as a fallback option.

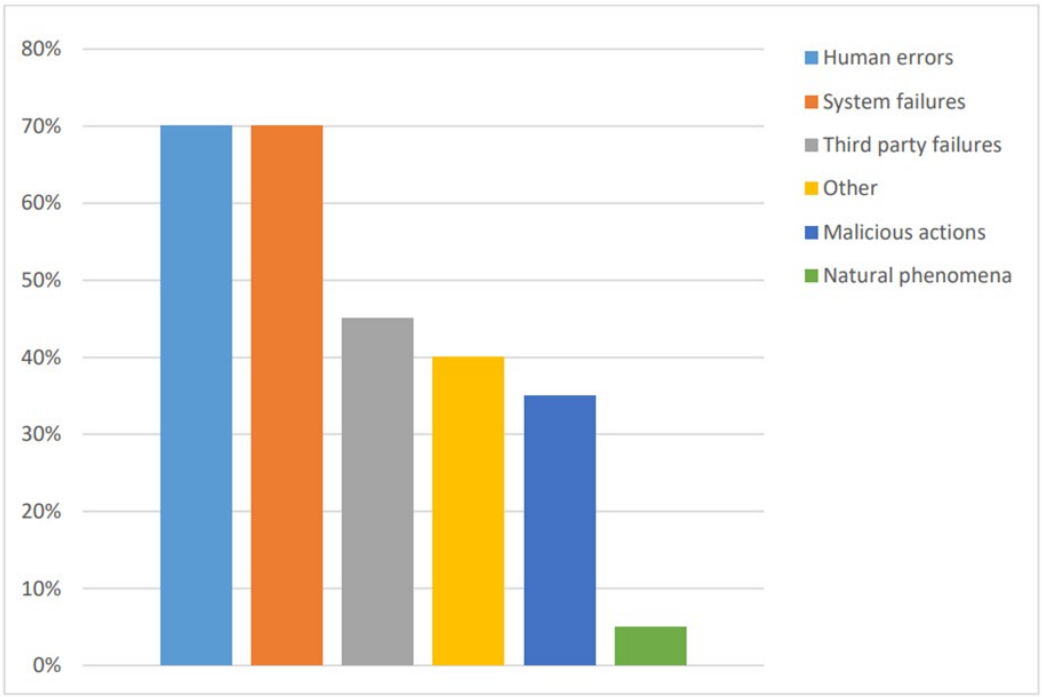


Fig 1 – Most common root causes for incidents as seen by DSPs

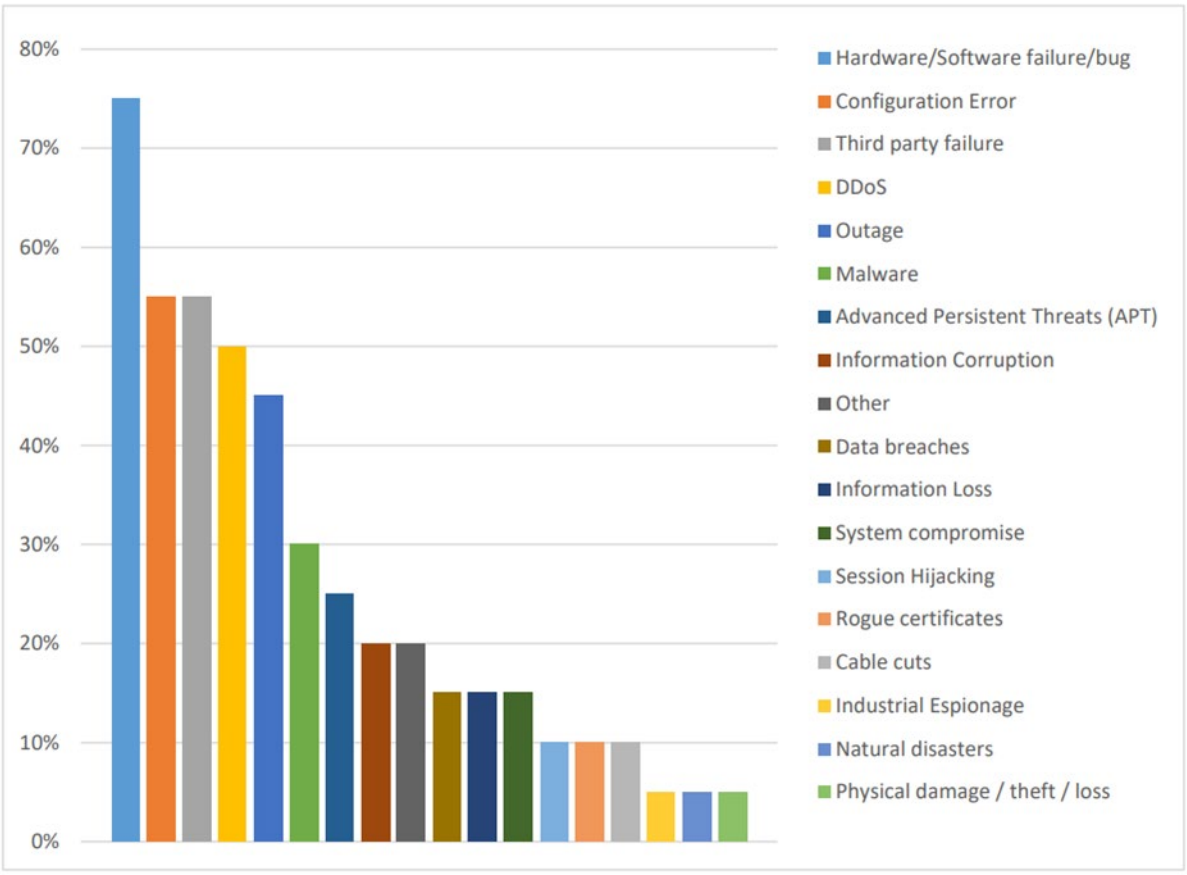


Fig 2 – Most common incident types as seen by DSPs

2.5 Threat landscape summary

The threat matrix below summarises the threats posed by threat actors against various targets. A key trend in recent years is the blurring of the lines between the 3 categories of threat actors, and the Russian war on Ukraine has accelerated this trend, where the co-opting of cybercrime groups with state sponsored actors features strongly, and hacktivist groups are increasingly active and are aligning themselves on both sides of the RU-UA conflict, and beyond[31]. The rise in the indiscriminate use of Ransomware in recent years by cyber criminals motivated by financial gain continues to leave a trail of destruction and devastation in its wake and has elevated the threat from this group to that of Nation State actors, across all target types, from operators of Critical National Infrastructure to large and small businesses, to individual citizens.

	Government/Public Sector	Critical Infrastructure	Enterprises	Citizen(s)
Nation State / State affiliated	Espionage	Disruption	Espionage	Espionage
	Data manipulation	Sabotage	System manipulation	
		Espionage		
Criminals	Disruption	Disruption	Disruption	Disruption
	System manipulation	System manipulation	Data manipulation	Data manipulation
	Data theft		Data theft	Data theft
			System manipulation	System manipulation
Terrorists / Hacktivists /script kiddies	Sabotage	Sabotage	Disruption	
	Disruption	Disruption	Data manipulation	
Unintentional acts	Breakdown/failure	Breakdown/failure	Breakdown/failure	Human error
	Data leak	Data leak	Data leak	

Fig 3 – Threat matrix[32] summarising the threats that various actors pose to various targets.

Caption:

Yellow: Actors have intent but lack the tools/knowledge (capacity)

OR activity has been detected but the actors possess limited tools/knowledge

OR activity has been detected but the actors only intend to attack specific targets

Orange: The actors possess tools/knowledge and substantial intent

OR the actors have substantial intent and activities have been detected.

Red: The actors have substantial tools/knowledge and very substantial intent

OR the actors have very substantial intent, possess substantial tools/knowledge and a great deal of activity has been detected.

The following threats are defined:

- Disruption: intentional temporary impairment of the accessibility of data, information systems or information services.
- Sabotage: intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction.
- Data manipulation: impairment of the integrity of information by means of the intentional editing of data.
- Data theft: impairment of the confidentiality of information by means of the copying or removal of data.
- Espionage: impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors.

- System manipulation: impairment of information systems or information services targeting the confidentiality or integrity of these systems/services. These systems or services are subsequently used to carry out other attacks.
- Breakdown/failure: impairment of integrity or availability due to natural causes, technical difficulties, or human error.
- Data leak: loss of confidentiality due to natural causes, technical difficulties, or human error.

3 Supply chain attacks on the rise

Supply chains increase vulnerability levels, particularly where third party software or managed services suppliers have privileged and wide-ranging access to an organisation's operations, which is frequently the case. Supply chain attacks are becoming increasingly attractive to threat actors and analysis by ENISA[33] showed that on at least 17 occasions between 2020 and 2021, investigations confirm that supply chain attacks were conducted by Advanced Persistent Threat (APT) groups, often state-sponsored, which makes up more than 50% of the attributed supply chain attacks during this period. While supply chain compromises by state-backed threat actors are not new, this type of attack has reached new levels of sophistication and impact. An example of a recent significant campaign that took place is the SolarWinds supply chain compromise. The SolarWinds supply chain compromise is a prominent example of how great an impact a supply chain attack can have, in which the attackers compromised widely used software at its source, which in turn gave them an entry point to anyone who used it, in this case the threat actors had potential access to 18,000 SolarWinds customers, including government information systems, critical infrastructure operators and other highly sensitive networks.

4 Understanding Systemic Cyber Risk

For over a decade, several risk reports from the WEF[34] have shed light on the increasing interconnectedness of our societies and the resulting evolution of the risks humans face. These reports recognise that these risks are becoming increasingly tangible and identifies the “resilience imperative” – an urgent need to find new avenues to withstand and mitigate a constantly evolving threat landscape.

The evolving nature of cyber risk – from seemingly isolated attacks against specific companies (e.g. data breaches) to system-wide attacks with the potential for massive cascading effects (e.g. as occurred in the Ukraine energy sector) – requires a robust and structured approach to identifying and predicting risks, which may not be obvious due to the complexity of interdependencies in the cyber realm. Organisations which have a good understanding of their technology and the complex underlying connections and dependencies within and between the systems which underpin their operations are best placed to identify and manage the risks within their digitalised operations.

This National Cyber Risk Assessment uses the World Economic Forum (WEF) definition for ‘Systemic Cyber Risk’ described below to examine the systemic risks with the potential for cascading consequences within and between the States Critical National Infrastructure (CNI) sectors and makes recommendations for measures to help manage these risks.

Systemic Cyber Risk (WEF Definition[35])

Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security.

Systemic cyber risks have the following characteristics:

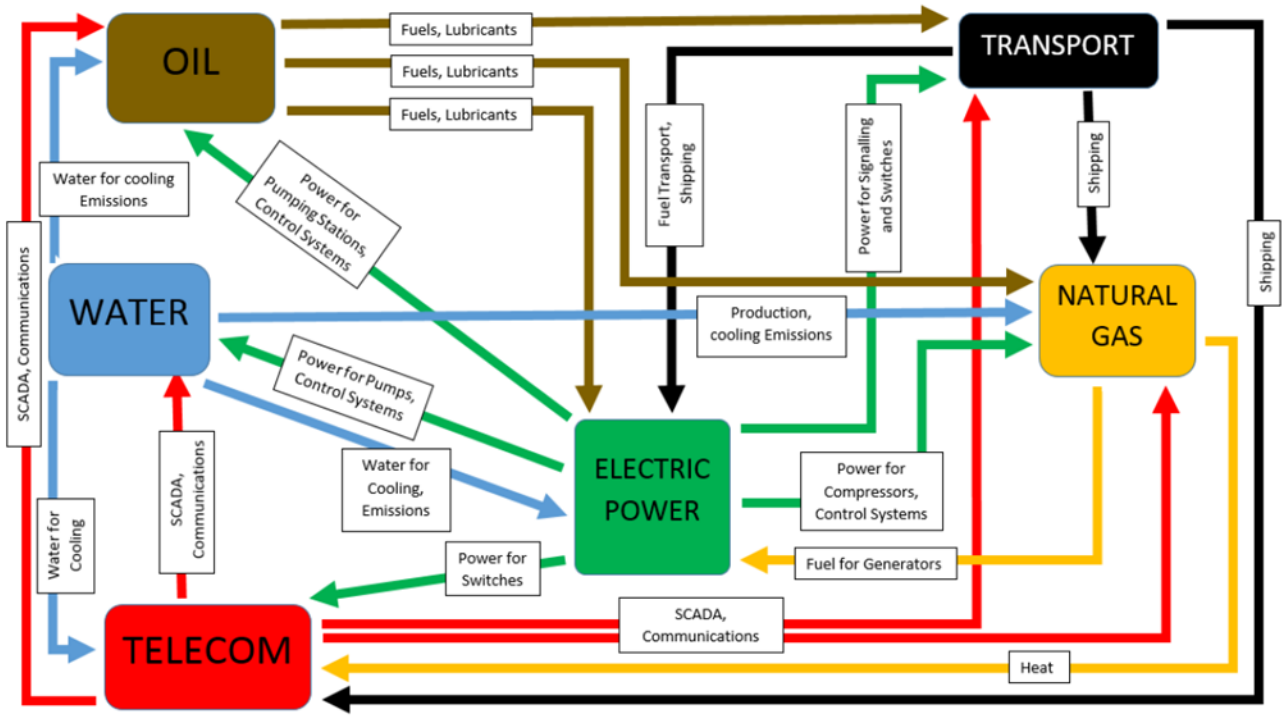
- Widespread consequences
- Can affect entire systems, not just individual parts or components
- Dependencies and interdependencies result in cascading, often unexpected consequences
- Can build up over time, e.g., common threat vectors across enterprises and ecosystems can result in large aggregate effects

Reliance on highly connected and interconnected technology gives rise to:

- The creation of single points of failure
- Sets of concentrated dependencies (e.g., as many businesses have grown dependent on technology and services provided by vendors which dominate their sector, should there be any compromise in the confidentiality, integrity or availability of the data stored by those vendors, ramifications would not only be felt by the customers of those vendors, but also the end users of every business affected)
- Complex dependencies and interdependencies between infrastructures.

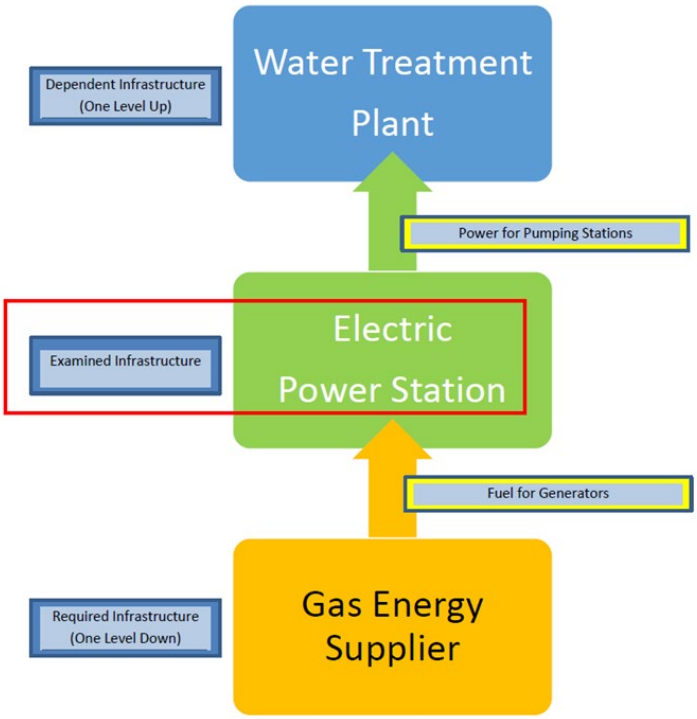
An approach to risk management which takes a structured approach to mapping and prioritising dependencies and interdependencies in the operational environment is the best approach to overcome the inherent 'dependency' complexity and allow an organisation to focus their resources to effectively mitigate and manage their operational risks –

move from this[36]:



This figure shows interdependencies in an industrial system. Such a system would also have dependencies on the financial sector for payments, and Telecoms for connectivity, among others.

and focus on this:



4.1 Sectoral overview of Systemic Cyber Risks

Systemic risks in the various CNI sectors are dynamic and constantly evolving in line with advances and changes in the technology landscape, the threat landscape and wider supply chain ecosystem. In order to stay current with the current risk environment, the NCSC has established close links with local, EU and international peer organisations, sectoral regulators, CNI operators and Lead Government Departments. The NCSC tested the National Cyber Emergency Plan (NCEP), in November 2022, and will continue to engage in periodic scenario planning exercises in collaboration with the wider stakeholder community to simulate cyber incidents with severe National level impacts. The output from such exercises will be used to continually refine and improve the NCEP and the NCSC's response capability and will help to better inform the wider stakeholder community on the systemic cyber risks which have the potential to trigger adverse national impacts and measures that are required to mitigate and manage these risks. The following sections give an overview of systemic risks in the Transport, Financial and Healthcare and Energy sectors. As stated above, such risks are dynamic in nature, and the NCSC and wider stakeholders will need to ensure that their risk management capabilities keep pace with the evolving threat landscape.

4.1.1 Financial Services sector

While all financial transactions are exposed to a level and variety of risks, payment, clearing and settlement arrangements are of fundamental importance for the functioning of the financial system and the conduct of transactions between economic agents in the wider economy. Disruption to these transactions have knock on effects that can impact all sections of the economy such as impairing the ability of government and private organisations to process payrolls, negative impacts on trade, impacts on the importation of essential commodities such as fuel for energy and transport etc, which in turn can lead to social unrest.

Any significant or prolonged disruption impacting payment, clearing and settlement arrangements could touch all major aspects of financial risk, such as:

- Credit risk – defaults on obligations within the payment system, imposing direct unexpected loss on other participants
- Liquidity risk – insufficient liquidity to fulfil settlement obligations
- Market risk and business risk – other transactional risks, including loss of revenue arising from suspension of payment services due to disruption or insolvency

While the potential patterns of attack on the financial services sector can vary significantly, they could include, but are not limited to:

- A number of simultaneous cyberattacks on systemically important institutions and critical/core financial infrastructures
- A coordinated, simultaneous cyberattack on the RTGS or SWIFT network, resulting in a widespread disruption that could create short-term catastrophic results in a global economy
- A cyberattack on automated trading systems that could take advantage of trading complexity and capacity, increasing the risk of disorderly markets – through the malfunction of algorithmic programmes – and the risk of market misconduct, such as unsolicited information leakage and possible market manipulation of “dark pools” (private exchanges for trading securities).

4.1.2 Transport Sector

The transportation sector includes the systems, networks, assets, people and vehicles of multiple transportation modes, including aviation, motorway and motor carrier, maritime,

mass transit and passenger rail, freight rail and shipping, and can also include pipeline systems.

Cyber threats to the Transport Sector are of concern because of the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation[37]. Potential risks include:

- Manipulation of data, or shutting down, of air traffic control systems, leading to immediate impact on the global travel industry
- Loss of trust in road transportation, following vehicular accidents resulting from hacks
- Tainted traffic control systems, resulting in accidents, injury and death
- Distorted status of freight movement in trucks, trains, ships and aircraft, damaging goods and creating general supply chain turmoil

Given the highly interdependent nature of the sector, the transportation sector would also be severely affected by systemic failures that might occur in logistics and financial payment systems, which are required to ensure transportation systems continue to operate. The globalised nature of trade and the trend in recent decades for industry in all sectors of the economy to outsource large parts of their manufacturing and operational requirements to geographically dispersed suppliers means that anything that impairs transport logistics can quickly cascade into the wider economy.

4.1.3 Healthcare Sector

Like the transport and financial sectors, the healthcare sector faces a range of risks stemming from its production of critical patient information and reliance on key clinical infrastructure. Cybercriminals can focus efforts not only on patients, but on healthcare providers, insurers, pharmaceutical manufacturers, and distributors as well. Cybercriminals can use multiple methods of entry, such as phishing, stealing laptops, capitalising off human error, social engineering and more.

The Ransomware attack on the HSE in 2021 has highlighted the interconnected nature of the healthcare ecosystem and its dependence on technology and exposed the significant gaps in cybersecurity resilience measures related to these critical healthcare systems which underpin the entire healthcare service. Impacts from the attacks meant that hospitals had to fall back on manual administration and clinical diagnostic procedures, which severely impacted the day to day operations during the early phases of the attack lifecycle. The long

term negative impacts on patient outcomes due to missed or delayed appointments etc may not be known for several years.

4.1.4 Energy Sector

A secure energy system is of critical importance to modern societies. Electricity derived from legacy fossil fuels such as gas and oil and increasingly renewable sources such as wind are not only needed for our day-to-day activities, but also underpins the operation of other critical infrastructure across all sectors of the economy. Failure of the electricity system can therefore have cascading effects with wide spread impacts. The EU has one of the most reliable electricity grids in the world, however, energy system vulnerabilities where they exist are open to exploitation, as has been observed in cyber-attacks on the Ukrainian electricity grid which have been attributed to Russian hackers[38].

Energy flows are increasingly remotely controlled and monitored by networked industrial control systems and the introduction of smart grids and smart meters is leading to the automation of more and more control functions. Industrial control systems are used in the operations of large parts of the electricity and gas grids to control electricity generation, storage and transmission as well as gas storage and pipeline transport. Malicious interference of industrial control systems can not only lead to disruption of energy supply, but also to physical damage of equipment and industrial accidents, including explosions and fires. The number of networked devices in the energy system is expected to grow with the spread of the 'industrial internet of things' enabled by the roll-out of 5G wireless communication networks, greatly increasing the “attack surface” and presenting more opportunities for cyber-attacks from all threat actors particularly cyber criminals and state sponsored threat actors.

Energy systems, in common with most systems which use “operational technology” (OT) have a number of particularities that necessitate a specialised approach to cybersecurity, above and beyond cybersecurity standards and measures applied to “information technology” (IT) systems:

- Real-time requirements: In an electricity grid, supply and demand must be balanced at any moment, meaning industrial control systems must react within fractions of a second.
- Mix of advanced and legacy technologies: Energy system components have a very long lifespan, of several decades. It is consequently very likely that the grid will be controlled by a mix of advanced technologies with cybersecurity certification, and older devices which need to be protected in other ways.

- Cascading effects of disruption: Due to the interconnected nature of an electricity system, a serious disruption in one part of the grid can also spread to other areas, potentially leading to a blackout over a wide area. This would also affect other critical services that depend on electricity such as healthcare, transport, telecommunications, water supply and finance.

5 Undersea fibre cables

Sometimes described as the “world’s information super-highways[39],” undersea cables carry over 95 percent of international data. In comparison with satellites, subsea cables provide high capacity, cost-effective, and reliable connections that are critical for our daily lives. There are approximately more than 400 active cables worldwide[40] covering 1.3 million kilometres. Given Ireland’s geographical position as the shortest point between Europe and North America, and the fact that Ireland is now Europe’s largest data hosting location with 25% of the European market[41], it is clear that the security of these undersea cables is of paramount importance to the Irish State.

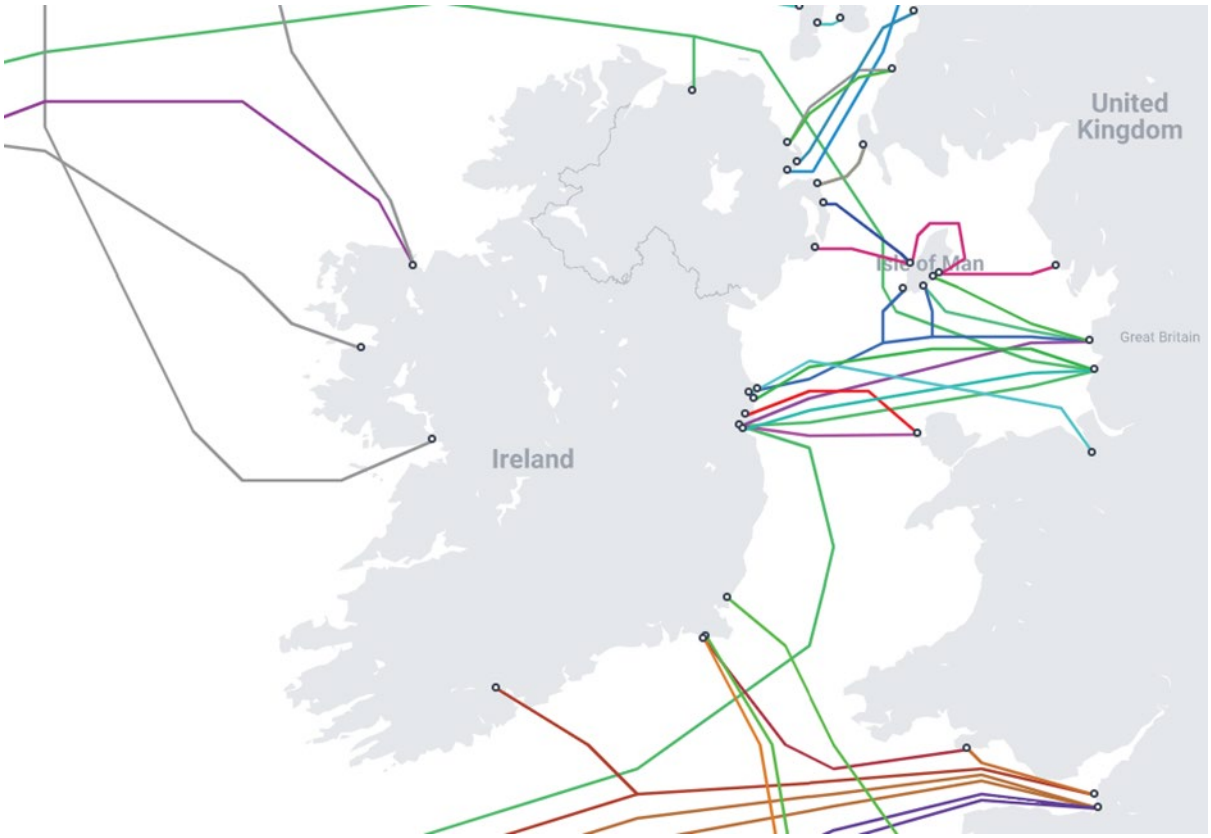


Fig 4 – Submarine cable map[42]

While there has been much media commentary in recent years about the threat posed to undersea fibre cables from Nation state actors [43] [44] [45], and while threats from Nation states should not be ignored, for example the sabotage of the underwater Nord Stream pipelines[46], the most immediate threat in fact comes from more mundane sources such as disruption of service due to natural events such as earthquakes, hurricanes and volcanoes [47] and accidental physical damage due to dredging, dumping, anchoring, commercial fishing.

Undersea fibre cables are not just vulnerable to undersea threats just described, but there are also vulnerabilities above sea which must be managed such as unmanned landing stations, concentrated landing zones and known cable paths. High capacity and multiple routes provide resilience in the event of failure, and where damage has occurred to cables in the past, the operators have shared a cable while repairs are made.

Across the EU, there is a recognition of the importance of submarine cables in providing the international connectivity which underpins international partnerships, trade and investment. This has prompted 25 EU countries, including Ireland, to sign a joint declaration[48] in March 2021 endorsing a plan to brand cables as critical infrastructure. The countries also pledged to map out how and where data flows in and out of Europe through submarine cables, identify systems that need replacement and come up with a plan to handle security risks.

6 National Cyber Risk Assessment methodology

The NCSC carried out the national cyber risk assessment using a 3 step approach:

1. Identify the National Critical Functions

   The starting point was to identify all of the National Critical Functions (NCFs) in the State which were underpinned by network and information systems (IT/OT). NCFs are the functions of government and the private sector so vital to the State that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

   The CISA National Critical Function set[49] and the and the proposed NIS2[50] directive, which expands the scope of the NIS Directive, were used as the basis for identifying the NCFs for the State.

2. Identify entities and assign criticality rating

   In collaboration with a nominated single point of contact (SPOC) in each of the Lead Government Departments and/or Sectoral Regulator, entities were identified and criticality ratings assigned, for the entities which are necessary for the operation/delivery of the National Critical Functions. The criticality ratings were assigned using the methodology described in the document 'Strategic Emergency Management Guideline 3 - Critical Infrastructure Resilience - Version 2'[51], published by the Office of Emergency Planning.

Level	Description	National Infrastructure Pyramid
5	This is infrastructure the loss of which would have a very high impact on the State. These assets will be of national importance whose loss would have significant national effects and may impact across a number of sectors. Relatively few are expected to meet the Level 5 criteria known as CNI. (>80 Criticality Score)	CNI
4	Infrastructure of high importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be high and may impact provision of essential services across Ireland. (>50 Criticality Score)	
3	Infrastructure of importance to the sectors, and the delivery of essential services, the loss of which would have a moderate impact. (>36 Criticality Score)	CI
2	Infrastructure whose loss would have a low impact on the delivery of essential services. (>27 Criticality Score)	
1	Infrastructure whose loss would cause very low disruption to service delivery, most likely on a localised basis. (<27 Criticality Score)	

Entities which score **3 or above** on the criticality scale are considered 'Critical Infrastructure' and are in scope for the cyber

Fig 5 – Criticality Scale

3. Identify systemic national infrastructure cyber risks

Each entity above the criticality threshold was invited to compete a voluntary online survey (Appendix B) to identify national infrastructure cyber risks at the sectoral level. This was an anonymous survey which did not seek to identify individual entities, only the sectors to which the entities belonged. The information gathered in this survey will form the basis for the creation of a National Registry which contains a list of essential and important entities containing at least the entities name, address, up to date contact details including email addresses, IP ranges and telephone numbers.

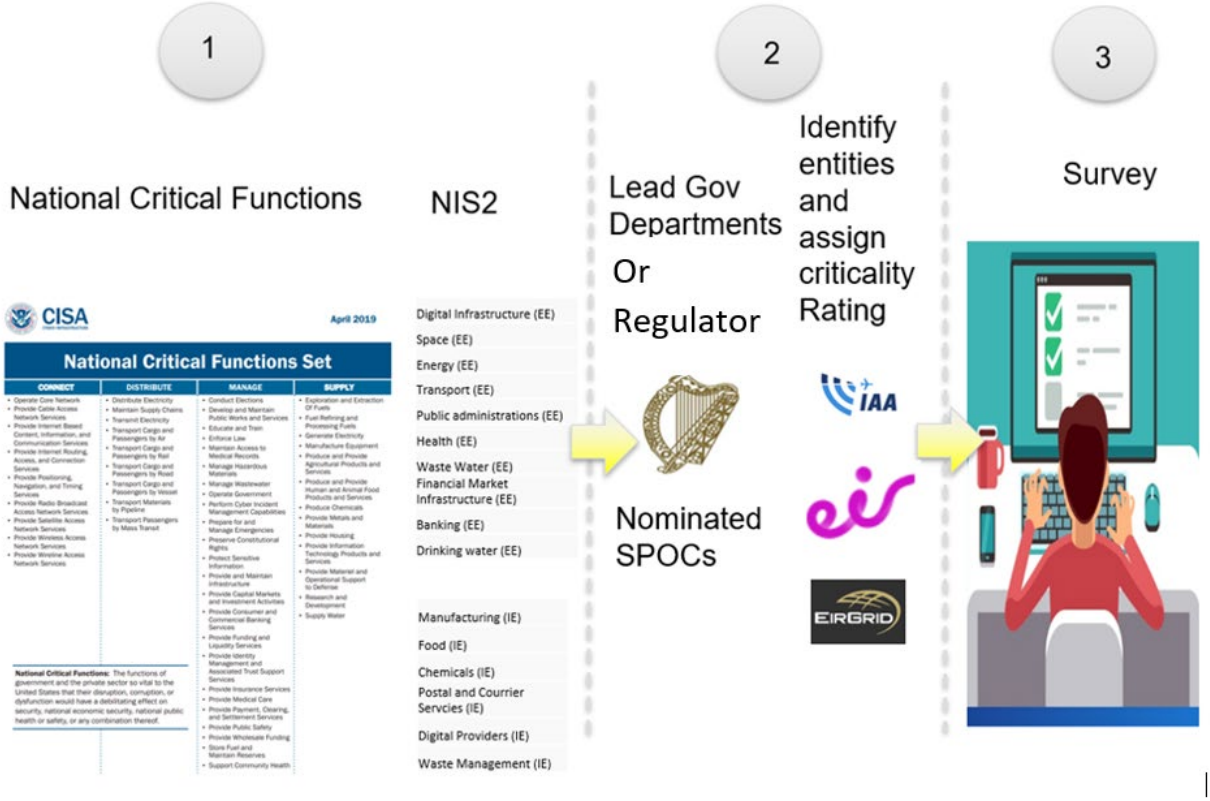


Fig 6 – 3 step process

7 Survey results

The cyber risks facing a country, economic sector or individual party are intertwined with each other and with other types of risks. Digital services, processes and systems are part of a larger whole; the global digital domain. The 2008 financial crisis and the 2020 COVID-19 pandemic show that certain events can rapidly have a global impact on other domains and strike at the heart of society and the economy. This is also true for cyber incidents and especially so when incidents occur on a large scale and in conjunction with other incidents. For example, the combination of the large-scale cyber attack against the HSE and the COVID-19 pandemic had major consequences. As a response to the pandemic there was a rapid acceleration in the digitalisation of commercial, educational and social activities, which allowed these activities to continue. The flip side of this is the unprecedented and rapid change across society which has ushered in new ways of working, social, educational and commercial interactions that are underpinned to a large extent by the digital domain. A large-scale digital breakdown post pandemic could cause more societal harm than it otherwise might pre pandemic, further underscoring the importance of **robust cyber resilience** across all sectors.

Practically all critical processes and services are entirely dependent on ICT. Due to a significant reduction in analogue or manual alternatives and the absence of fallback options, dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage.

Geopolitical developments can also affect cyber risks due to the concentration of companies producing key technologies such as 5G communications systems, Cloud Computing, Artificial Intelligence and Semiconductor production in territories outside of the EU, leading to **over reliance on supply chains for key technologies** which could be adversely affected by geopolitical developments such as trade sanctions, regional conflicts or national strategic interests.

There is a high dependency on a relatively small number of providers of hardware and software, cloud services, and service providers from a limited number of suppliers, with a significant reliance on service suppliers outside the State. For example, several critical services in the State rely on space based positioning, navigation and timing services such as the US owned GPS (Global Positioning System) and the Galileo system which is operated by the European Space Agency. These providers often possess multiple means of protecting against attacks, although at the same time, if these systems are disrupted or otherwise compromised, the impact can be substantial. Products or services provided by foreign or

domestic providers can be compromised by malicious actors either with or without the provider's knowledge. Moreover, providers must comply with legislation, meaning that in some countries, there is a possibility they may be forced to cooperate with espionage activities, or the preparations for sabotage by prepositioning for example, where surreptitious access is achieved on critical systems, to be activated at some point in the future.

The visualisation of the survey results are provided in Appendix A, and below is a list of conclusions drawn from some of the most significant survey results.

7.1 Electricity and Communications critical

Most organisations said they directly rely on the Energy/Electricity supply & Communications (Fig. 7) to support their operations. This was an anticipated result as these two NCFs are a fundamental requirement for all network and information systems in all sectors, and underscores the criticality of these NCFs in supporting a resilient National ecosystem. Any disruption to either of these NCFs has a high potential to cause cascading impacts on other sectors.

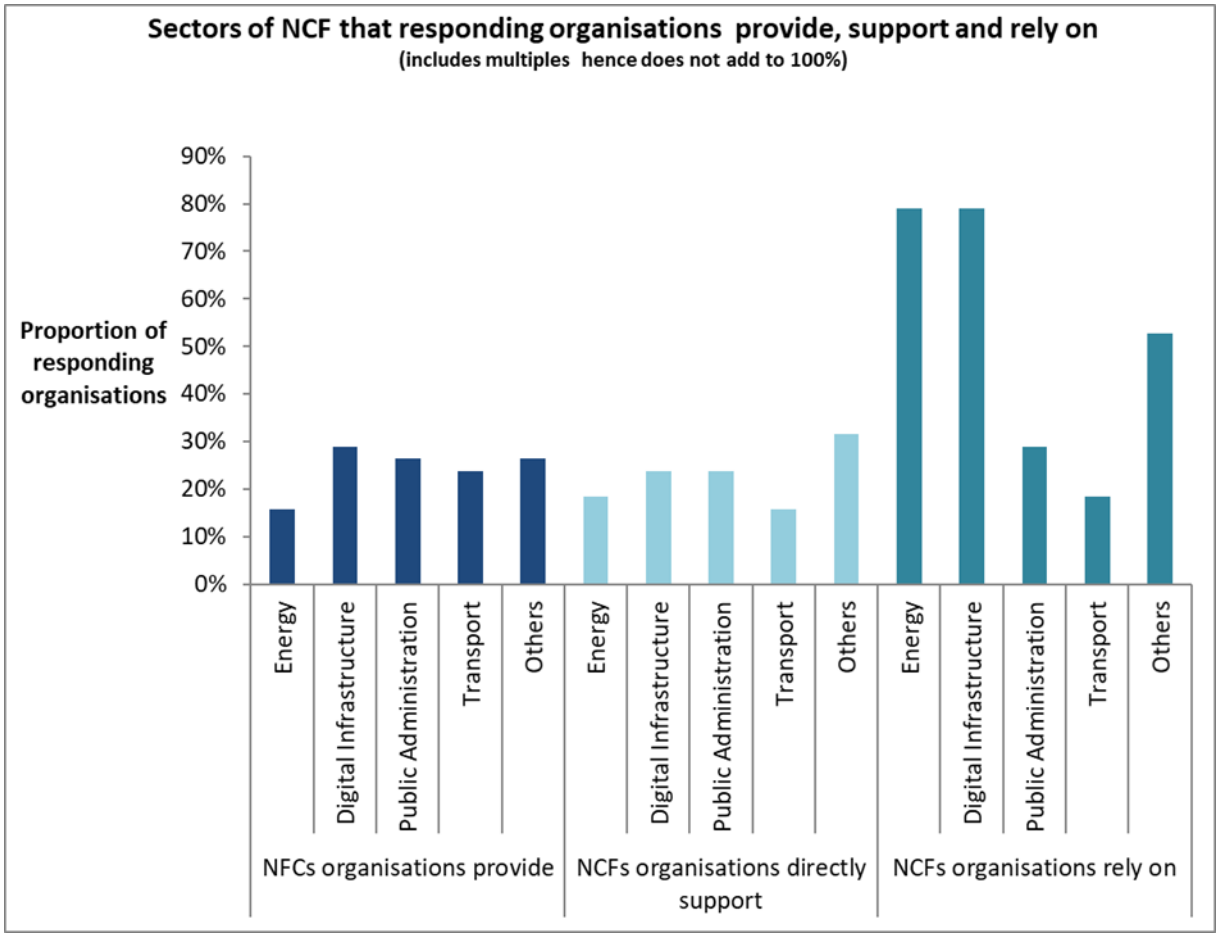


Fig 7 – Electricity and Communications are critical for ALL sectors

7.2 More focus on supply chain security required

MSPs are widely used and critical for the functioning of NCFs (92% - Fig. 8) with most having remote access (89%). Despite this only 66% of respondents demand specific security requirements from MSPs during the procurement process. Furthermore, when survey respondents were asked to rate the threats from the ENISA threat taxonomy, 'Failure or disruption of Service Providers (Supply Chain)', did not make the top 10 threats. This is surprising given the criticality of MSPs to most NCF operators and may be indicative of a lack of awareness or focus by operators on the importance of supply chain/MSP security.

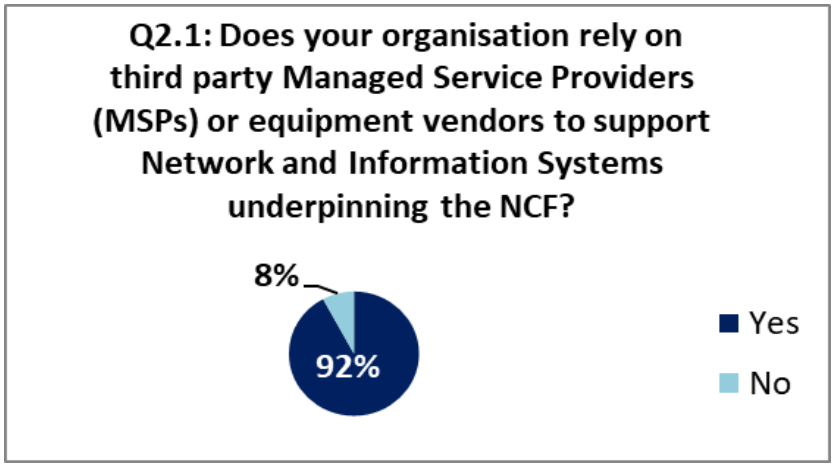


Fig 8 – High dependency on MSPs

7.3 C-suite appreciation for cyber risks is high

There is a high level of awareness of cyber risks within the C-suite, with 97% of respondents indicating C-level and Board members have an awareness of the main cyber risks that have the potential to have a significant impact on the organisations critical functions, and 95% have an awareness of the key measures/strategy in place to ensure cyber resilience. However 21% of respondents indicated that they do not implement baseline security standards/best practices to fulfil their cybersecurity requirements, indicating that more work needs to be done to ensure all critical operators embed formal cyber security programmes to manage their cyber risks.

Fig 9 – Not all CNI have cybersecurity programmes

7.4 High dependency on a small number of non-EU companies

Respondents were asked to provide information on the technology 'classes/types' in use within their critical estate. As expected, there was a wide spread of technology in use, however almost all organisations use Microsoft technologies in their operations. Apart from the obvious 'dependency' risks associated with the concentrated use of technology from a single, non EU vendor, there is also potential for 'class failures' leading to impacts across a wide range of sectors and operators. For example, in 2017 organisations all over the world were adversely impacted by the WannaCry cryptoworm, which auto replicated after infecting computers running Microsoft windows operating systems which had not applied a recently introduced patch to fix a vulnerability in the operating systems Server Message Block (SMB) protocol. And in 2020 there was widespread disruption when it was discovered that Advanced Persistent Threat (APT) actors had inserted a backdoor through the supply chain into SolarWinds, allowing the attackers to access systems running SolarWinds, a network and systems management product which would typically have privileged access across an organisations technology estate.

Furthermore, 50% of respondents indicated that they use cloud services in their operations, mostly related to business data but also significant proportion indicated they also use cloud services in their Industrial Control Systems. Almost all cloud services were based in Azure or AWS technology, both US based companies, leading to further dependency on non EU based companies.

7.5 Novel technologies on the rise

There is currently substantial use of novel technologies such as Artificial Intelligence, Big Data, 5G and IoT in use within critical entities, and this use is set to rise in the medium term with 61% of respondents indicating their intention to use novel technologies in their operations within the next 6 – 24 months. In order to maximise the potential of modern technologies, it is imperative therefore that the education system in the State has got sufficient capacity to meet the demand for skilled workers in these key technology areas, particularly in high value areas such as research, design, and understanding the risks associated with these new technologies and how to manage them.

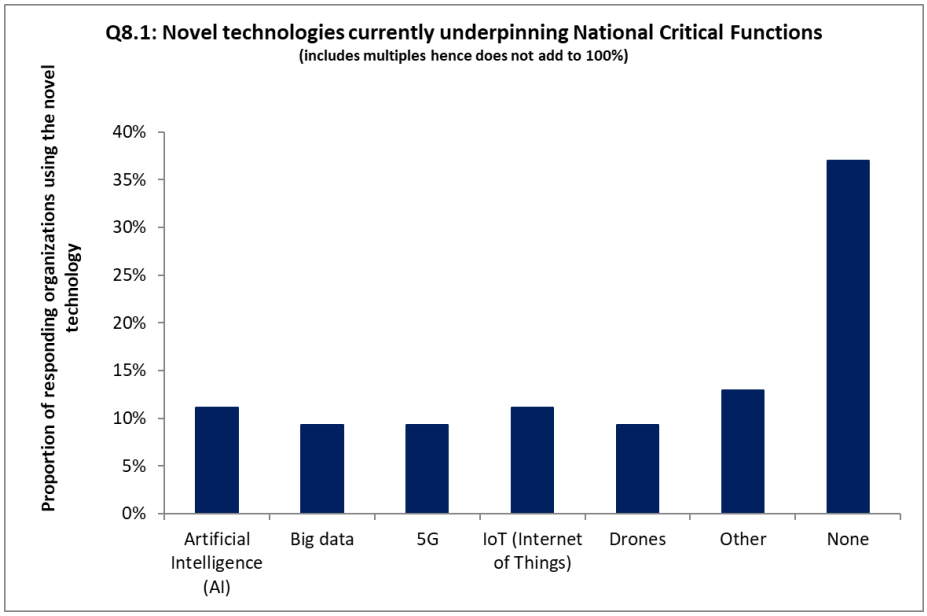


Fig 10 – Novel technologies on the rise.

8 Recommendations

There remain substantial variances in the degree of resilience between sectors. Organisations are being successfully attacked using simple methods and many incidents could have been prevented or damage mitigated if basic measures had been implemented by operators, service providers and technology vendors. Increasing complexity and connectivity of the ICT landscape is putting more and more pressure on resilience levels. Boosting resilience by raising the cybersecurity 'bar' across all elements of the technology ecosystem remains the most effective means of reducing risk to critical services.

The key recommendations to build resilience and mitigate systemic cyber risks are:

1. **Boost cyber resilience by maximising the potential of current and upcoming statutory regulations to ensure operators of critical and important services, services providers and technology vendors embed appropriate and proportional cyber security measures in their products and services from the outset.**

   The introduction of a suite of legal measures such as the Network and Information Systems (NIS) Directive and its upcoming replacement NIS2, the Cyber Security Act for certifying products and services and the upcoming Cyber Resilience Act which seeks to embed security into products, will place an emphasis on organisations to ensure services and products are created and delivered with embedded security from the outset.

2. **Manage High Risk Vendors in the supply chain by bringing forth primary legislation to allow the Minister to assess the risk profile of critical services and their underpinning Network and Information Systems, and if required, to designate certain vendors as being high risk, with the power to direct that high-risk vendors may not be used in such services or Network and Information Systems.**

   At the end of 2021, the Government endorsed the 'EU 5G Security Toolbox[52]', as the framework by which Ireland will secure its next generation electronic communications networks. This framework is now underpinned by primary legislation (Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023) which allows the Minister of the Environment, Climate and Communications to assess the risk profile of electronic communications networks or services, and if required, to designate certain vendors as being of particular concern.

Recommendation 2 is to bring forth additional primary legislation to allow the Minister to assess the risk profile of ALL critical Network and Information Systems and services, and if required, to designate certain vendors as being high risk, with the power to direct that high risk vendors may not be used in such services or NIS systems. The assessment will follow clear objective criteria such as those described in paragraph 2.37 of the 'EU Coordinated Risk Assessment of 5G Security[53]' and adding country specific information e.g., threat assessment from national security services etc:

The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

- The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks. Such interference may be facilitated by, but not limited to, the presence of the following factors:
    - a strong link between the supplier and a government of a given third country.
    - the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country.
    - the characteristics of the supplier's corporate ownership.
    - the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.
- The supplier's ability to assure supply.
- The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

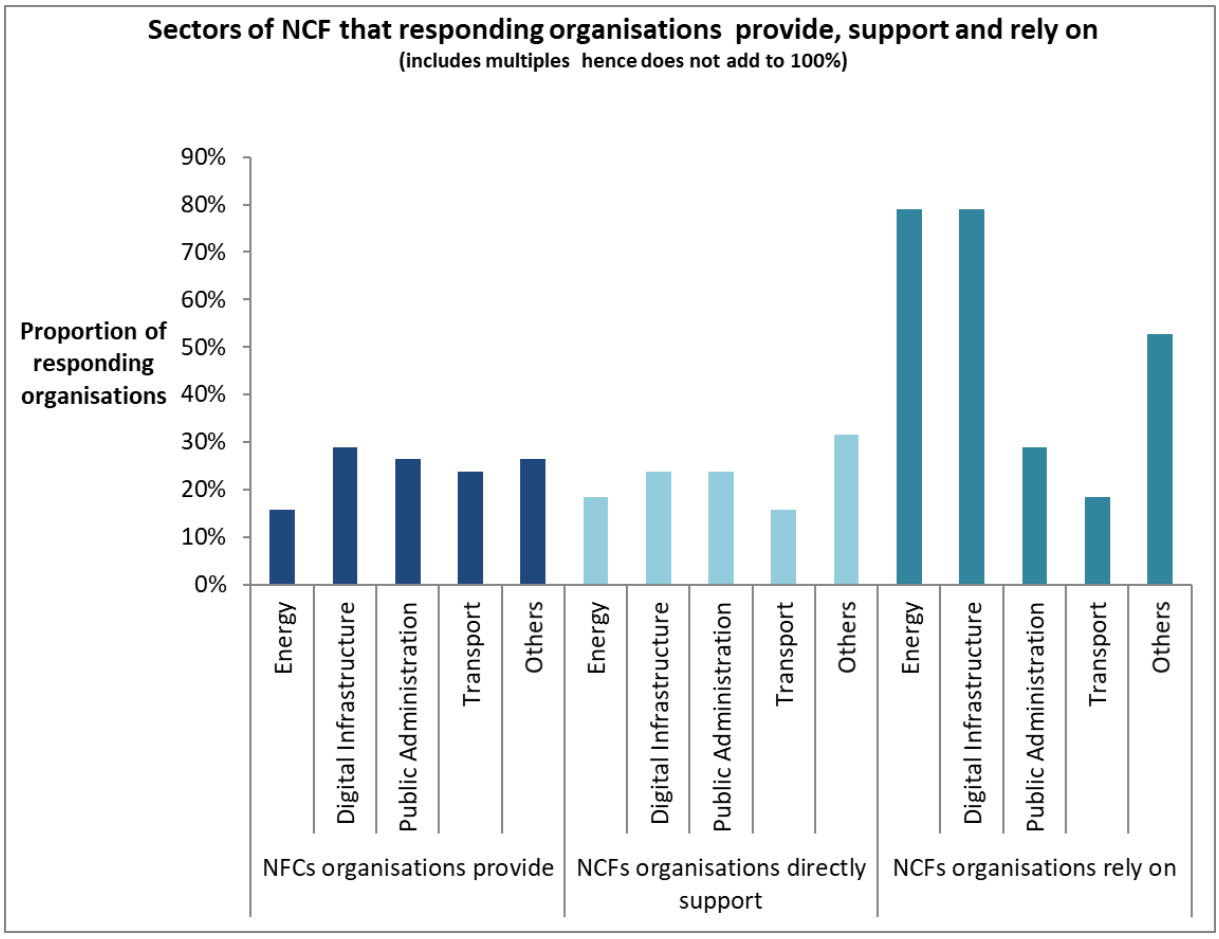
3. **Establish a Central Register of all Essential and Important Entities in the State.**

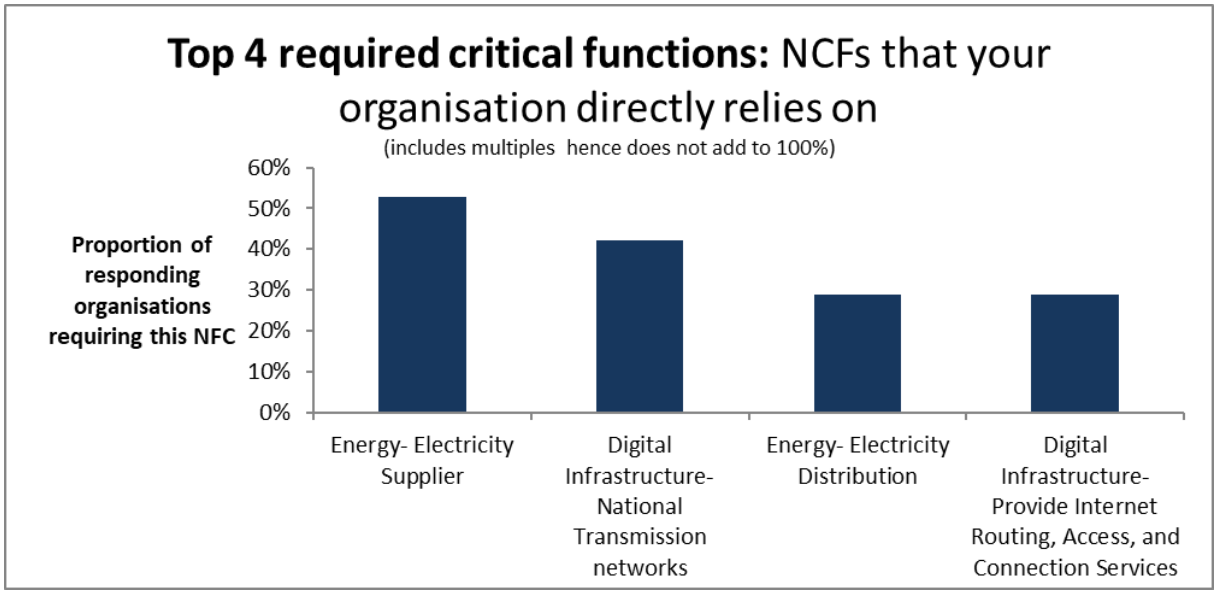
As has been previously mentioned in the methodology section of this report, the methodology and information gathered in the survey will form the basis for the creation of a National Registry which contains a list of essential and important entities containing at least the entities name, address, up to date contact details including email addresses, telephone numbers, IP ranges, key infrastructure, suppliers and MSPs. The mechanism for gathering this information has yet to be decided, however

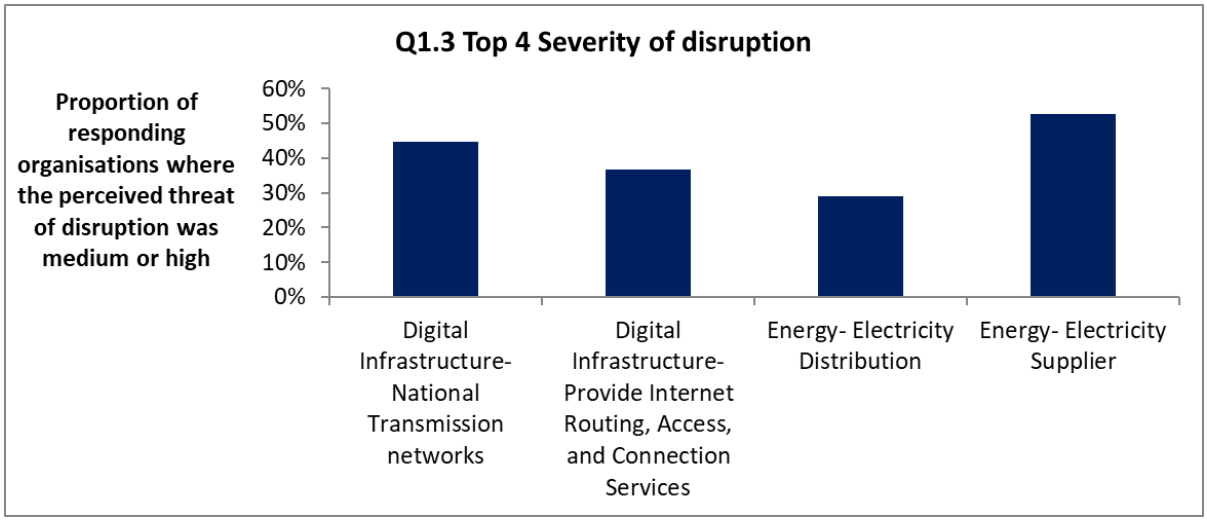
under the proposed NIS2, Member States should be able to establish national mechanisms to allow entities to register themselves.

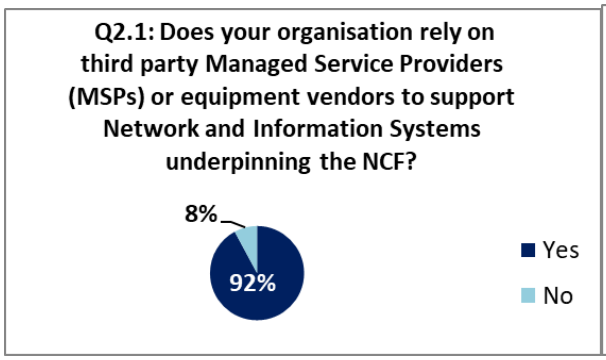
This information when combined with the criticality criteria will facilitate the identification and categorisation of Critical National Infrastructure allowing authorised users from the NCSC and other agencies to prioritise risk management activities, capture and visualise interdependencies, produce reports and conduct analysis.

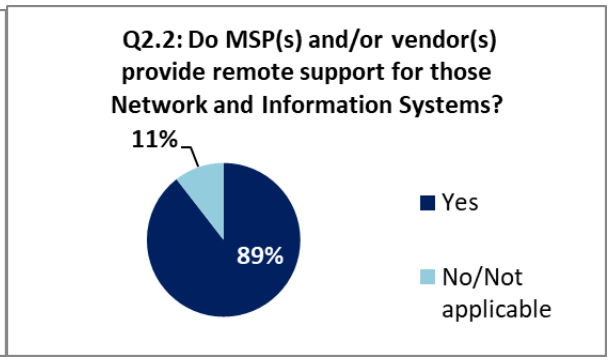
Appendix A – Survey Results

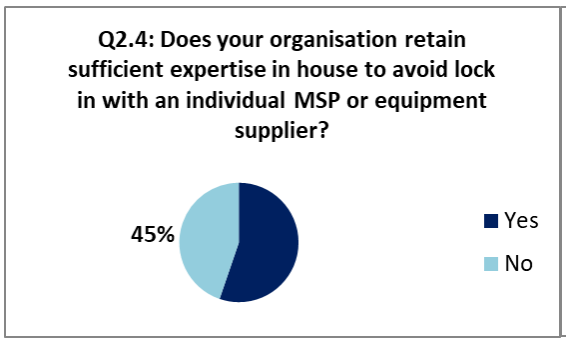


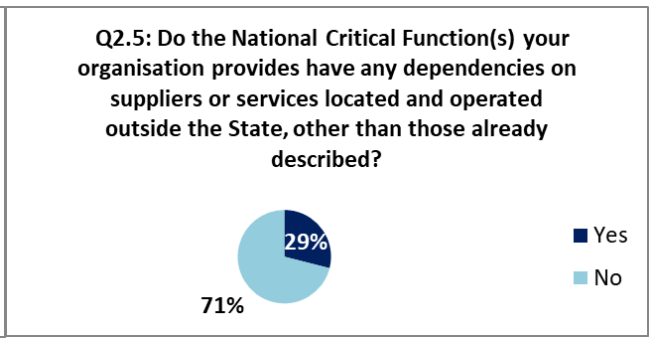


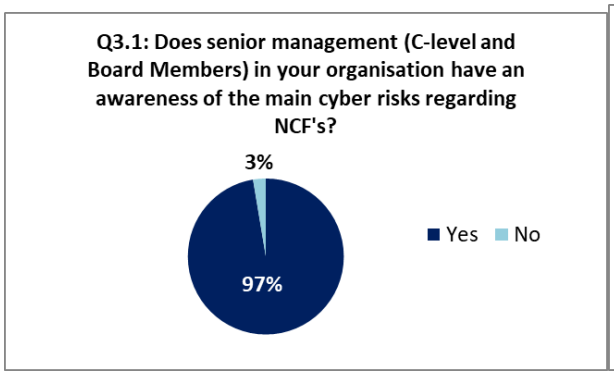

Q1.3 Top 4 Severity of disruption
Proportion of responding organisations where the perceived threat of disruption was medium or high
60%
50%
40%
30%
20%
10%
0%
Digital Infrastructure- National Transmission networks
Digital Infrastructure- Provide Internet Routing, Access, and Connection Services
Energy- Electricity Distribution
Energy- Electricity Supplier


Q2.1: Does your organisation rely on third party Managed Service Providers (MSPs) or equipment vendors to support Network and Information Systems underpinning the NCF?
8%
92%
Yes
No


Q2.2: Do MSP(s) and/or vendor(s) provide remote support for those Network and Information Systems?
11%
89%
Yes
No/Not applicable

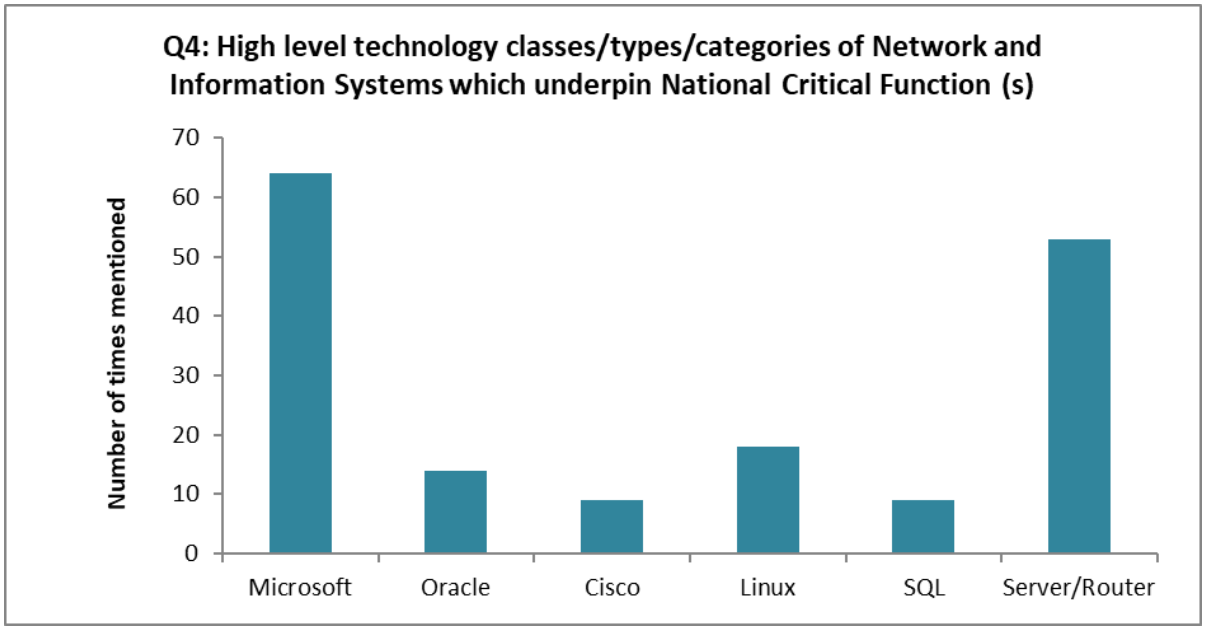

Q2.4: Does your organisation retain sufficient expertise in house to avoid lock in with an individual MSP or equipment supplier?
45%
Yes
No

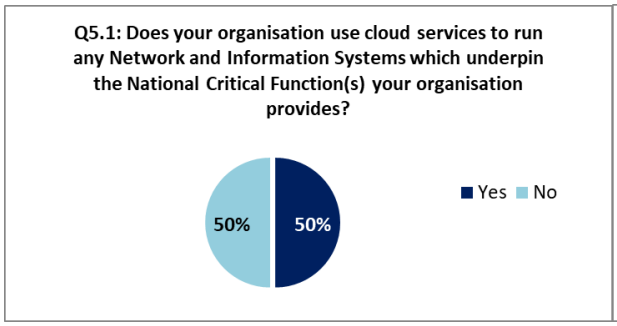

Q2.5: Do the National Critical Function(s) your organisation provides have any dependencies on suppliers or services located and operated outside the State, other than those already described?
29%
71%
Yes
No

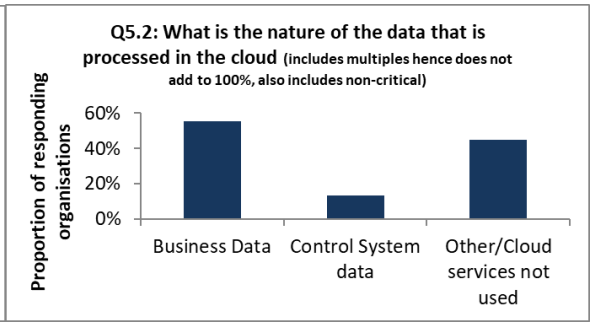

Q3.1: Does senior management (C-level and Board Members) in your organisation have an awareness of the main cyber risks regarding NCF's?
3%
97%
Yes
No

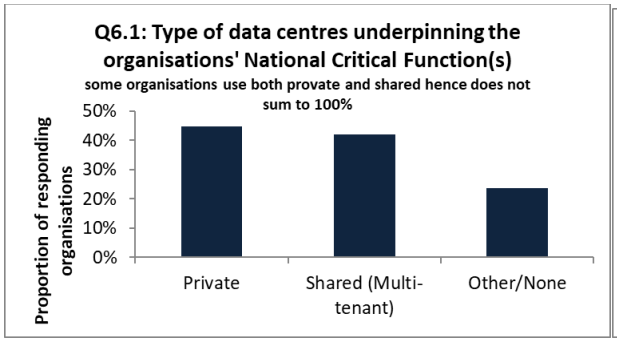

Q3.2: Does senior management (C-level and Board Members) in your organisation have an awareness of the key measures/strategy in place to ensure cyber security and resilience?
5%
95%
Yes
No

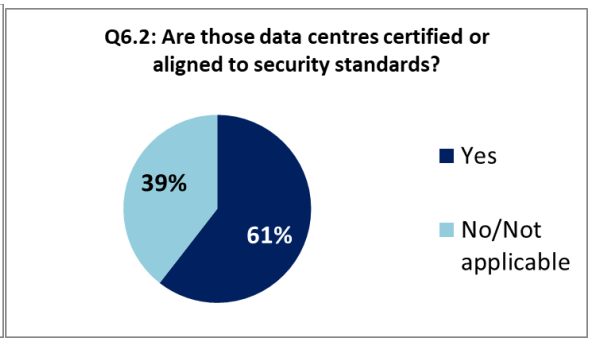

Q3.3: Does your organisation implement baseline security standards/ best practices regarding cybersecurity and NCF's?
21%
79%
Yes
No

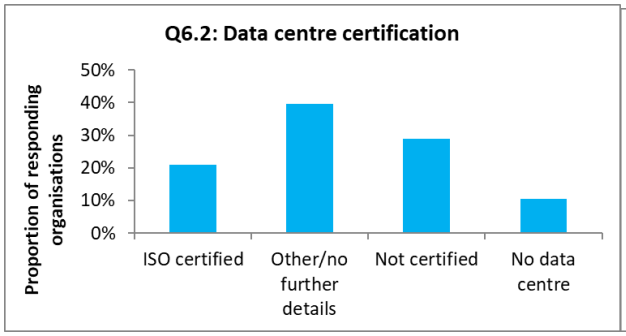

Q4: High level technology classes/types/categories of Network and Information Systems which underpin National Critical Function (s)
Number of times mentioned
70
60
50
40
30
20
10
0
Microsoft
Oracle
Cisco
Linux
SQL
Server/Router

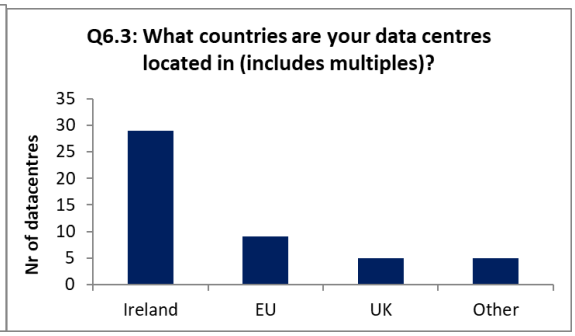

Q5.1: Does your organisation use cloud services to run any Network and Information Systems which underpin the National Critical Function(s) your organisation provides?
50%
50%
Yes
No

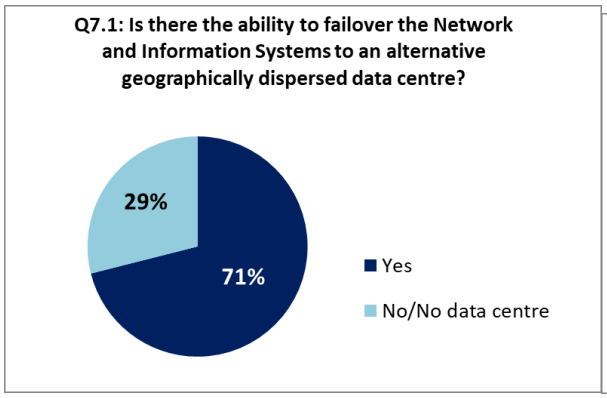

Q5.2: What is the nature of the data that is processed in the cloud (includes multiples hence does not add to 100%, also includes non-critical)
Proportion of responding organisations
60%
40%
20%
0%
Business Data
Control System data
Other/Cloud services not used

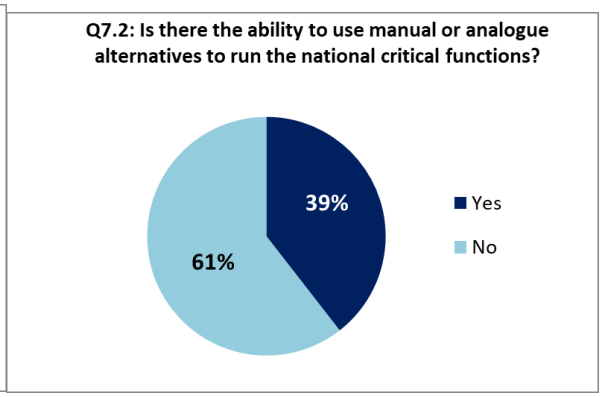

Q6.1: Type of data centres underpinning the organisations' National Critical Function(s)
some organisations use both provate and shared hence does not sum to 100%
Proportion of responding organisations
50%
40%
30%
20%
10%
0%
Private
Shared (Multi-tenant)
Other/None

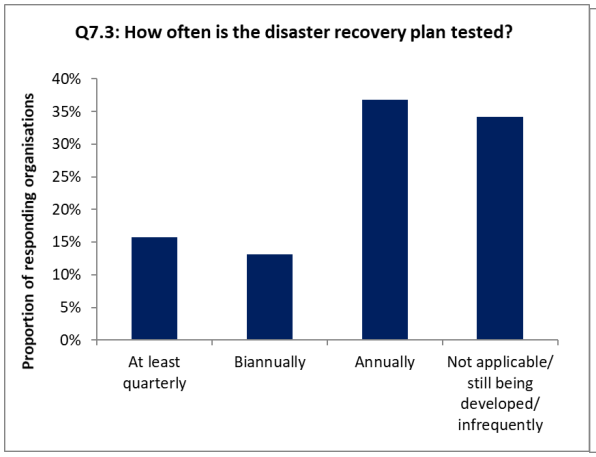

Q6.2: Are those data centres certified or aligned to security standards?
39%
61%
Yes
No/Not applicable

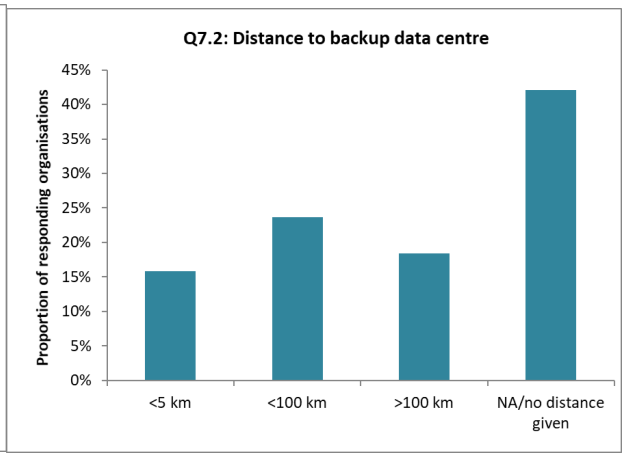

Q6.2: Data centre certification
Proportion of responding organisations
50%
40%
30%
20%
10%
0%
ISO certified
Other/no further details
Not certified
No data centre

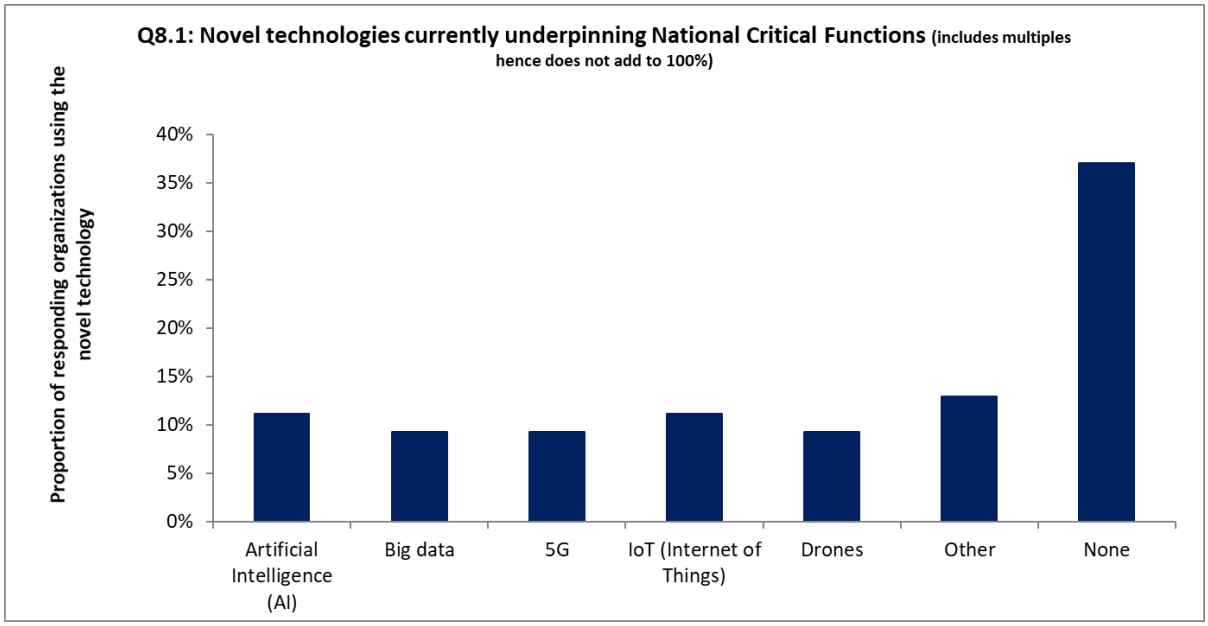

Q6.3: What countries are your data centres located in (includes multiples)?
Nr of datacentres
35
30
25
20
15
10
5
0
Ireland
EU
UK
Other

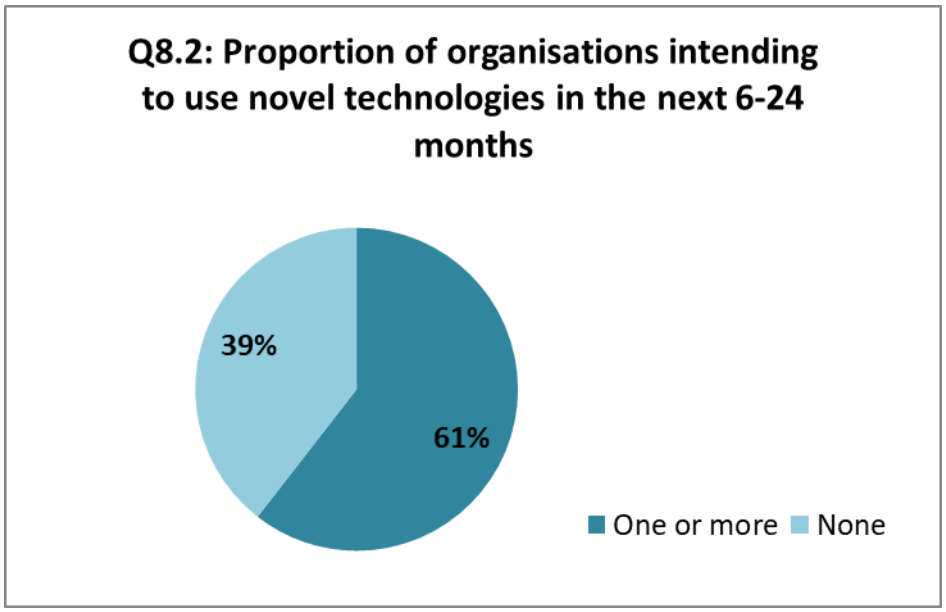

Q7.1: Is there the ability to failover the Network and Information Systems to an alternative geographically dispersed data centre?
29%
71%
Yes
No/No data centre

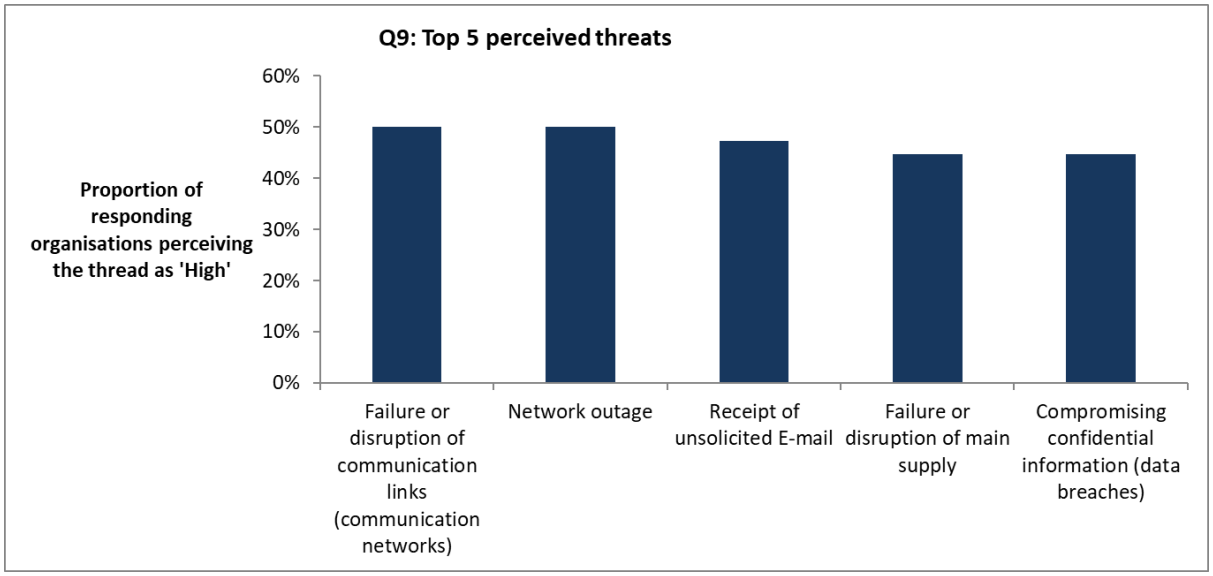

Q7.2: Is there the ability to use manual or analogue alternatives to run the national critical functions?
39%
61%
Yes
No

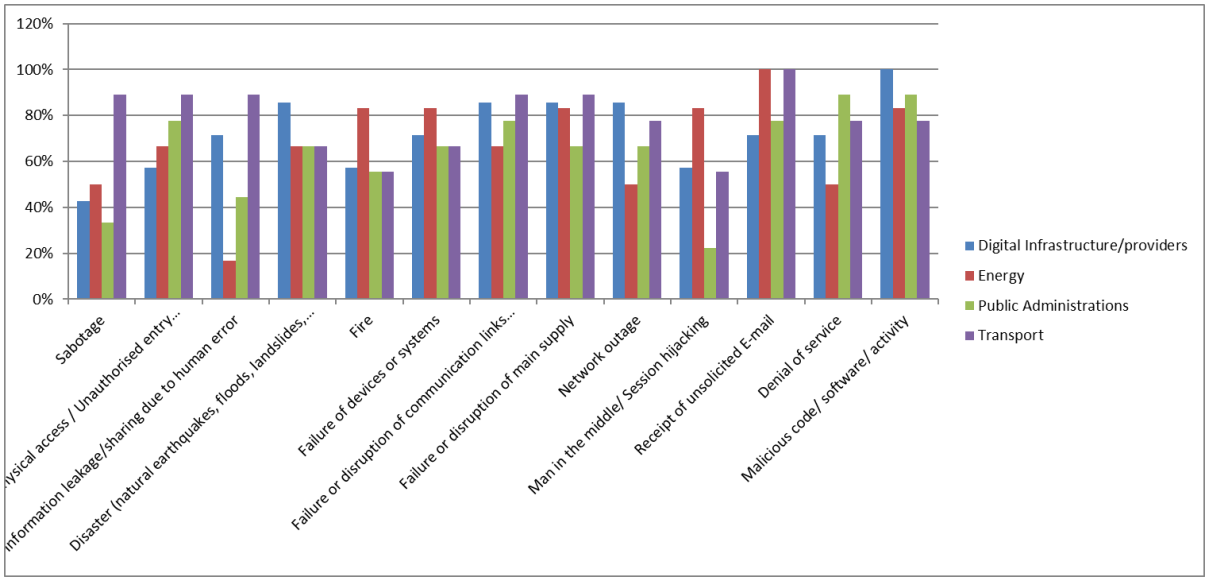

Q7.3: How often is the disaster recovery plan tested?
Proportion of responding organisations
40%
35%
30%
25%
20%
15%
10%
5%
0%
At least quarterly
Biannually
Annually
Not applicable/ still being developed/ infrequently


Q7.2: Distance to backup data centre
Proportion of responding organisations
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
<5 km
<100 km
>100 km
NA/no distance given


Q8.1: Novel technologies currently underpinning National Critical Functions (includes multiples hence does not add to 100%)
Proportion of responding organizations using the novel technology
40%
35%
30%
25%
20%
15%
10%
5%
0%
Artificial Intelligence (AI)
Big data
5G
IoT (Internet of Things)
Drones
Other
None


Q8.2: Proportion of organisations intending to use novel technologies in the next 6-24 months
39%
61%
One or more
None


Q9: Top 5 perceived threats
Proportion of responding organisations perceiving the thread as 'High'
60%
50%
40%
30%
20%
10%
0%
Failure or disruption of communication links (communication networks)
Network outage
Receipt of unsolicited E-mail
Failure or disruption of main supply
Compromising confidential information (data breaches)


120%
100%
80%
60%
40%
20%
0%
Sabotage
ysical access / Unauthorised entry...
nformation leakage/sharing due to human error
Disaster (natural earthquakes, floods, landslides,...
Fire
Failure of devices or systems
Failure or disruption of communication links...
Failure or disruption of main supply
Network outage
Man in the middle/ Session hijacking
Receipt of unsolicited E-mail
Denial of service
Malicious code/ software/ activity
Digital Infrastructure/providers
Energy
Public Administrations
Transport

Appendix B – Online Survey

Entities identified as critical were invited to complete a voluntary anonymous survey which was hosted on the EU Survey Platform[54].

1. Organisation Details:

1.1 Please select the most appropriate category for your organisation from the list below. If your Organisation falls under more than category. Please select other and list the categories in the below box.

See Annex to the Proposed directive on measures for a high common level of cybersecurity across the Union (.pdf) for entity types under the 16 sectors
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72172

1.2 National Critical Functions (NCF) and Dependencies

Guidance Notes

Provides: The NCF your organisation provides. Most organisations will provide only 1 NCF, however some organisations provide more than one NCF.
Relies: Does your organisation rely on this NCF

Dependent NCFs:NCFs that your organisation directly supports (one level up). Select the top 5 only.

Required NCFs:NCFs that your organisation directly relies on (one level down). Select the top 5 only.

See example of a dependency model in Annex A : Strategic Emergency Management Guidelines 3 – Critical Infrastructure Resilience – Version 2”

1.3 Please rate the severity of disruption your organisation would face, if the top 5 NCFs that you rely on was to suffer a disruption to service.

1.4 Please list other functions your organisation provides not listed above, which you believe qualify as a National Critical Function, and a short rationale why ot should be included.

2. Supplier Considerations

2.1 Does your organisation rely on third party Managed Service Providers (MSPs) or equipment vendor to support the Network and Information Systems which underpin the National Critical Function(s) your organisation provides?
Note: MSPs also include services provided to your organisation at Group level.

If yes, please list the MSPs/vendor(s) and the nature of the services/functions they provide using the format in the example below.

Do any of your MSP(s) and/or vendor(s) provide remote support for the Network and Information Systems which underpin the National Critical Function(s) your organisation provides?

2.2 Do any of your MSP(s) and/or vendor(s) provide remote support for the Network and Information Systems which underpin the National Critical Function(s) your organisation provides?

If yes, please list the country or countries where all your MSPs or vendors delivers the remote support to your organisation. Please list all countries, including Ireland, that apply.

2.3 Does your organisation demand specific security requirements/standards/certifications from MSPs or equipment suppliers during the procurement process?

If yes, please list the requirements, e.g. Common Criterial security evaluation level for product or system, ISO27001 certification for organisation, right to audit etc.

2.4 Does your organisation retain sufficient expertise in house to avoid lock in with an individual MSP or equipment supplier?

2.5 Do the National Critical Function(s) your organisation provides have any dependencies on suppliers or services located and operated outside the State, other than those already described? e.g. position, navigation or timing services, satellite services etc This would include navigation services such as the Galileo, GPS, GLONASS, etc

3. Baseline Security Measures

3.1 Does senior management (C-level and Board Members) in your organisation have an awareness of the main cyber risks with the potential to have a significant impact National Critical Function(s) your organisation provides?

3.2 Does senior management (C-level and Board Members) in your organisation have an awareness of the key measures/strategy in place to ensure cyber security and resilience[1]? [1] “resilience” means the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity

3.3 Does your organisation implement baseline security standards/ best practices to fulfil the cybersecurity and resilience requirements for the Network and Information Systems which underpin the National Critical Function(s) your organisation provides?

If yes, please describe e.g. aligned or certified with security standards or frameworks such as ISO27001, IEC62443, NIST Cyber Security Framework etc.

4. Technology class/type/category failures

4.1 Please list the high level technology classes/types/categories of Network and Information Systems which underpin the National Critical Function(s) your organisation provides.
This question is to capture potential cascading failures which could affect network and information systems which are common within or between critical sectors.Note: Technology class/type/category in this context refers to technology vendor and its function within your ICT estate. Some examples are listed below, please expand this list where necessary. Software versions, hardware model numbers etc are not required.

- Desktop estate runs Microsoft operating system

- Midrange Server estate runs Red Hat Linux operating system
- Midrange Server estate runs Microsoft operating system
- Network equipment (switches, routers) are CISCO/ Ericsson/ Huawei based
- Industrial Control Systems (SCADA/ DCS) are Honeywell/Siemens/Schneider based Middleware environment is Oracle WebLogic/ Apache Tomcat based
- Database environment is Microsoft SQL/ Oracle/ Ingres based
- Messaging platform is Kafka/ IBM MQ based CMS is WordPress/ Joomla based

Note: Answers should be high level and not more than one line answers for each technology classes/types/categories.

5. Cloud Services

5.1 Does your organisation use cloud services to run any Network and Information Systems which underpin the National Critical Function(s) your organisation provides?

If yes, please list:
- the cloud service provider, eg Azure, AWS, etc
- the cloud service model (IAAS, PAAS, SAAS)
- the cloud deployment model (Private, Public, Hybrid, Community)
- the geographical locations your organisations cloud services configured to run in, and or geographical locations your data resides

5.2 What is the nature of the data that is processed in the cloud?
- Business Data
- Control System data
- Other

6. Data centres

6.1 Does your organisation use private or shared (multi tenant) data centres to run the Network and Information Systems which underpin the National Critical Function(s) your organisation provides.
- Private
- Shared (Multi-tenant)
- Other

6.2 Are your data centres which host the Network and Information Systems which underpin the National Critical Functions your organisation provides certified or aligned with any relevant security standards or certifications, eg Uptime Institute Tier classification, ISO standard etc

6.3 What Countries are your data centres located in?

6.4 Please provide details of ancillary systems if any, other that the usual HVAC, UPS etc, which are necessary for the operation of your organisations Network and Information Systems which underpin the National Critical Functions your organisation provides: e.g. constant water supply, transport services, critical materials or chemicals etc

7. Disaster Recovery / Contingency planning

7.1 Does your organisation have the ability to failover the Network and Information Systems which underpin the National Critical Functions your organisation provides to an alternative geographically dispersed data centre to prevent or minimise the impact of an incident?

7.2 Please provide additional details, eg distance between data centres

7.3 How often is the disaster recovery plan tested?

7.4 Does your organisation have manual or analogue alternatives to run national critical functions your organisation provides which are ordinarily dependent on Network and Information Systems selected in section 1?

Manual or analogue alternative in this context refers to performing a function without the use of network and information systems, eg using a paper based system to record transactions or issue tickets, manual interventions in an industrial process etc

8. Novel Technologies

8.1 Please select any novel technologies which your organisation uses to underpin the National Critical Functions your organisation provides?

- Artificial Intelligence (AI)
- Augmented Reality (AR)
- Robotics
- Quantum Computing
- Big data
- 5G
- Novel Energy Storage
- Blockchain
- IoT
- Drones
- 3D Printing
- Other
- None

8.2 Please list any novel technologies your organisation intends to use in the near or medium term future to make use of novel technologies in the near to medium term future (within 6 - 24 months) to underpin the National Critical Functions your organisation provides?

9. Threats

Please indicate how your organisation rates the following threats to the Network and Information Systems which underpin the National Critical Function(s) your organisation provides?
Options: High, Medium, Low, Not Rated (ie threat has not been considered), Not Applicable
Note: Please apply a rating based on the inherent risk of the threat, without taking into account any controls in place.
Threats are taken from the ENISA Threat Taxonomy.

9.1 Physical attack (deliberate/intentional)

- Fraud
- Sabotage
- Vandalism
- Theft (devices, storage media and documents)
- Information leakage/sharing
- Unauthorized physical access / Unauthorised entry to premises
- Coercion, extortion or corruption
- Damage from the warfare

- Terrorists attack

9.2 Unintentional damage / loss of information or IT assets
- Information leakage/sharing due to human error
- Erroneous use or administration of devices and systems
- Using information from an unreliable source
- Unintentional change of data in an information system
- Inadequate design and planning or improperly adaptation
- Damage caused by a third party
- Damages resulting from penetration testing
- Loss of information in the cloud
- Loss of (integrity of) sensitive information
- Loss of devices, storage media and documents
- Destruction of records

9.3 Disaster (natural, environmental)
- Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)
- Fire
- Pollution, dust, corrosion
- Lightning Strike
- Water
- Explosion
- Dangerous radiation leak
- Unfavourable climatic conditions
- Major events in the environment
- Threats from space / Electromagnetic storm
- Wildlife

9.4 Failures/malfunction
- Failure of devices or systems
- Failure or disruption of communication links (communication networks)
- Failure or disruption of main supply
- Failure or disruption of service providers (supply chain)
- Malfunction of equipment (devices or systems)

9.5 Outages
- Loss of resources
- Absence of personnel
- Strike
- Loss of support services
- Internet outage
- Network outage

9.6 Eavesdropping/ Interception/ Hijacking
- War driving
- Intercepting compromising emissions
- Interception of information
- Interfering radiation
- Replay of messages
- Network Reconnaissance, Network traffic manipulation and Information gathering
- Man in the middle/ Session hijacking

9.7 Nefarious Activity/ Abuse

- Identity theft (Identity Fraud/ Account)
- Receive of unsolicited E-mail
- Denial of service
- Malicious code/ software/ activity
- Social Engineering
- Abuse of Information Leakage
- Generation and use of rogue certificates
- Manipulation of hardware and software
- Manipulation of information
- Misuse of audit tools
- Misuse of information/ information systems (including mobile apps)
- Unauthorized activities
- Unauthorized installation of software
- Compromising confidential information (data breaches)
- Hoax
- Remote activity (execution)
- Targeted attacks (APTs etc.)
- Failed of business process
- Brute force
- Abuse of authorizations

Legal

- Violation of laws or regulations / Breach of legislation
- Failure to meet contractual requirements
- Unauthorized use of IPR protected resources
- Abuse of personal data
- Judiciary decisions/court orders

Other Information

Please include any other information (for example threats or vulnerabilities external to your organisation which you cannot directly control), which you believe could lead to ‘systemic cyber risks’.

[1] ENISA Threat Landscape 2022, Section 10.1.4

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[2] Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Consilium (europa.eu)

https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[3] Cyber-attacks: Declaration by the High Representative on behalf of the European Union expressing solidarity with Albania and concern following the July malicious cyber activities | EEAS Website (europa.eu)

https://www.eeas.europa.eu/delegations/albania/cyber-attacks-declaration-high-representative-behalf-european-union-expressing_en?s=214

[4] China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory - Consilium (europa.eu)

https://europa.eu/!3mPkR4

[5] Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union

https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[6] Cyber-attacks: Declaration by the High Representative on behalf of the European Union expressing solidarity with Albania and concern following the July malicious cyber activities

https://www.eeas.europa.eu/delegations/albania/cyber-attacks-declaration-high-representative-behalf-european-union-expressing_en?s=214

[7] UK condemns Iran for reckless cyber attack against Albania

https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania

[8] Sustained Activity by Threat Actors- Joint Publication

https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication

[9] ENISA Threat Landscape 2022, Page 90, Threat actors linked to China,

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[10] EU imposes the first ever sanctions against cyber-attacks

https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

[11] Council implementing regulation concerning restrictive measures against cyber-attacks threatening the Union or its member states, 30 July 2020

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125&from=EN

[12] Threat Group Cards: A Threat Actor Encyclopedia

https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima

[13] Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape

https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

[14] What is Cyber Big Game Hunting? | CrowdStrike

https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/?msclkid=aed170d2cfa911ec8c49d59fe8fb591c

[15] *National Security Council cyber chief: Criminals are closing the gap with nation-state hackers*, 25-04-2019,

https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/.

[16] https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5

[17] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[18] The mechanics of a sophisticated phishing scam and how we stopped it

https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

[19] Verizon – 2021 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir

[20] CERT-EU - Threat Landscape Report (Volume 1)

https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

[21] Coveware – Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority – https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

[22] CrowdStrike - 2021 Global Threat Report

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

[23] ZDNet - Ransomware as a service is the new big problem for business - https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/

[24] Checkpoint - Ransomware Evolved: Double Extortion

https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/

[25] IBM Security Intelligence - The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015 - https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/

[26] Dark Reading - The State of Hacktivism in 2020

https://www.darkreading.com/the-state-of-hacktivism-in-2020-/d/d-id/1338382

[27] Predatory Sparrow operation against Iranian steel maker (2022)

https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022)

[28] https://techmonitor.ai/technology/cybersecurity/ignitis-ddos-attack-lithuania-killnet-russia

[29] https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/

[30] https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport

[31] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[32] The threat matrix is based on the actor typology in *'Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment'*, by M. de Bruijne, M. van Eeten, C. Hernandez Ganan and W. Pieters (TU Delft, 2017).

[33] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[34] https://www.weforum.org/reports/global-risks-report-2022

[35] World economic Forum – Understanding Systemic Cyber Risk

https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

[36] Strategic Emergency Management Guidelines 3 – Critical Infrastructure Resilience – Version 2 https://assets.gov.ie/90683/7d83eda8-4ff1-4a42-9c22-2d614c8a2d28.pdf

[37] US Department of Homeland Security and US Department of Transportation, *Transportation Systems Sector-Specific Plan 2015*, available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

[38] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[39] https://www.csis.org/analysis/securing-subsea-network-primer-policymakers

[40] https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

[41] https://www.irishtimes.com/business/technology/dublin-is-now-europe-s-largest-data-hosting-cluster-1.3808500

[42] https://www.submarinecablemap.com/

[43] https://www.telegraph.co.uk/news/2021/05/22/exclusive-russia-number-one-threat-submarines-circle-britain/

[44] https://www.businessinsider.com/russian-agents-went-to-ireland-to-inspect-undersea-cables-report-2020-2?r=US&IR=T

[45] https://www.irishmirror.ie/news/irish-news/could-russia-cut-ireland-worlds-26050218

[46] European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears

[47] https://www.washingtonpost.com/world/2022/01/19/tonga-volcano-eruption-cable-damage/

[48] Digital Day 2021: Europe to reinforce internet connectivity with global partners

https://politico.us8.list-manage.com/track/click?u=e26c1a1c392386a968d02fdbc&id=3ae098f666&e=a2366b0924

[49] https://www.cisa.gov/national-critical-functions-set

[50] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[51] SEM Emergency Planning Documents

https://www.gov.ie/en/collection/5ef65-publications/#sem

[52] EU 5G Security Toolbox

https://op.europa.eu/en/publication-detail/-/publication/7def1c03-da16-11eb-895a-01aa75ed71a1/language-en

[53] EU Coordinated risk assessment of the cybersecurity of 5G Networks

https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[54] EU Online Survey Platform

https://ec.europa.eu/eusurvey/home/welcome