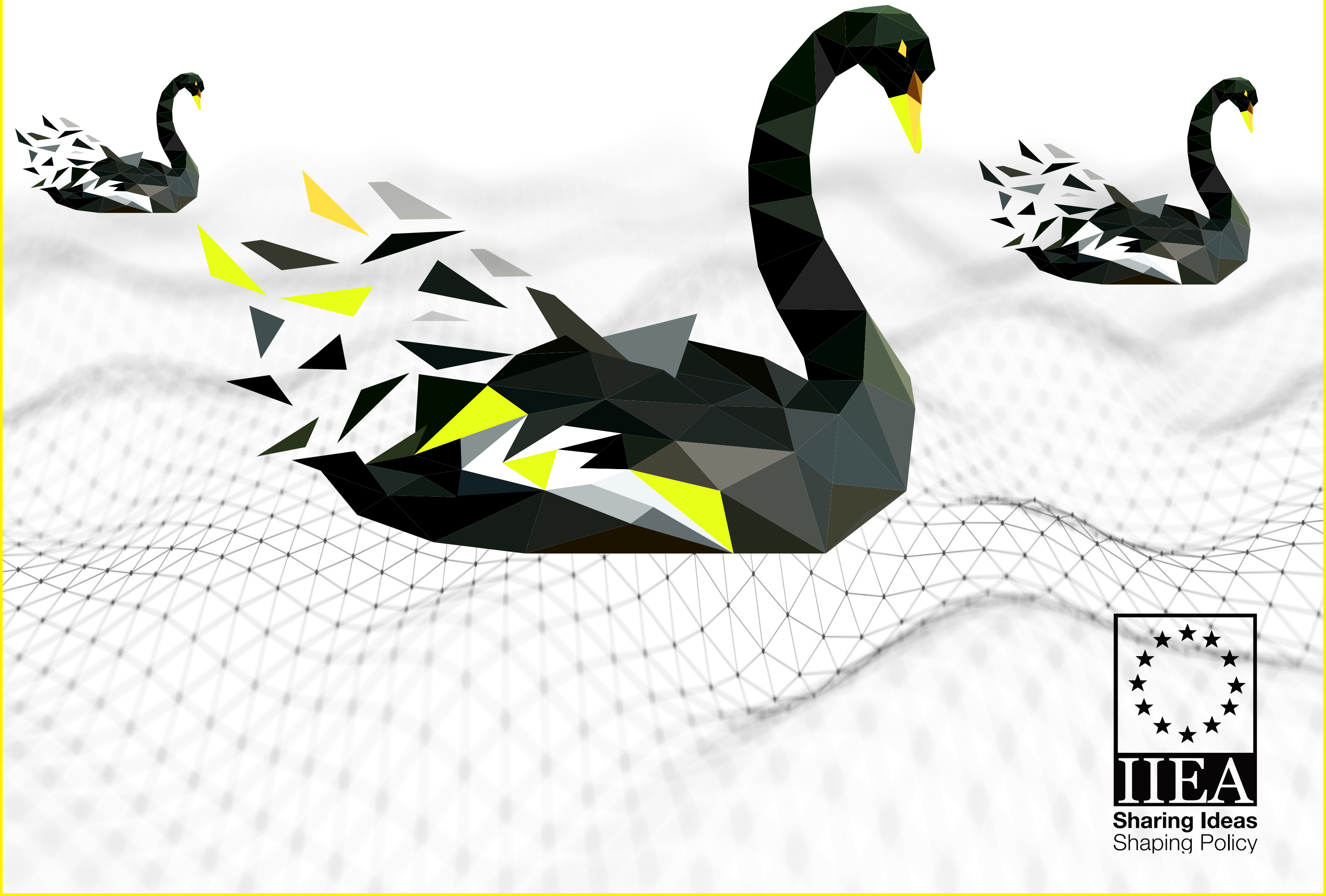
# BLACK SWANS IN THE GREY ZONE:

## Defending Ireland's Energy System Against Cyber Threats

Cian Fitzgerald



IIEA
Sharing Ideas
Shaping Policy

## Table of Contents

# I. Executive Summary

Ireland finds itself in a more contested and dangerous international context, in which threats are more multifaceted, frequent, and severe. Crises such as a cyber-attack on the electricity grid are understood as 'Black Swan' events and in this new geopolitical environment the likelihood and frequency of such events occurring is increasing.

Since Russia's annexation of Crimea in 2014, this process of geopolitical destabilisation has accelerated. The Russian Federation is deploying a diverse range of tools ranging from the use of cyberwarfare instruments, the use of denial-of-service and malware attacks, information and economic warfare, public military exercises, energy market manipulation, and, of course, using military force to achieve its political aims and enhance its relative power.

Ireland is potentially an attractive target for such an attack. Ireland's economic and international successes, its relationship to both the EU and the UN, its attractiveness to multinational companies, and the large amount of important global communications infrastructure, combined with the State's relatively soft defences, could potentially enable would-be attackers to cause disruption on an exponential scale – disrupting life not only in Ireland, but potentially across the North-Atlantic area.

Consequently, the Irish State will have to develop the means to not only actively defend energy infrastructure from attack but will likely have to develop the means to make society more resilient against the shocks caused by potential cyberwarfare campaigns against the state. The government is already obliged to consider the resilience of its critical entities due to the Critical Entities Resilience (CER) Directive which came into force in January 2023.

This paper will explore both the present Irish threat environment and how the implementation of the CER directive could potentially be augmented through a whole-of-society approach modelled on the Swedish Total Defence Framework. Drawing on this, this paper makes a number of recommendations for howthe resilience of the Irish energy sector, and ultimately the state itself, can be increased.

## II. Introduction

Ireland finds itself in a more contested and dangerous international context, in which threats are more multifaceted, frequent, and severe. Crises such as a cyber-attack on the electricity grid are understood as 'Black Swan' events and in this new geopolitical environment the likelihood and frequency of such events occurring is increasing.[1] Black Swan events are events which have seismic impacts and which, due to flawed or limited empirical information, are assumed to be highly improbable. Yet, Black Swan events are more probable than we would like to think. The expression's origins can be traced back to the 2nd century CE, when, until Dutch explorers encountered them in 1697 in Western Australia, Black Swans were simply thought not to exist by Europeans. In the Western knowledge system, Black Swans did not exist - until they did.

In the last few decades, as the world has shifted away from an ostensible period of monopolarity, the intensification of competition between powers means the global security landscape has changed from one of relative stability to one of relative instability. In this unstable environment, in which hostile state actors project power and influence through the use of hybrid attacks, Ireland is at increased risk of a major attack of national scale.

In particular, Ireland's economic and international successes, its relationship to both the EU and the UN, its attractiveness to multinational companies and the large amount of important global communications infrastructure mean it is a potential target. Its interconnectedness and openness means that potential adversaries based in Ireland may be able to create disruption and deliver attacks which can reverberate throughout the international system and affect our partners. In other words, Ireland may be both a target and a vector of attack by which to disrupt economic, political, and social life in both Ireland and the wider Euro-Atlantic region.

As will be discussed in this paper, Ireland's energy grid may be a target for such an attack. As a host to some 30% of all European data as well as cable infrastructure critical to global communications,[2] sustained and large-scale power outages would not only likely disrupt Irish communications and society but would have the potential to disrupt life in other EU Member States.

In particular, disruptions to Ireland's electrical grid infrastructure could interrupt the operations of other critical infrastructure such as financial, communication, and healthcare services, resulting in significant societal, commercial, and human costs in Ireland as well as the wider Euro-Atlantic region.

This paper will analyse the present threat environment, before assessing how increasingly assertive actors such as Russia deploy a range of instruments as part of a coordinated campaign designed to tilt the global balance of power in their favour, and examine the position of Ireland in this contested space.

This paper will look at the EU's CER Directive, which came into force in January 2023, and which now obliges the State and actors in Ireland's energy system to conduct assessments of the risks posed by antagonistic state and non-state actors' use of cyberattacks.

[1] See Taleb 2001 Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets. Random House; and Taleb 2007 The Black Swan: The Impact of the Highly Improbable. Random House

[2] NCSC 2019: 8 National Cyber Security Strategy. Available at: https://www.ncsc.gov.ie/strategy/

This paper will also consider the potential lessons for Ireland from Sweden's model of Total Defence which utilises a whole-of-society approach to national security, and how this approach can be used to augment Ireland's implementation of the CER Directive. In keeping with this, this paper will make recommendations as to how the State can enhance its resilience through a whole-of-society approach towards defence.

## III. Ireland in a Geostrategic Battlespace

In the past decade, competition between states has intensified. Revanchist states such as China, but today most notably, the Russian Federation, express dissatisfaction with the multilateral order and are working to reorder it in their favour.[3] As Ireland plays an ever-growing role in the interconnected economies of the Euro-Atlantic area,[4] it is likely to be perceived by the adversaries of the West as aligned, if not allied, with the West's interests. Irish society, business, and citizens could be considered legitimate targets in this ostensible struggle over the future of the international system.

While this is unlikely to manifest as direct conflict, there are other potential threats that exist beneath the threshold of conflict. The main exponent of such methods in recent years has been the Russian Federation. As things stand, and as aptly demonstrated by Russia's military failures in Ukraine, a direct confrontation with the West would not be viable for Russia. Instead, it has elected to pursue an oblique mode of engagement termed non-linear warfare or 'hybrid warfare' against its perceived adversaries in the West. Hybrid warfare is a strategic-level effort to shape the governance and geopolitical orientation of a target state[5] which can include the use of disinformation, espionage, cyber-attacks, military exercises, and potentially the use of military force as demonstrated in Ukraine.

Of particular note for this paper is cyberwarfare techniques, which are mobilised to great effect by Russian state and state-sponsored non-state actors. Online networks can be used to try to undermine democratic processes, launch disinformation and propaganda campaigns, steal information, and release sensitive data into the public domain. In the worst cases, Russian cyber activity can allow them to effectively take control of military systems and assets of other states.[6] Most importantly for this paper, the growth of digitalisation and internet-based public and private services has created potential vulnerabilities which can enable state and non-state actors alike to disable or weaken critical infrastructure including electricity grid, communications, financial, and medical services.

Although Russia is technologically inferior to the West in terms of both capability and resources, it has been able to deploy cyberwarfare techniques with a high degree of success.[7] As Dr Richard Brown, the head of Ireland's National Cyber Security Centre, stated at an Oireachtas hearing in spring 2022, Russia is responsible for 65% of cyber incidents

[3] Mazzar 2015: 4 Mastering the Grey Zone: Understanding A Changing Era of Conflict. Strategic Studies Institute and U.S. Army War College.

[4] David O'Sullivan 30 June 2022. Ireland will need to develop a new vocabulary to talk about national security. Irish Times. Available at: https://www.irishtimes.com/opinion/2022/06/30/ireland-will-need-to-develop-a-new-vocabulary-to-talk-about-national-security/

[5] Clark 2020: 11 Russian Hybrid Warfare:  Military Learning and the Future of War Series. Institute for the Study of War. Available at: https://understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

[6] Fiott and Parkes 2019: 5 Protecting Europe: The EU's Response to Hybrid Threats. Challiot Paper 151 April 2019. EUISS. Available at: https://www.iss.europa.eu/content/protecting-europe-0

[7] Kristiansen and Hoem 2021. Russian Cyber Strategy. Small Wars Journal. Available at: https://smallwarsjournal.com/jrnl/art/russian-cyber-strategy#_edn87

globally, and is believed to have been behind the cyber-attack against the Health Service Executive (HSE) in May 2021.[8] Normally, cyber-attacks are viewed individually and as limited in scope and not as part of a coherent and intentional state-backed campaign. This view of cyber-attacks has resulted in the mistaken perception that they are not necessarily among the most serious of national security threats insofar as their effects will only be limited to the digital realm.[9]

However, Russia's cyberwarfare strategy operates incrementally and is intended to maximise impact on the target state while minimising the risk of punishment in response to its actions. By favouring incrementalism, while requiring a greater degree of strategic patience, Russia's cyber campaign enables it to make 'small changes' none of which 'in isolation amount to' an act of war, but which can compound over time to change the strategic picture.[10] Since cyberattacks allow antagonists to act from a distance and can be difficult to attribute,[11] this makes them a weapon of choice for the Russian Federation for targeting the military, private sector, and government networks of other states. Moreover, the Russian Federation further complicates the picture by veiling its cyberwarfare campaign with cybercriminality, giving state-backed cyberwarfare the appearance of run-of-the-mill criminal behaviour, which often causes target states to underestimate the danger they are facing. One such example was the NotPetya attack[12] - a ransomware attack carried out by Russian hacking groups, acting on behalf of the Kremlin, which targeted both private companies and government services in Ukraine. In this attack alone, Maersk lost 300 million USD and the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant was knocked offline. Global losses are estimated to exceed 10 billion USD.[13]

In light of the increasingly adversarial relations between Russia and the West, and the successes Russia has achieved to date in its cyberwarfare campaigns, it is likely that it will continue to target networks and resources that are critical to maintaining the functioning of society without discriminating between private and public resources or respecting borders in order to weaken the resolve, resilience, and ability of the West's to protect itself and its interests.

Consequently, the realities of the present geostrategic threat environment mean that Irish businesses are in danger of attack by an adversary who is willing to target civilians to achieve its political aims. In Europe it is estimated that 80-90% of critical infrastructure, including energy infrastructure, are operated by the private sector,[14] rendering businesses in the energy sector prospective targets in Russia's logic of warfare. In this way,

[8] Richard Brown 30 March 2022. Oireachtas Hearing: Cybersecurity and Hybrid Threats Following the Russian Invasion of Ukraine: Discussion. Oireachtas. Available at: https://debatesarchive.oireachtas.ie/debates%20authoring/debateswebpack.nsf/committeetakes/TTJ2022033000002#N02300

[9] Leigher 2021:9 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

[10] Mazzar 2015: 15 Mastering the Grey Zone. US Army War College

[11] Aho, Midoes and Snore 2020: 19 Hybrid Threats in the Financial System. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf

[12] Leigher 2021:12 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/publications/hybrid-coe-paper-10-cyber-conflict-in-a-hybrid-threat-environment-death-by-a-thousand-cuts/

[13] NATO Cooperative Cyber Defence Centre of Excellence 2022 NotPetya (2017). CCCDOE. Available at: https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)

[14] Limnell 2018 Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed. Hybrid COE. Available at: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-6-countering-hybrid-threats-role-of-private-sector-increasingly-important-shared-responsibility-needed/

the Kremlin considers the prosecution of this war between itself and its adversaries as a whole-of-government activity.[15] As the Kremlin deploys its resources against our societies, a whole-of-society approach to national security will be required to ensure both government and commercial interests, as well as civilians, are protected. Yet, though private companies' core business duty is not national security, industry will have to play an integral part of Ireland's and Europe's security architecture, nonetheless.

## IV. Threats to Ireland's Energy Sector

Disruption to the energy supply can damage the economy and can limit access to clean drinking water, spread disease, cause food shortages, and increase mortality rates in hospitals and nursing homes.[16] Cognisant of the effects energy supply disruptions can have for target states, the Russian Federation has instrumentalised and targeted energy as a means of coercion. Indeed, it has been highlighted that energy can be both a target and a means of antagonistic behaviour. For example, energy infrastructure could be targeted by sabotaging electricity grids while Europe's (now decreased) reliance on Russian gas imports has been weaponised as a form of political blackmail[17] in an attempt to undermine Europe's support for Ukraine's self-defence against Russia's war of aggression.
Consequently, it is possible that the Russian Federation may yet target the energy grids of vulnerable states using cyber means. Russia has already demonstrated its capabilities when it comes to disabling energy infrastructure via cyber means when on 23 December 2014, Russia, after months of targeting and preparatory attacks,[18] carried out a devastating cyber-attack on the Ukrainian power grid. Some 225,000 customers were left without power following the synchronised attack on three regional electric power distribution companies.[19] In this incident, Russia demonstrated that it had the capability to reach and disrupt critical infrastructure without immediate physical access or proximity and that they had the technical and structural capability to perform the long-term preparations required to learn about their target's vulnerabilities. Finally, the attack demonstrated that Russia could execute highly synchronised, multistage and multisite attacks. Importantly, by disrupting infrastructure through cyber means, the attack illustrates that Russia is willing to expand the scope of its cyber operations to achieve effects in the *'real'* world,[20] and not just effects in the digital realm.

In April 2022, the Irish Government developed a strategy it termed the *National Energy Security Framework* in response to concerns about energy shocks following the war in Ukraine. Though the Framework does mention the risks of cyberattacks on energy infrastructure, at the time, such a scenario was deemed unlikely.[21] However, the situation

[15] Clarke 2020: 15 Russian Hybrid Warfare: Military Learning and the Future of War Series. Institute for the Study of War. Available at: https://understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

[16] Jonsson 2020: 1 Preparing for Greyzone Threats to the Energy Sector. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/preparing-greyzone-threats-energy-sector

[17] Jonsson 2020: 7 Preparing for Greyzone Threats to the Energy Sector. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/preparing-greyzone-threats-energy-sector

[18] Leigher 2021 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

[19] Leigher 2021 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

[20] Kristiansen and Hoem 2021 Russian Cyber Strategy. Small Wars Journal. Available at: https://smallwarsjournal.com/jrnl/art/russian-cyber-strategy#_edn87

[21] Department of the Environment, Climate and Communications 2022: 26 National Energy Security Framework. Available at: https://www.gov.ie/en/publication/ea9e4-national-energy-security-framework/

has continued to escalate as the Kremlin has increasingly threatened to attack critical infrastructure in the West. Commenting on the Nordstream sabotage, which, to date, has not been officially attributed to any state or actor, Vladimir Putin stated that 'any critical infrastructure in transport, energy or communication infrastructure is under threat — regardless of what part of the world it is located, by whom it is controlled, laid on the seabed or on land'.[22] As a result, continued escalation and cyber-attacks on the energy grids of Western-aligned countries like Ireland should not be ruled out.

## V. The Critical Entities Resilience (CER) Directive: Moving in the Right Direction

On 16 January 2023, the EU's CER directive came into force, which creates obligations for Irish policymakers to ensure that Critical Entities (CEs) in Ireland, such as energy grid infrastructure, are sufficiently protected from disruption by hostile state actors.[23] This directive is intended to ensure that critical entities are receiving sufficient government support to equip them for the present 'dynamic threat landscape', a threat picture which includes the emerging hybrid and cyber threats discussed previously in this paper.[24] The CER Directive operates alongside the EU's Network's Information Security 2 (NIS2) Directive, which has also come into force since 16 January 2023, and focuses on Cybersecurity in EU Member States.[25]

The CER Directive creates obligations for the Irish State in how it approaches the resilience of its Critical Infrastructure. Though not an exhaustive list of the requirements set out in the Directive, this paper will explore how the State could potentially augment some of the requirements of the Directive by integrating elements of Sweden's Total Defence model to enhance the resilience of the State's energy infrastructure.

Among the two flagship elements of this directive is the requirement for the Irish State to conduct a risk assessment of potential threats to the operation of CEs, such as electricity provision, by January 2026.[26] This risk assessment will be conducted at least every four years and will examine the threats posed by natural disasters, public health emergencies, and, most importantly for this paper, hybrid or other antagonistic threats to Critical Infrastructure in Member State jurisdictions. Similarly, CEs themselves will have to conduct risk assessments 'to assess all relevant risks that could disrupt the provision of their essential services'[27] while accounting for the same threats listed above.

[22] Charlie Cooper 12 October 2022 Putin threatens Europe again as Brussels braces for winter. Politico. Available at: https://www.politico.eu/article/eu-energy-crisis-package-gas-gazprom-putin-vladimir-alexey-miller-winter-kadri-simson/

[23] See European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-1

[24] See article 3 European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-

[25] See article 30. European Council 14 December 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available at: https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1676386256093&from=en

[26] See II.5.1 See European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-1

[27] See III.12.1 See European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-1

The second important element of the Directive is the required development of a strategy for CE resilience, which must be adopted by 2026. The State is obliged to publish an outline of how it intends to enhance the overall resilience of critical entities, an account of the CEs in the state and how they were identified, a list of the main authorities and stakeholders involved in the implementation of the strategy, a policy framework for the coordination of information sharing among CEs, and a list of the threats posed to CEs. This strategy will be updated at least every four years.[28]

Finally, the Directive will oblige the state to support CEs in enhancing resilience. This support can range from facilitating information sharing between CEs; developing guidance materials for prevention of disruptions and methodologies for crisis management; supporting exercises to test resilience and, where justified by public interest, providing financial support.

The importance of the CER Directive for this paper is that it has now set a minimum standard for how Ireland can approach the resilience of critical entities within its jurisdiction. However, the CER Directive sees hybrid and cyberthreats from antagonistic state and non-state actors as one threat among many, and much of the approach is focused on either facilitating cooperation between the State and CE's or by facilitating cooperation amongst critical entities themselves.

Though it should be noted that the recommendations of this paper need not be limited to the CER Directive implementation process, the CER Directive provides a prime opportunity for Ireland to augment the security of CEs and the security of Irish society through examining best practices from other similar sized EU Member States such as Sweden's whole-of-society model of Total Defence.

## VI. Total Defence: A model for Ireland?

Turning to how Ireland can augment its ability protect itself though a whole-of-society approach, this paper bases its recommendations on Sweden's *Totalförsvaret* (Total Defence) model. Published in 2020, Sweden's Total Defence programme works to enhance the basic robustness of society which is instrumental in enabling it to withstand peacetime crises and contribute to deterring future attacks.[29] Sweden's Total Defence Concept has already been noted as a potentially 'useful reference for Ireland'[30] by Senior Members of the Irish Defence Forces. As a similarly sized 'small-state'[31] which, when the Concept was published, was also a European neutral state, Sweden's Total Defence Concept provides an imitable template which can be drawn upon to augment existing directives and legislation designed to protect Ireland's Critical Infrastructure. What the Total Defence document highlights is that varying means, in peacetime, in heightened alert and ultimately in wartime, can be used by hostile states to 'deliberately disrupt the functionality

[28] See I.4.1 and I.4.2 European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-1

[29] Swedish Ministry of Defence 2020: 3 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[30] Cudmore 2020: 22. Integrating our National Security and Defence Capabilities: A More Comprehensive Response to Evolving Challenges. Defence Forces Review 2020. Available at: https://www.military.ie/en/public-information/publications/defence-forces-review/review-2020.pdfhttps://www.military.ie/en/public-information/publications/defence-forces-review/review-2020.pdf

[31] McGourty 2020: 18 Irish Defence Planning and its Guiding Strategy in a Changing Strategic Environment. Defence Forces Review 2020. Available at: https://www.military.ie/en/public-information/publications/defence-forces-review/review-2020.pdf

of societies or influence public opinion, decisionmakers and democratic process'[32] and that the best way to counter these threats is by a whole-of-society approach to protecting the state and society. In short, the coordination of resources and capabilities which Total Defence concepts such as Sweden's provide are a force multiplier which can, against certain threats, enable the State to address larger threats which it may not be able to do using only the resources traditionally available to the government in the form of its security services. In this model, the Riksdag (Sweden's Parliament), the Government, public authorities including county administrative boards, municipalities and regions, industry and NGOs, as well as individual citizens, are all part of, and are expected to contribute to, Total Defence.[33] The capabilities of Total Defence are created by these actors working in concert, are enhanced through cooperation with other states and international organisations, and work to strengthen society's capacity to prevent and address extraordinary events in peacetime such as a mass cyber-attack against critical infrastructure.[34] Indeed, in this complex threat landscape, the Swedish government now deems it necessary for the private sector to increasingly 'include hybrid threat perspectives in their planning.'[35]

What lessons can Ireland draw from this strategy? Drawing on the Total Defence model, this paper proposes the below six recommendations for consideration.

## Recommendation 1: Ireland could enhance its resilience through greater cooperation between the public and private sectors

To enhance Ireland's security position, the state can boost partnerships with the private sector to boost national resilience to attacks against the energy sector. The societal and systemic resilience of the national energy infrastructure can play a role in deterring antagonistic behaviour by raising the stakes for any hostile actor and by increasing the risks of detection and attribution, thereby changing the cost/benefit calculus of any aggressor. However, the responsibility for defending Irish society and the energy grid from attack cannot be the sole responsibility of energy providers. In Ireland, the State is either the sole owner or majority stakeholder of the two largest operators of Ireland's energy system. Eirgrid manages the operation of the Irish electricity grid and is a fully state-owned company. The Electricity Supply Board (ESB) manage the generation, transmission, distribution, and supply of electricity within the State and is 95% owned by the state with the remaining 5% held by its employees. While companies such as ESB and Eirgrid have an important role to play in protecting their customers and wider society from supply disruption, the pursuit of national security cannot be driven by these energy market actors alone and will require collaboration between the State , electricity market actors, and private sector companies such as firms who specialise in cybersecurity.

From the perspective of the private sector, cybersecurity risks are often approached from a business risk perspective which works to prevent disruption to customers and not necessarily to defend against state-sponsored attacks. As illustrated by the NotPetya attack,

[32] Swedish Ministry of Defence 2020: 51 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[33] Swedish Ministry of Defence 2020:81 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[34] Swedish Ministry of Defence 2020:81 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[35] Swedish Ministry of Defence 2020: 152 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

this can still leave firms vulnerable to the consequences of cyberwarfare despite good cyber governance practices. Government will have to work to protect itself, private companies, and energy market actors from the consequences of proliferating cyberwarfare practices. To ensure energy market actors and private companies receive the support required to protect them from hostile state sponsored cyberattacks, the Government should cultivate a confidential information-sharing ecosystem including government agencies, private sector companies such as cybersecurity firms, and energy companies. Foremost among the issues facing Government when it comes to defending against cyber threats is the State's sometimes limited access to relevant data. When cyberattacks occur against private companies, incident response and reporting data collected by cybersecurity or insurance companies is often proprietary and not publicly reported.[36] This disparity in the information between the private sector and the public sector has been termed the 'Cyber Security Data Gap'.[37] Bridging this gap presents an important opportunity to enhance state resilience against cyberthreats. Though, under the Network and Information Systems (NIS) directive, operators in the energy sector must report cybersecurity incidents,[38] this still only provides a partial image of the threat environment as many industries in the private sector have no such obligation. Since Government agencies tend to possess advantages when researching cyber threats, including: the ability to conduct active cyber espionage operations against adversary networks as well as the capacity to make use of human intelligence sources, such entities have unparalleled insights into the threats facing different states.[39] Conversely, industry actors have detailed insights into victim networks, with some leading cyber security companies operating on all continents potentially providing a global vantage point.[40] 'This disparity in the information between the private sector and the public sector has been termed...'

A key step which could be taken would be to promote information-sharing of cyber incidents while protecting confidentiality, and a regularisation of cyber incident reporting to the National Cyber Security Centre (NCSC) which at present relies on victims of cyberattacks reaching out on an incident-by-incident basis when they may be of a 'national impact.'[41] Greater information-sharing not solely by energy market actors, but by the wider private sector including cybersecurity companies, would enhance the information environment for both the State and private sector companies, providing a mutually beneficial framework, which would enhance Irish society's resilience to cyber threats.

## Recommendation 2: Build awareness in critical industries about cyber risks to operational technology and their role in national security

As part of enhancing partnerships between the State and industry, the Irish Government should focus on building awareness within private industry about the risks that state-backed cyberattacks can pose to both business interests and to national security. Gov-

[36] Shore 18 October 2022 Data Incoming: How to Close the Cyber Data Gap. War on the Rocks. Available at: https://warontherocks.com/2022/10/data-incoming-how-to-close-the-cyber-data-gap/

[37] Shore 18 October 2022 Data Incoming: How to Close the Cyber Data Gap. War on the Rocks. Available at: https://warontherocks.com/2022/10/data-incoming-how-to-close-the-cyber-data-gap/

[38] NCSC 2019: 25 National Cyber Security Strategy. Available at: https://www.gov.ie/en/publication/8994a-national-cyber-security-strategy/

[39] Collier 2021 Optimising Cyber Security Public-Private Partnerships. Available at: https://rusi.org/explore-our-research/publications/commentary/optimising-cyber-security-public-private-partnerships

[40] Collier 2021 Optimising Cyber Security Public-Private Partnerships. Available at: https://rusi.org/explore-our-research/publications/commentary/optimising-cyber-security-public-private-partnerships

[41] NCSC. Incident Reporting. National Cyber Security Centre. Available at: https://www.ncsc.gov.ie/incidentreporting/

ernment Departments and agencies responsible for national security and defence can address the vulnerabilities of critical infrastructure by working to increase awareness of potential vulnerabilities in specific sectors, and by also raising awareness of the strategies and habits of hostile geopolitical actors, rather than purely by focusing on the principles of crisis management.[42] Moreover, as knowledge and awareness are an important part of modern deterrence,[43] the Government can promote awareness among industry actors that risks to business activities have national security implications which geopolitical actors may seek to exploit.

To build awareness regarding responsibilities and risks facing critical infrastructure, Sweden, as part of its Total Defence initiative, established a 'national commerce and business council', a council which included private businesses, industry associations and government agencies,  to create long term interaction between public and private actors at central, regional, and local levels to help to enable actors from industry to provide for the needs of national security.[44] As part of this council, Sweden has emphasised the role that private sector critical infrastructure operators such as those in Ireland's energy system have to play in the Total Defence framework.[45] The fact that the Irish Government remains a key actor in Ireland's energy market will enhance the ability of the Government to coordinate among key stakeholder companies within Ireland's energy system.

## Recommendation 3: Enhance the resilience of Ireland's electricity grid through greater redundancy and micro-generation programmes

Though information sharing and awareness are important in defending against antagonistic cyber threats to the energy grid, Ireland will also have to enhance the resilience of its electricity infrastructure against shocks by creating greater redundancy in the national grid as well as by exploring the role micro-generation can have in enhancing societal resilience to outages caused by antagonistic cyber behaviour. Though these might appear more costly and drawn-out compared to previous recommendations, Sweden's Model of Total Defence has highlighted how increasing redundancy and capacity in the national grid are key components of creating a physically resilient electricity system which can minimise the societal impacts of outages, deter antagonistic cyber activity, and enhance national security.[46]

Likewise, the vulnerability of the national grid to cyber disruption means that there is a need to create better conditions for the local production and distribution of electricity.[47] Programmes which already exist to encourage microgeneration should be considered in

[42] Jonsson 2020: 25 Preparing for Grey zone: Threats to the Energy Sector. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/preparing-greyzone-threats-energy-sector

[43] Jonsson 2020: 27 Preparing for Greyzone Threats to the Energy Sector. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/preparing-greyzone-threats-energy-sector

[44] Swedish Ministry of Defence 2020: 181 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[45] See Swedish Ministry of Defence 2020: 162 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf; and Swedish Ministry of Defence 2020:81  Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[46] Swedish Ministry of Defence 2020: 82 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[47] Swedish Ministry of Defence 2020: 167 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

a national security context. In this view, Ireland's Microgeneration Support Scheme, which provides up to €2,400 for households to install solar panels[48], should be expanded. Not only would this assist the State in meeting its climate targets, but it would also enhance the State's resilience to outages which may arise from a cyber-attack against the national grid.

## Recommendation 4: The Development of a Threat Lead Penetration Testing Framework, modelled on the existing TIBER-EU/IE Framework, should be considered for operators in Ireland's energy system

As part of a project to enhance the resilience of the energy system, the Irish Government could encourage the inclusion of a Threat Lead Penetration Testing (TLPT) Framework, such as the already existing Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU/IE) testing framework for operators in Ireland's energy system. This sector-agnostic framework, developed by the European Central Bank and national central banks, is designed to deliver a controlled, bespoke, 'intelligence-led Red Team test' of institutions' critical live production systems.[49] Intelligence-led Red Team tests mimic the tactics, techniques and procedures (TTPs) of real life threat actors, who on the basis of threat intelligence are perceived as posing a genuine threat. Such a test would enable operators in Ireland's energy system to identify their strengths and weaknesses, enabling them to reach a higher level of cyber maturity. It would also provide important insights into the readiness of Ireland's energy sector to address crises arising from cyber-attacks, while simultaneously providing important data which could be shared with other EU Member States.

## Recommendation 5: Ireland should develop its intelligence capacities to counter cyber threats

The Irish Government should both clarify the legal role of its foreign intelligence capability in the Defence Forces and enhance investment in its foreign intelligence capabilities in order to develop greater situational awareness about the present security environment. Good situational awareness is a pre-requisite  to be able to act proactively and to introduce appropriate measures in the event of a security crisis such as a cyber-attack against the energy grid.[50] In line with the recommendations of the Report of the Commission on the Defence Forces, the present lack of clarity in terms of the roles and responsibilities of Ireland's Military Intelligence is not in line with comparator counties.[51] In order to optimise the State's ability to anticipate threats and respond to crises, the State should further seek to invest in the intelligence capabilities of the national security services, such as Military Intelligence within the Defence Forces and An Garda Síochána's Security and Intelligence Section. Government should also clarify the role of the State as part of a 'coherent national

[48] Government of Ireland 2022: 61 National Energy Security Framework. Department of the Environment, Climate and Communications. Available at: https://www.gov.ie/en/publication/ea9e4-national-energy-security-framework/

[49] Aho, Midoes, and Snore 2020: 19 Hybrid Threats in the Financial System. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf#:~:text=Like%20hybrid%20threats%20in%20general%2C%20hybrid%20threats%20emerging,and%20cascading%20effects%20in%20all%20parts%20of%20society.

[50] Swedish Ministry of Defence 2020:173/4 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[51] Commission on the Defence Forces 2022: vii Report of the Commission on the Defence Forces. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

intelligence architecture' underpinned by appropriate legislation.[52]

Ireland may be able to amplify its intelligence capacities through continued cooperation with an expanded EU Intelligence and Situation Centre (INTCEN) which is a part of the European External Action Service (EEAS) – the EU's Diplomatic service. As part of its Strategic Compass,[53] the Council of the European Union has proposed that the Union as a whole works to build its intelligence capacities with a specific focus on hybrid and cyber threats.[54]

Though beyond the scope of this paper, the all-island nature of Ireland's energy grid should also be considered within this context. Since an attack on the energy grid in the Republic of Ireland may cause outages to those living in Northern Ireland, this may create opportunities for collaboration and intelligence sharing between the governments in Dublin and Westminster in countering hybrid threats to critical infrastructure.

Situational awareness and strategic foresight, as enablers of good and rapid decision making, will contribute to the overall deterrence of antagonistic cyber behaviour.[55] A key part of this could also be the introduction of defence attachés from the Irish Defence Forces distributed throughout Ireland's network of embassies in line with the recommendations of the Commission on the Defence Forces.[56] This would foster greater cooperation with partner armed forces and might facilitate greater information sharing which would enhance the State's ability to anticipate threats and respond to them. Consequently, greater investment in national intelligence capacities will both increase the resilience of the State to attacks against critical infrastructure such as against the energy grid while also potentially reducing the likelihood of an attack occurring in the first place.

### Recommendation 6: The Irish Government should examine the implications of the development of offensive cyber for defensive purposes to increase costs for perpetrators of cyber-attacks against critical infrastructure operators

Though increased awareness and cooperation between the public and private sectors may enhance readiness and resilience to threats, it has become clear that 'cyber defences such as passwords, firewalls, monitoring and patching security bugs in software are not in themselves sufficient'[57] to address the threat of state-backed antagonistic cyber behaviour. Ireland should consider how it can meaningfully deter antagonistic behaviour by imposing costs while responsibly managing escalation.'[58]

The responsibility for developing and managing these capabilities would likely be required to reside within a Joint Cyber Defence Command section of the Irish Defence

[52] Commission on the Defence Forces 2022: 62 Report of the Commission on the Defence Forces. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

[53] For a summary of the EU's Strategic Compass, see FitzGerald C. 2022 The Cost of Passivity: Can the Strategic Compass Guide the EU in an Era of Insecurity. IIEA. Available at: https://www.iiea.com/blog/the-cost-of-passivity-can-the-strategic-compass-guide-the-eu-in-an-era-of-insecurity

[54] Council of the European Union 2022: 3 A Strategic Compass for Security and Defence. Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[55] Swedish Ministry of Defence 2020:173/4 Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

[56] Commission on the Defence Forces 2022: 10 Report of the Commission on the Defence Forces. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

[57] Leigher 2021: 14 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

[58] Leigher 2021: 14 Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

Forces whose establishment was proposed by the Commission on the Defence Forces in its report.[59] The overall mission for this command would be to conduct *'full spectrum cyberspace operations for defensive purposes (up to limited offensive and strategic reconnaissance capability) in line with national policy guidelines'* to support the security of the State.[60] Developing even these limited cyber capabilities for defensive purposes could enable Ireland to change the calculus of potential perpetrators of antagonistic cyber activity and to potentially deter such activity altogether.

## VII. Conclusion: All Swans are White, Until They are Not

The present geopolitical environment poses clear and direct dangers to Ireland. Hostile actors, most notably the Russian Federation, have illustrated a willingness and capacity to attack the energy systems of other states. Ireland, as a member of the EU, as a participating member in the EU Military Assistance Mission to train Ukrainian troops,[61] and as a state with a comparatively underdeveloped security apparatus relative to other EU countries, is clearly vulnerable in this environment.[62] A cyber-attack against Ireland's energy grid would still be a Black Swan event, that is to say, an event that is highly improbable but which would have a significant impact on Irish society should it occur. Given the increasing willingness of the Russian Federation to violate the norms of international law, Russia's targeted attacks against energy infrastructure in Ukraine, and its continued naked threats against infrastructure in Europe, the Irish Government should make appropriate preparations for such an attack happening here. The threat to Ireland's energy grid is a clear and present one, and it cannot be left to the energy companies alone to secure the state from a potential cyber-attack - originating from Russia or anywhere else.

Ultimately, as the current geopolitical moment of competition creates an ever more dangerous environment for small countries like Ireland, the State should focus on how it can protect itself and its citizens not only from armed attacks, but also from non-kinetic attacks against civilian infrastructure and society as a whole. In this environment, no one group alone can protect the State. The Government, energy market actors, the private sector, and Irish society as a whole need to be full participants in the maintenance of Ireland's national security. In a world where societies are targeted to undermine states, it is the strength and collaboration of the whole of society that will provide the State with the best protection from foreign aggression arising from both state and non-state actors.

[59] Commission on the Defence Forces 2022: 57 Report of the Commission on the Defence Forces. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

[60] Commission on the Defence Forces 2022: 58 Report of the Commission on the Defence Forces. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

[61] FitzGerald 2022 Will the Stars Align? What the Creation of an EU Military Assistance Mission for Ukraine May Mean for Ireland. IIEA. Available at: https://www.iiea.com/blog/will-the-stars-align-what-the-creation-of-an-eu-military-assistance-mission-for-ukraine-may-mean-for-ireland

[62] Commission on the Defence Forces 2022: 28 Report of the Commission on the Defence Forces. Available at: https://www.military.ie/en/public-information/publications/report-of-the-commission-on-defence-forces/report-of-the-commission-on-defence-forces.pdf

## VIII. Bibliography[63]

Aho, Midoes and Snore 2020 *Hybrid Threats in the Financial System*. Hybrid COE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf

Brown, Richard 30 March 2022. Oireachtas Hearing: *Cybersecurity and Hybrid Threats Following the Russian Invasion of Ukraine: Discussion.* Oireachtas.
Available at: https://debatesarchive.oireachtas.ie/debates%20authoring/debateswebpack.nsf/committeetakes/TTJ2022033000002#N02300

Cooper 12 October 2022 *Putin threatens Europe again as Brussels braces for winter*. Politico. Available at:https://www.politico.eu/article/eu-energy-crisis-package-gas-gazprom-putin-vladimir-alexey-miller-winter-kadri-simson/

Clarke 2020 *Russian Hybrid Warfare: Military Learning and the Future of War Series.* Institute for the Study of War. Available at: https://www.understandingwar.org/military-learning-and-future-war-project#anchor6

Collier 2021 *Optimising Cyber Security Public-Private Partnerships.* Available at: https://rusi.org/explore-our-research/publications/commentary/optimising-cyber-security-public-private-partnerships

Commission on the Defence Forces 2022 *Report of the Commission on the Defence Forces*. Available at: https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/

Council of the European Union 2022 *A Strategic Compass for Security and Defence. Council of the European Union*. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

Cudmore 2020 *Integrating our National Security and Defence Capabilities: A More Comprehensive Response to Evolving Challenges.* Defence Forces Review 2020. Available at: https://www.military.ie/en/public-information/publications/defence-forces-review/review-2020.pdf

European Council 14 December 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) European Council 14 December 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557&from=EN#d1e911-164-1

Fiott and Parkes 2019 *Protecting Europe: The EU's Response to Hybrid Threats.* Challiot Paper 151 April 2019. EUISS. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

FitzGerald 2022 *Will the Stars Align? What the Creation of an EU Military Assistance Mission for Ukraine May Mean for Ireland.* IIEA. Available at: https://www.iiea.com/blog/will-the-stars-align-what-the-creation-of-an-eu-military-assistance-mission-for-ukraine-may-mean-for-ireland

Government of Ireland 2022 *National Energy Security Framework. Department of the Environment, Climate and Communications.* Available at: https://www.gov.ie/en/publication/ea9e4-national-energy-security-framework/

[63] All links valid as of 18 April 2023

Jonsson 2020 *Preparing for Greyzone Threats to the Energy Sector*. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/preparing-greyzone-threats-energy-sector

Kristiansen and Hoem 2021 *Russian Cyber Strategy.* Small Wars Journal. Available at: https://smallwarsjournal.com/jrnl/art/russian-cyber-strategy#_edn87

Leigher 2021 *Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts*. Hybrid COE. Available at: https://www.hybridcoe.fi/publications/hybrid-coe-paper-10-cyber-conflict-in-a-hybrid-threat-environment-death-by-a-thousand-cuts/

Limnell 2018 *Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed.* Hybrid COE. Available at: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-6-countering-hybrid-threats-role-of-private-sector-increasingly-important-shared-responsibility-needed/

Mazzar 2015 *Mastering the Grey Zone.* US Army War College

McGourty 2020 *Irish Defence Planning and its Guiding Strategy in a Changing Strategic Environment.* Defence Forces Review 2020. Available at: https://www.military.ie/en/public-information/publications/defence-forces-review/review-2020.pdf

NATO Cooperative Cyber Defence Centre of Excellence 2022 *NotPetya* (2017). CCCDOE. Available at: https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)

NCSC 2019 *National Cyber Security Strategy.* Available at: https://www.ncsc.gov.ie/strategy/

O'Sullivan 30 June 2022. *Ireland will need to develop a new vocabulary to talk about national security.* Irish Times. Available at: https://www.irishtimes.com/opinion/2022/06/30/ireland-will-need-to-develop-a-new-vocabulary-to-talk-about-national-security/

Shore 18 October 2022 *Data Incoming: How to Close the Cyber Data Gap.* War on the Rocks. Available at: https://warontherocks.com/2022/10/data-incoming-how-to-close-the-cyber-data-gap/

Swedish Ministry of Defence 2020 Summary of Government bill *'Totalförsvaret 2021–2025'* (Total defence 2021–2025). Available at: https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

Taleb 2001 *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*. Random House

Taleb 2007 *The Black Swan: The Impact of the Highly Improbable*. Random House

The Institute of International and European Affairs (IIEA) is Ireland's leading international affairs think tank. Founded in 1991, its mission is to foster and shape political, policy and public discourse in order to broaden awareness of international and European issues in Ireland and contribute to more informed strategic decisions by political, business and civil society leaders.

The IIEA is independent of government and all political parties and is a not-for profit organisation with charitable status. In January 2021, the Global Go To Think Tank Index ranked the IIEA as Ireland's top think tank.

The IIEA acknowledges the support of the Citizens, Equality, Rights and Values (CERV) Programme of the European Union

IIEA

Sharing Ideas
Shaping Policy