

Secure Connections: Ireland's Digital Infrastructure and the Resilience of European Connectivity

Cian FitzGerald
Barry Colfer



Acknowledgements

The authors of this paper would like to acknowledge the contributions made by Ava Sydell, Lyndsay Rowlands, and David O'Grady who supported this project. The authors also wish to thank the roundtable participants who gave so generously of their time and the thinkers and colleagues who read and discussed early drafts of this work.

About the Authors

Cian FitzGerald (Principal Investigator) is a Senior Researcher specialising in Defence and Security, as well as Foreign Policy analysis. He is a leading Irish expert on whole-of-society approaches to national security, and the role of the private sector in defence. His research interests include geostrategic competition with a specific focus on irregular and hybrid warfare. Additionally, he works on developments in EU Common Security and Defence Policy (EU CSDP), and matters pertaining to Ireland's national security.

Cian has appeared before the Joint Oireachtas Committee on Foreign Affairs and Defence to provide evidence on Russian cyber and hybrid warfare operations and how they threaten critical national infrastructure. His research has featured in both Irish national and international media including Al-Jazeera, RTE, the Irish Examiner, and the Irish Times.

Barry Colfer PhD is the IIEA's Director of Research. Barry holds a Ph.D. and M.Phil from the Department of Politics and International Studies (POLIS) at the University of Cambridge. Prior to joining the IIEA, Barry was a Max Weber Fellow at EUI Florence and he previously held postdoctoral fellowships at the University of Oxford, Harvard University, and the Politecnico di Torino in Italy.

Barry has worked at both the Irish and European Parliaments as well as with a number of leading European think tanks. Barry's research interests include the politics of European integration, the future of work, and British-Irish relations.

Table of contents

1. Introduction: ‘Resilience is Symbiotic’ 8

2. Essential yet exposed: Ireland’s defence limitations and their implications for European digital connectivity. 9

3. Putting the Pieces Together: Ireland and Systemic Risks to European Telecommunications Infrastructure..... 11

4. ‘The costs have to fall somewhere’: Resilience, Regulation, and Permitting 14

5. Recommendations: Building a Resilient Telecommunications System through a Whole-of-Society Approach..... 17

6. Conclusion: ‘When we work together, it works’ 21

7. Bibliography..... 23

Foreword from Sabrina Casalta, CEO, Vodafone Ireland

Connectivity sits at the heart of modern life. It powers our economies, supports public services, enables innovation and helps keep communities connected. As our dependence on digital infrastructure continues to grow, so too does the importance of ensuring that the networks that underpin them are secure, resilient and future-ready.

Vodafone brings a unique perspective to this discussion. Every day, Vodafone connects more than 300 million customers and businesses across Europe and Africa, supporting critical communications and digital services at scale. That experience gives us a deep understanding of both the opportunities digital connectivity creates, and the responsibility involved in securing and maintaining the infrastructure on which societies increasingly rely.

Here in Ireland, Vodafone has been part of that journey for 25 years. As Ireland's longest-serving mobile telecommunications provider, we have invested more than €20 billion in the country over that period, helping to build and strengthen the connectivity infrastructure that supports consumers, businesses, communities and public services nationwide. We remain committed to continuing that investment as Ireland's digital ambitions evolve.

However, delivering resilient, reliable connectivity requires a policy and regulatory environment that provides certainty for sustainable long-term investment. The decisions taken today will shape Ireland's ability to compete, innovate and prosper in an increasingly digital world over the next decade and beyond.

I would like to thank the Institute of International and European Affairs for its leadership in convening this important discussion, and all those who contributed their expertise and insights.

We hope this report helps inform the conversation on how best to strengthen and secure Ireland's digital future.

Sabrina Casalta
CEO, Vodafone Ireland

Foreword from Dr Orlaigh Quinn, Interim Director General of the Institute of International and European Affairs

Telecommunications infrastructure is critical for the functioning of Ireland's economy and society. Communications infrastructure, including subsea cables, data centres, and space-based communications, ensures that people in Ireland can communicate with each other and with the world. It supports business across the island, underpins essential public services, and connects Ireland to European and global markets.

Ireland's role in this ecosystem is significant. Ireland's role as a small open economy and as a major hub for digital connectivity means that the country depends on secure and resilient telecommunications infrastructure to sustain its prosperity and competitiveness. Yet, this infrastructure is not only Irish infrastructure. The digital infrastructure located in and around Ireland forms part of the wider European digital environment. Subsea cables landing in Ireland, data centres operating in the country, and the networks that connect them simultaneously contribute to Europe's resilience and strategic autonomy.

Yet, against the backdrop of a deteriorating security environment, such infrastructure is now increasingly seen as a preferred target during times of conflict, crisis, or geopolitical competition. Recent events have demonstrated these risks. In the Middle East, attacks on data centres have shown how digital infrastructure can become a target during conflict, with often major consequences for civilian populations. Around Europe, subsea and terrestrial data cables have been subject to sabotage and disruption.

This paper, *Secure Connections: Ireland's Digital Infrastructure and the Resilience of European Connectivity*, focuses on these challenges. It considers Ireland's role in European telecommunications, the risks posed by a more volatile geopolitical environment, and the practical steps required to build resilience. It highlights an important fact: neither Government nor industry can meet these risks alone.

We are delighted to have had the opportunity to partner with Vodafone on this important project. Through this collaboration, we have sought to identify practical steps that can be taken to ensure that Europe and Ireland can develop a resilient and robust telecommunications system that can meet the needs of citizens and the challenges of a more dangerous world.

The Institute of International and European Affairs (IIEA) is Ireland's leading international affairs and public policy think-tank. Through our programme of events, research, and publications, we provide a unique space for honest and open discussion on the challenges facing Ireland, Europe, and the wider world. Our work seeks to support evidence-based policymaking and to assist in identifying the choices available to decision-makers as they respond to the growing challenges that have come to define our ever more volatile world.

Dr Orlaigh Quinn,
Interim Director General, IIEA

Executive Summary

Telecommunications and digital infrastructure play an essential role in Ireland's economy, society, and connectivity. Terrestrial networks, subsea cables, data centres, cloud infrastructure, radio spectrum, and satellite systems enable the functioning of our financial services, technology ecosystem, and pharmaceutical and medtech sectors, as well as government services such as healthcare, policing, and defence both during crises and day-to-day.

This paper argues that Ireland's digital infrastructure is essential to Ireland's national and economic security, as well as to Europe's overall resilience. It notes that a large proportion of the transatlantic data cables pass through or near Ireland, and that the State hosts a substantial share of Europe's data-centre infrastructure. In this context, digital infrastructure located in Ireland not only supports Irish society and businesses, but also the wider European digital ecosystem. Any serious incident or disruption in or around Ireland could have disproportionate consequences not just on the Island, but throughout the continent, with potentially major implications for transatlantic data flows and connectivity. The impact of this for economic activity and society, as well as for Ireland's credibility as a major venue for tech investment and activity, could be highly consequential.

Telecommunications infrastructure has increasingly become a target in the ever more volatile global security environment. In Europe, reports of suspicious activity around telecommunications infrastructure such as cables has increased, as well as concerns of sabotage by state actors including the Russian Federation. In the Middle East, the deliberate targeting of data centres has demonstrated that attacks against such infrastructure can lead to real world consequences for civilians, including losing access to banking services.

Drawing on a series of roundtables that the IIEA convened which brought together high-level representatives from Government, academia, and the private sector, this paper highlights that protecting this infrastructure, and increasing its resilience, in a more dangerous world will need to be a joint effort involving the State and industry. No single actor will be able to manage the full range of risks alone. This new environment and the scale of it also creates challenges around how responsibility, costs, and risk should be allocated, which this paper seeks to explore and analyse.

The paper examines the growing quantity of regulations affecting the telecommunications sector designed to increase resilience and security, as well as the obstacles posed by delays in permitting of new projects. It argues that, while well-intentioned, the growing range of regulatory requirements has increased regulatory complexity and, in some instances, could discourage investment in new and ongoing projects, thereby ultimately reducing the overall resilience of European telecommunications.

The paper sets out seven recommendations for decision makers to consider relating to how to build a more resilient telecommunications system through a whole-of-society approach. First, Ireland should develop a clearer framework for balancing resilience responsibilities between the State and the private sector. Government should identify which costs can be borne by operators, and where government support is justified to protect Ireland's society and prosperity. A resilience tax credit, modelled on the Research and Development Corporation Tax Credit, could support private investment in resilience and security. Second, the Department of Culture, Communications, and Sport should provide greater long-term certainty on spectrum policy to enable industry to make long-term, sustainable investments in capability and resilience.

Third, the Government should expedite the creation of a national security clearance system to enable trusted and confidential sharing of information between industry and the State. This is particularly relevant in relation to geopolitical risks such as hostile state activity. Fourth, Government should augment existing trusted networks through regular joint exercises and crisis simulations. Such exercises would provide opportunities to identify risks and gaps in Ireland's security, as well as improve preparedness. They would simultaneously build peer-to-peer relationships between senior stakeholders and provide training which could enhance response times during crises.

Fifth, Government should increase institutional and regulatory capacity and capability, including through additional resourcing for key bodies such as MARA to manage an increasingly complex regulatory, technological, and risk landscape. Sixth, national security and societal resilience should be explicitly reflected in the proposed 'public interest test' for judicial review reform. Finally, Ireland should integrate space-based infrastructure into telecommunications resilience planning including through engagement with EU programmes such as 'IRIS2' (Infrastructure for Resilience, Interconnectivity and Security by Satellite).

1. Introduction: ‘Resilience is Symbiotic’

For telecommunications, Ireland is very exposed....The extent of disruption and threat is at a different scale than what the Irish system has had to deal with before.

- Roundtable Participant

Telecommunications, and the digital infrastructure which underpins it, are essential to the good functioning of Europe’s economy, prosperity, and society. In the context of Ireland, telecommunications infrastructure including terrestrial, subsea data cables, data centres, and satellite communications, enable the functioning of our financial services, technology ecosystem, pharmaceutical and medtech sectors, as well as government services such as healthcare, policing, and defence both during crises and day-to-day.

Yet, against the backdrop of an increasingly strained geopolitical environment, global telecommunications infrastructure has become ever more exposed. Suspected incidents of sabotage in Europe at sea and on land, as well as cyber-attacks and supply chain risks means that the infrastructure that support individuals’ daily lives and Ireland’s economy is facing the risk of potentially significant disruption. That the spectrum of threat vectors is increasing at a time when our societies are more dependant on telecommunications than ever means a serious incident would have cascading consequences throughout Irish society and economy.

This paper draws on a series of private roundtables¹ convened by the IIEA that brought together senior civil servants, as well as representatives from industry and academia. Across these discussions, among the areas of clear consensus is that Ireland’s telecommunications infrastructure is exposed to geopolitical risk, that the threat environment has become too complex for any one organisation to manage, and that industry and government will have to find innovative solutions to enhance dialogue and cooperation. Yet at the same time, while the perception of risk was broadly shared, Government and industry stakeholders had diverging views on the most appropriate possible solutions to these risks—something which dialogue and cooperation would assist in bridging.

This paper explores the role of Ireland’s digital infrastructure in the European telecommunications ecosystem. It explores the growing range of risks facing Ireland’s telecommunications and digital infrastructure including the growing risk of physical attack and sabotage, the risk of cyberattacks, as well as supply-chain vulnerabilities. The paper explores how to achieve greater alignment between Government and industry on the risks to the telecommunications infrastructure, and potential solutions to mitigate these threats. The paper examines the impact of regulation on resilience, as well as the cost of resilience. This paper also explores the impact of delays in permitting for the resilience of telecommunications infrastructure and how policymakers and industry can work together to build a more resilient telecommunications system that supports society and prosperity in Ireland and across Europe.

1. These roundtables were held under the Chatham House Rule on 30 April 2026 and 5 June 2026

2. Essential yet exposed: Ireland's defence limitations and their implications for European digital connectivity.

The threats are very real. Trillions come in through subsea cables... Ireland hosts much of the world's data and this means that Ireland is very exposed to the international threats that we see..

- Roundtable Participant

Ireland plays host to a large amount of infrastructure essential to Europe's digital connectivity. As one representative from a government organisation expressed, Ireland 'is a big player when it comes to digital infrastructure'. Yet, Ireland's disproportionate role in global connectivity can at times be underrepresented. In many ways, it is easier to argue that Ireland is an essential node in global data connectivity not only due to the large proportion of data centres in Ireland, but due to the fact that approximately 75% of all transatlantic cables pass through or near Ireland,² with approximately 95% of all internet data traveling through underwater cables worldwide.³ According to Ireland's 2019 National Cyber Security Strategy, Ireland plays host to approximately 30% of all EU data.⁴ Ireland's data centre infrastructure has continued to grow since then with 23% of Ireland's electricity generated in 2025 serving data centre infrastructure,⁵ with that figure expected to grow another 30% by 2030.⁶ Consequently, Ireland's outsized and essential role in Europe's data sovereignty and connectivity is likely to increase. According to a representative from industry, it is important that this infrastructure is not only seen as Irish infrastructure, but that this should be seen as a 'key part of Europe'.

While Ireland's importance in European telecommunications is increasing, the possibility of an attack on such infrastructure has also increased in likelihood. According to a report from the International Institute for Strategic Studies, Russian sabotage operations against European critical infrastructure increased by 246% from 2023 to 2024.⁷ The centrality of Irish telecommunications infrastructure means that this is not only a risk to Ireland, but could also lead to service outages and disruption throughout the European Union. Indeed, the 2022 Report of the Commission on the Defence Forces has highlighted a 'growing risk that Ireland's land, air, maritime, and cyber domain [could] become vectors of attacks on or threatening moves against Ireland's neighbours and European partners'.⁸ Significantly, the criticality of telecommunications to the provision of essential services such as healthcare, banking, and transport cumulatively mean that significant disruptions caused by malicious actors at sea or on land could lead to cascading consequences throughout Ireland, with significant implications for Ireland's social and economic vibrancy.

2. RTE 19 February 2025 *How many of world's undersea cables pass through Irish waters?* RTE. Available at: <https://www.rte.ie/news/2025/0219/1497714-irish-undersea-cables/>

3. Colin Wall and Pierre Morcos 11 June 2021 *Invisible and Vital: Undersea Cables and Transatlantic Security*. CSIS. Available at: <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>

4. National Cyber Security Centre 2019: 8 *National Cyber Security Strategy 2019 – 2024*. Available at: <https://assets.gov.ie/static/documents/national-cyber-security-strategy-2019-2024.pdf>

5. Central Statistics Office 7 July 2026 *Data Centres Metered Electricity Consumption 2025*. Available at: <https://www.cso.ie/en/releasesandpublications/ep/p-dcmec/datacentresmeteredelectricityconsumption2025/>

6. Caroline O'Doherty 9 June 2026 *Data centre electricity demand could exceed power usage of the republic*. The Irish Times. Available at: <https://www.irishtimes.com/politics/2026/06/09/data-centre-electricity-demand-could-exceed-power-usage-of-entire-country/>

7. Charlie Edwards and Nate Seidenstein 2025: 9 *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. IISS. Available at: <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian-sabotage-operations--against-europes-critical-infrastructure>

8. Commission on the Defence Forces 2022: 4 *Report of the Commission on the Defence Forces*. Available at: <https://assets.gov.ie/static/documents/report-of-the-commission-on-the-defence-forces.pdf>

Yet, there has been a growing focus on Ireland's limited capacity to protect and defend European telecommunications infrastructure from Irish and European policymakers. In particular, the threat to subsea telecommunications infrastructure, which ostensibly requires increased military capabilities to protect, is already well documented. While the 2024 National Risk Assessment highlights the risk of sabotage to telecommunications as a key hybrid threat to the Ireland,⁹ and the State has recently published its first ever Maritime Security Strategy, Ireland has historically ignored its maritime area and has not invested in the necessary capabilities to protect critical infrastructure in the maritime.¹⁰ This is occurring against the backdrop of increased Russian activity around subsea telecoms cables in the Atlantic from vessels such as the 'Yantar',¹¹ as well as suspected sabotage incidents in the Arctic and Baltic sea such as the 2022 Svalbard Cable damage¹² which caused disruption to a Svalbard Satellite Station, and the 2023 Balticconnector damage between Finland and Estonia.¹³

As of 2025, Ireland can only have two vessels actively operational at sea, largely due to shortages of personnel.¹⁴ Ireland claims a maritime zone up to 13 times the land mass of Ireland, with responsibility for almost a million square kilometres within its EEZ and territorial waters.¹⁵ While Ireland has announced significant investments in military radar and sonar, one representative from academia argued that these are 'not defensive technologies, they are sensing technologies'. While these technologies will assist in attribution of those responsible should there be a sabotage incident of a transatlantic data cable, these technologies do not prevent sabotage, and it is unclear as to whether Russians, or other geopolitical actors, care about attribution in the first place.

Importantly, it was observed by the roundtable, that while increasing military capabilities to protect such infrastructure is important, due to the nature of the risks to subsea telecoms cables, military responses often arrive after the fact, to an incident that can appear as an accident, and that there is simply too much ocean to cover in the first place. It was stressed throughout that redundancy will be an essential element in defending against the risks posed by hybrid activity, with one representative from industry noting that 'redundancy is resilience'.

Moreover, the changing geopolitical risk environment in the North Atlantic, with an increase in suspected incidents of state-backed sabotage in recent years, coupled with Ireland's documented maritime security limitations, could affect the insurability and viability of future subsea cable projects. Simultaneously, it is possible that sabotage may need to be included in risk-registers for future projects which may create barriers to new projects by making it more challenging to access private funding for future projects. Consequently, while potentially viewed as administrative by the State, such barriers to new projects could reduce systemic redundancy, and thereby impact the resilience of the European telecommunications system as a whole.

While documented, Ireland's exposure to geopolitical risk has radically changed in the years following Russia's full-scale invasion of Ukraine, at a time when the Country's importance in global telecommunications has grown exponentially. While policymakers are increasingly aware of the risks to critical telecommunications infrastructure, much of the emphasis has thus far been on the risks to subsea telecommunications cables and Ireland's current defence challenges in sufficiently being able to monitor, secure, and protect these critical assets. Ireland will need to invest more into ensuring that the subsea telecommunications cables are secured against geopolitical risk vectors. While important, this is only one piece of the telecommunications security puzzle. Europe faces a number of broader systemic risks to its telecommunications infrastructure that will need to be addressed.

9. Department of An Taoiseach 2024 *National Risk Assessment 2024 – Overview of Strategic Risks*. Available at: <https://assets.gov.ie/static/documents/national-risk-assessment-2024-overview-of-strategic-risks.pdf>

10. Mark Mellett 2024: 2 *What's Past is Prologue: Ireland's Security and Defence In a New European Context*. IIEA. Available at: <https://www.iiea.com/publications/whats-past-is-prologue-irelands-security-and-defence-in-a-new-european-context>

11. Conor Gallagher 19 November 2025 *Russian spy ship on course for Irish waters, with UK threatening 'military options'*. The Irish Times. Available at: <https://www.irishtimes.com/ireland/2025/11/19/russian-spy-ship-on-course-for-irish-waters-with-uk-threatening-military-options/>

12. Niels Nagelhus Schia, Lars Gjesvik and Ida Rødningen 2023 *The Subsea Cable Cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed*. NUPI. Available at: https://www.nupi.no/content/pdf_preview/26372/file/NUPI_Policy_Brief_1_23_Schia_Gjesvik_R%C3%B8dningen-FERDIG.pdf

13. Claudia Chiappa and Pierre Emmanuel Ngendakumana 1 December 2023 *'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says*. Politico. Available at: <https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/>

14. See House of the Oireachtas 8 May 2025 *Naval Service*. Available at: <https://www.oireachtas.ie/en/debates/question/2025-05-08/184/>; and BBC 24 August 2024 *Only two Irish Navy Ships available to go to sea*. Available at: <https://www.bbc.com/news/articles/cprwlpdv04lo>

15. Mark Mellett 2024: 2 *What's Past is Prologue: Ireland's Security and Defence In a New European Context*. IIEA. Available at: <https://www.iiea.com/publications/whats-past-is-prologue-irelands-security-and-defence-in-a-new-european-context>

3. Putting the Pieces Together: Ireland and Systemic Risks to European Telecommunications Infrastructure

**In a context of hybrid threats, we are
not at war, but we are not at peace.
The threat is different to any threat
that we have faced in the past.**

- Roundtable Participant

European telecommunications face a broad spectrum of strategic and operational risks which could impact the connectivity required for the essential functions of our society. The proliferation of hybrid threats such as sabotage risks and cyber-attacks mean that private telecommunications operators are at increased risk of attack from state or state-backed organisations. Meanwhile, supply chains and technological security are increasingly becoming instrumentalised as a means of securing geopolitical leverage. A representative with experience of cabinet expressed that ‘the stability and predictability, and drive for efficiencies that we had become accustomed to, that is really of yesterday’s world.’ Moreover, it was expressed by numerous representatives that risks to telecommunications infrastructure represent a broader social risk. One representative from the space sector observed the interconnected nature of data, energy, and infrastructure – noting that risks to one part of this triad, not only represent risks to the others, but also could cascade throughout Irish society, causing social and economic harm to the people who live there. Against this backdrop, profound and novel geopolitical risks will require a shift from government and private sector entities, with a need for greater cooperation, on how to ensure a resilient telecommunications system.

Kinetic Attack

Kinetic attack on critical telecommunications infrastructure featured prominently in the roundtable discussions. While there had been an acknowledgement that sabotage to subsea telecoms cables was a documented risk amongst roundtable participants, significant concerns were expressed at the growing risk to terrestrial telecoms infrastructure and to data centres. In particular, many of the representatives from industry and government expressed that the 2026 war in the Persian Gulf, which saw a number of drone strikes on the Gulf States emerging from Iran, as a watershed.

In March 2026, a number of Iranian Shahed-136 attack drones struck an Amazon Web Services data centre in the UAE, as well as other data centres in Bahrain. According to the Guardian, millions in the UAE were unable to pay for a taxi, order a food delivery, or check their bank balance on their mobile apps.¹⁶ One representative from industry noted that ‘the war in the Gulf has opened our eyes to where the targets are’, with a government representative expressing that ‘this is the first time that data centres have become identified in a war environment for people to attack’. Not only has this incident highlighted that data centres are now considered a valuable target in geopolitical contestation and that attacks on data centres can cause mass disruption to civilian populations when attacked, but this incident has also called into question whether the Gulf States may be able to build, and importantly defend, the data infrastructure it needs to be a part of the transformative effects of the AI revolution.¹⁷

While representatives at the roundtable noted that the Irish case was different and that the chances of a physical attack on data centre and terrestrial infrastructure of the kind seen in the Gulf was low, Ireland is still exposed to the

16. Daniel Boffey 7 March 2026 ‘it means missile defence on datacentres’: drone strikes raise doubts over Gulf as AI superpower. The Guardian. Available at: <https://www.theguardian.com/world/2026/mar/07/it-means-missile-defence-on-data-centres-drone-strikes-raises-doubts-over-gulf-as-ai-superpower>

17. See Daniel Boffey 7 March 2026 ‘it means missile defence on datacentres’: drone strikes raise doubts over Gulf as AI superpower. The Guardian. Available at: <https://www.theguardian.com/world/2026/mar/07/it-means-missile-defence-on-data-centres-drone-strikes-raises-doubts-over-gulf-as-ai-superpower>

same geopolitical forces and risks. In France, during its hosting of the Olympic Games in 2024, long distance land-based internet cables were cut,¹⁸ while there has been a growing number of arson attacks on 5G masts in the United Kingdom.¹⁹ Moreover, not only are these types of attacks on telecommunications growing in impact and frequency, the threshold for such attack was assessed at being quite low, with one roundtable participant from industry noting that anyone with ‘a homemade device is a risk and could attack this infrastructure.’ Of particular concern, will be the distributed and diverse range of potential risks to this infrastructure, ranging from lone wolf attackers to terrorist organisations, to foreign intelligence services, to – at the upper end of the risk curve – armed attacks.

Yet, Ireland’s ambitions to become a global player in AI infrastructure is exposed to geopolitical risk in this context. While Ireland’s telecommunications infrastructure is resilient, any attack on Ireland’s subsea data cables – even one which might cause minimal disruption to service, would have profound political consequences in Ireland. The known limitations in Ireland’s defence capabilities could see cable and data centre operators reduce their investments in Ireland if they consider their infrastructure to be at risk and unprotected in an increasingly volatile geopolitical context – instead choosing locations in Europe with greater defence capacities.

Supply Chain and Capacity Constraints

A key area of concern which was highlighted by representatives from industry and from Government were related to supply chain risks and capacity constraints within the telecommunications sector. In particular, representatives from Government and industry both agreed that dependencies on third countries such as the United States and China could pose potential issues for European telecommunications.

Participants from industry and government expressed that the growing dominance of a small number of hyperscalers,²⁰ such as Meta, Google, and AWS may impact the overall resilience of the sector. Likewise, the overreliance on US-based hyperscalers for the provision of cloud infrastructure was repeatedly expressed as a concern, with US hyperscalers responsible for 70-80% of cloud infrastructure, according to participants. Meanwhile concerns over Chinese 5G technology is well documented. The European Commission’s updated Cybersecurity Act (CSA2) would restrict access from some Chinese suppliers such as Huawei and ZTE to European telecommunications.²¹

Yet, how to approach the concerns of these dependencies and the role of digital sovereignty was a contested issue amongst participants. It was expressed by a representative from a government agency that ‘cybersecurity is being used as a backdoor for protectionism’ and that ‘Irish citizens deserve access to the best technologies’, while another representative from the technology sector cited concerns over the mass collection of data by third countries. While the matter was contested, there was a general consensus that Europe should ensure that it has access to diverse supply chains, that benefit its society, and that minimises dependencies and security risks.

The growth of AI infrastructure was raised as a physical risk to resilience. With up to 700bn USD of investment into data centres and chips expected by 2030,²² much of the world’s production capacity for fibre optics, memory, and chips are now being redirected towards AI, and away from other telecoms infrastructure. It was raised by a representative from industry involved in the telecoms supply chain that the ‘AI bubble has sucked up a lot of the spare capacity’, adding to additional costs and lead times for projects. Consequently, the redirection of supply chains away from telecommunications could degrade the resilience of the telecommunications system, make building additional redundancy too costly, and ultimately make repair more challenging due to supply chain bottlenecks.

18. Matt Burgess 29 July 2024 *Saboteurs Cut Internet Cables in Latest Disruption During Paris Olympics*. Wired. Available at: <https://www.wired.com/story/saboteurs-cut-internet-cables-in-latest-disruption-during-paris-olympics/>

19. Jake Wood 2 July 2025 *Arson Attacks on 5G masts ‘driven by conspiracy theories online’*. BBC. Available at: <https://www.bbc.com/news/articles/cd788lg2yn5o>

20. Harry Baldock 18 February 2025 *Hyperscalers: Seizing the reins of the submarine cable industry*. Total Telecom Newsletter. Available at: <https://totaltele.com/hyperscalers-seizing-the-reins-of-the-submarine-cable-industry/>

21. Barbara Moens 17 January 2026 *Brussels in move to bar Chinese suppliers from EU’s Critical Infrastructure*. Financial Times. Available at: <https://www.ft.com/content/eb677cb3-f86c-42de-b819-277bcb042295?syn-25a6b1a6=1>

22. Blackrock Investment Institute 21 November 2024 *AI’s big questions*. Available at: <https://www.blackrock.com/corporate/insights/blackrock-investment-institute/publications/investment-perspective/november-21-2024>

The spectrum of risks which Ireland's telecommunications sector is facing is therefore broadening at precisely the moment when Irish society would face severe consequences from any major geopolitical disruption to connectivity. What emerged from the discussions is that the security challenge is no longer focused on the protection of subsea cables alone, but extends increasingly to terrestrial infrastructure, data centres, supply chains, and the growing strategic importance of cloud and AI infrastructure. Ireland's exposure is not only shaped by its limited defence capacity, but also by its dependencies on external suppliers, a small group of hyperscalers, and infrastructure. Attacks, regardless of the actual extent of the disruption, on this infrastructure could damage long term investment in Ireland, and harm Ireland's economic and social vibrancy. Against this backdrop, resilience will need to become a shared strategic responsibility between government and industry, which will come with costs.

4. 'The costs have to fall somewhere': Resilience, Regulation, and Permitting

There is definitely a moral hazard, if you assume the State will pick up the pieces then you won't take responsibility for your own security. On the other side is that the private sector can't be left to fend for itself. The costs have to fall somewhere.

- Roundtable Participant

The costs of resilience featured prominently throughout both roundtables; with where should the costs fall becoming a focal point of the discussion. Against the backdrop of the EU's Digital Networks Act, the Cybersecurity Act, and the EU's preparedness agenda, industry will be required to increase their resilience, security, as well as being subject to increased regulatory reporting requirements. The roundtables highlighted that redundancy plays a foundational role in resilience. Yet, regulation and permitting has created challenges for industry when attempting to build additional capacity and redundancy, either by increasing costs or creating delays which make projects unviable.

Regulation and Resilience

It was noted by a senior representative of a government department that resilience, security, and strategic autonomy are the overriding themes in Brussels. The EU's Preparedness Union Strategy will require the development of 'minimum preparedness criteria' for telecommunications,²³ including stockpiling at a time when supply chains are stressed by AI investment and rising costs for industry. Moreover, it was noted by a representative from the telecommunications sector that 'resilience is not the only thing being asked' of telecommunications, with another stating that 'telco needs to do everything and be everything.' It was expressed that the demands at EU and national level, 'industry-led growth, decarbonisation, and competitiveness', mean that industry is being asked to do too much at the same time. According to the European Commission's Impact Assessment of the 'updated Cybersecurity Act (CSA2)', the cost of removing all 'high-risk Chinese equipment across European operators 3G, 4G, and 5G, mobile networks could be between 3.4 billion EUR and 4.3 billion EUR, per year, for three years.²⁴ Yet, it is estimated that the cost of the updated EU Cybersecurity Act to industry in Ireland alone could be near 730 million EUR.²⁵ Consequently, the costs to industry may be greater than initially assessed by the Commission in its impact assessment, and could risk reducing the overall resilience of the network.

Cumulatively, there was a sense amongst industry that the European Commission has determined that there is a major risk around security, but that 'the response has been to privatise responsibility for this risk', rather than provide sufficient supports to enable European telecommunications operators to manage supply chain risks.

Yet, representatives from Government expressed a clear desire to engage with industry to provide the supports and regulatory clarity at the level of national implementation. A senior representative from a government agency with knowledge of the sector expressed that while they did not want a situation whereby risk was being 'transferred' from 'the companies to the regulator', they were clear that from a State view 'having companies that are not making a good return on investment, was not good from a resilience perspective.' Consequently, an area of common agreement

23. European Commission 26 March 2025 *EU Preparedness Strategy to Prevent and React to Emerging Threats and Crises – Press Release*. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_856/IP_25_856_EN.pdf

24. European Commission 2026: 86 *Impact Assessment - Proposal for a Regulation for the EU Cybersecurity Act*. Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>

25. Aine Clarke 15 April 2026 *EU Cybersecurity Act Review (CSA2)*. IBEC. Available at: <https://cdn.ibec.ie/-/media/documents/connect-and-learn/insights/ibec-position-on-csa2---april-2026.pdf?rev=5291574cb7f34d32aac47941452cc166>

between the State and industry was the importance of how the financial sustainability of the sector is critical to the resilience, to ensure that industry can continue to invest in future capacity and redundancy.

Moreover, it was assessed by Government and private sector participant that the regulatory burden on telecommunications – as well as other critical sectors – had resulted in a form of ‘archaeological stratification and layering of regulations’ which has led to a scenario whereby good intentioned regulation is unable to affect outcomes as originally anticipated by policymakers. Importantly, many of these regulations on security and resilience such as the Critical Entities Resilience Directive and the NIS2 Directive have significant consequences to private sector organisations for breaches including fines of up to 10 million EUR or 2% of total worldwide turnover.²⁶

Many of the representatives expressed concern about how this stratification and layering of regulations often leads to duplication. This compounding of regulation poses risks to the overall resilience of the telecommunications sector, as the regulatory burden can pose a significant barrier to new entrants into the market, further exacerbating the risk of increased dependencies, reduced redundancies, and reduced overall resilience of the telecommunications sector. While this was acknowledged as a broader risk to European telecommunications infrastructure, it is a particularly acute challenge for a small market such as Ireland where the market can only support a certain number of actors in the telecommunications sector in the first place.

Importantly, while representatives from Government did caution against a ‘big blunderbuss of deregulation,’ there was acceptance that there is ‘too much complexity’ and that regulation has ‘grown at a pace that has outstripped our ability to manage it properly.’ In this regard, while well intentioned, the regulatory requirements placed on the telecommunications sector may have compounded to such an extent that they are in fact reducing overall resilience, rather than increasing it.

Permitting and its Impacts on Resilience

Permitting and planning represent significant obstacles not only to the building of additional redundancy and capacity of Ireland’s submarine cable network and wider telecommunications infrastructure, but delays in permitting represent a long-term strategic risk to Ireland. At present 14 cables land in Ireland, and many of them are approximately 80% of the way through their expected lifetime. A representative from industry with knowledge of data centre infrastructure and telecommunications expressed that many of the hyperscalers, as well as the new AI organisations funding new infrastructure projects, are choosing not to land cables in Ireland due to the perceived extended timelines for approval. However, the establishment of the Maritime Area Regulatory Authority, with powers to grant Maritime Usage Licenses for subsea data cables,²⁷ was viewed positively, with wait times reduced from years to months.

Yet, persistent bottlenecks in the approval of critical enabling infrastructure, such as energy and grid infrastructure for data centres and telecommunications has discouraged investment. In 2025, 5.6 billion EUR of investment in data centre infrastructure has been delayed due to a lack of energy to support their operation in Ireland.²⁸ Ireland has announced a Critical Infrastructure Bill which will serve to fast-track approvals for projects designated as critical infrastructure, such as energy and telecommunications infrastructure.²⁹

Yet, this is unlikely to address the issue entirely. Representatives from Government and from industry noted that the judicial review process remains a significant barrier to investment in infrastructure in Ireland. One senior representative from Government explicitly remarked that permitting is a ‘profound problem’ and that investment will not happen if projects continue to find themselves in the high court at a late

26. National Cyber Security Centre 18 NIS 2 A Quick Reference Guide. National Cyber Security Centre. Available at: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

27. Maritime Area Regulatory Authority Applying for a MUL. Available at: <https://www.maritimeregulator.ie/our-work/maritime-usage-licences/applying-for-a-mul/>

28. Arthur Beesley 13 October 2025 Data centres costing €5.6bn have planning approval but no electricity, industry warn. The Irish Times. <https://www.irishtimes.com/ireland/2025/10/13/data-centres-costing-56bn-have-planning-approval-but-no-power-industry-warns/>

29. Government of Ireland 4 March 2026 Minister Chambers Announces Government Approval for Development of Critical Infrastructure Bill. Available at: <https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/press-releases/minister-chambers-announces-government-approval-for-development-of-critical-infrastructure-bill/>

stage in the process. The Government has proposed a change to the judicial review process, a process designed to ensure that citizens have a right to challenge decisions – such as planning – made by public bodies in Ireland’s High Court, which would introduce a ‘public interest test’ for those taking such cases.³⁰

Cumulatively, the obstacles presented by planning and permitting were viewed as a significant obstacle to investment in new telecommunications and energy infrastructure. A representative from industry noted that industry views that under the current regime ‘the time frame is a black hole’, and that projects continue to not go ahead or be relocated outside of the State. Consequently, under the present system, Ireland risks being unable to replace aging infrastructure, unable to build new infrastructure which would benefit Ireland’s society, and unable to build the additional capacity and redundancy required for a resilient telecommunications system which can meet the challenges of increased geopolitical contestation.

Overall, the roundtables have highlighted that the current policy framework risks making resilience harder to achieve in practice for the private sector and for the State. At EU and national level, telecommunications operators are being asked to increase their security, manage their supply-chain risk, invest in capacity and redundancy, even while planning, economic, and regulatory conditions create obstacles to those objectives. Consequently, there is now a growing tension between the strategic objective of resilience and the practical and financial conditions required to deliver it.

In the present system, Ireland risks creating a scenario whereby the compounding burden of regulation and delay discourages investment, weakens competition, and ultimately reduces the very redundancy and capacity required to have a resilient telecommunications system. Government and industry will need to find ways and means to work together to ensure that Ireland can build a truly resilient telecommunications system that can support essential services, daily life, and the State’s prosperity.

30. Government of Ireland 7 January 2026 Minister Jim O’Callaghan publishes Civil Reform Bill to overhaul Judicial review and streamline courts processes. Available at: <https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/press-releases/minister-jim-ocallaghan-publishes-civil-reform-bill-to-overhaul-judicial-review-and-streamline-courts-processes/>

5. Recommendations: Building a Resilient Telecommunications System through a Whole-of-Society Approach.

The resilience piece is symbiotic. We rely on the State to protect our infrastructure; we rely on the State to give us a grid for our power. So, if I think about resilience its not event about legislation, it is a system. How do we build trust and how do we build partnerships?

- Roundtable Participant

Today, Ireland faces a radically deteriorating security environment shaped by growing hybrid threats, cyberattacks, espionage, and increased risks to critical infrastructure including telecommunications networks.³¹ The deteriorating security environment means that critical infrastructure, much of which is operated and overseen by the private sector, is under pressure from geopolitical risks. While telecommunications networks tend to be physically quite robust, recent events have illustrated that states and non-states alike are willing and able to attack subsea cables, terrestrial networks, and even data centres using both kinetic and cyber means. Defending this infrastructure and protecting society from the cascading consequences which could follow from a targeted attack or extreme weather incident such as 2025's Storm Eowyn,³² requires a whole-of-society approach whereby the State and the private sector work in tandem to share expertise and capabilities for the common good.

1. Ireland should develop a clearer framework for balancing the responsibilities of resilience between the State and the private sector as a part of the operationalisation of the National Strategy for the Resilience of Critical Entities (2026-2029).

As the range of threats to telecommunications infrastructure continues to grow, private sector telecommunications organisations must face up to the need to be more resilient. Operators must increasingly absorb the costs of redundancy, supply-chain derisking, and preparedness, and often have to overcome serious regulatory obstacles which can cause delays and increased costs. Ireland should consider where resilience can reasonably be considered to be primarily a private sector responsibility, and where the State may need to provide additional support. The National Strategy for the Resilience of Critical Entities (2026-2029) identified that it may be necessary to provide supports such as 'exemptions from or simplification of certain requirements' for SME's, for example.³³

While this is an important step, the broader context, which includes the changing equipment requirements for telecommunications operators should be also considered. An industry representative expressed to us that telecommunications is different to state monopolies and utilities such as water and energy where 'realistically the State can come in and cover those costs for security.' To support increased resilience across sectors, Ireland could consider developing a tax credit, based on the model of the Research and Development (R&D) Corporation Tax Credit,³⁴ to support the private sector as it manages the costs of measures designed to build and bolster resilience. This could assist in enabling the private sector to build resilience capabilities faster, while lowering the risk of private sector organisations reducing their footprints or exiting due to perceptions around the commercial viability of doing business.

31. Cian FitzGerald and Barry Colfer: 2025 *Secure Together: Enhancing Ireland's Security and Resilience in a time of Geopolitical Risk*. IIEA. Available at: <https://www.iiea.com/publications/secure-together-enhancing-irelands-security-and-resilience>

32. Met Éireann 29 August 2025 *Hurricane Force Eowyn*. Available at: <https://www.met.ie/cms/assets/uploads/2025/10/Eowyn.pdf>

33. Government of Ireland: 35 2026 *National Strategy for the Resilience of Critical Entities (2026-2029)*. Available at: <https://assets.gov.ie/static/documents/9222c1da/National-Strategy-on-the-Resilience-of-Critical-Entities-20262029.pdf>

34. Government of Ireland: 35 2026 *National Strategy for the Resilience of Critical Entities (2026-2029)*. Available at: <https://assets.gov.ie/static/documents/9222c1da/National-Strategy-on-the-Resilience-of-Critical-Entities-20262029.pdf>

2. The Department of Culture, Communication, and Sport should seek to provide greater long-term certainty on spectrum policy in the context of implementing the Digital Networks Act (DNA).

A number of participants highlighted that long-term investment depends not only on the availability of finance, but on predictable policy. One representative from industry expressed that the current spectrum arrangement was as if they were being asked to build a house and subsequently auction the land underneath every 15 years. Greater levels of certainty on the future of radio spectrum bands would assist in building confidence and would help operators plan for long-term upgrades, redundancy, and for next-generation capability. The proposed Digital Networks Act (DNA), which has identified the challenges posed by short licencing periods,³⁵ is intended to encourage Member States to provide long-term licence arrangements to telecommunications providers to encourage investment. Thus, the DNA could provide an opportunity for the Department of Culture, Communications and Sport to provide longer licences to telecommunications companies in a bid to enable greater policy certainty, and to allow for operators to invest in future systems and additional resilience.

3. Government should expedite the creation of a security clearance system to support the exchange of information and intelligence.

Representatives from Government and industry consistently express a desire for greater levels of coordination between the State and industry to enable the exchange of information and intelligence, in particular regarding classified information on geopolitical risks emerging from potential State actors such as the Russian Federation. Government should seek to expedite the Department of Justice, Home Affairs, and Migration in the process of establishing a National Security Authority to facilitate security clearances. At present, there are a number of 'trusted networks' in operation, including the Telecommunications Response and Resilience Group (T-RRG) which was established in 2025.³⁶ While the Resilience of Critical Entities Directive (CER Directive) does legislate for background checks to defend against risks,³⁷ a developed security clearance system for Ireland should be viewed as a key strategic enabler.

4. Government and Industry should augment 'trusted networks' through regular joint exercises and simulations to strengthen preparedness, trust, and identify risks.

A senior representative from Government acknowledged that for many years, Ireland's approach to emergency planning has been relatively poor. For example, it was noted that there is a divergence in how Government and industry navigate Europe's more volatile security landscape. While Government representatives express concern about strategic level risks that can impact society, the private sector also have to contend with day-to-day operational risks. As one industry representative remarked, there are a lot of 'mundane risks', and there was perhaps 'a little bit of catastrophising' going on in wider discourse. Though the gap in how to navigate these risks was accepted to be narrowing, more scenario planning and crisis simulations could assist in further bridging this gap beyond simply the exchange of information.

While exercises were carried out in the wake of Storm Eowyn in 2025, the range of risk-based scenarios which telecommunications infrastructure face is expanding to take in weather-related risks, to cyberattacks, sabotage, and kinetic attacks. While concerns about the capacity across the civil service and the private sector to regularly conduct exercises was raised by a representative from Government, simulations would greatly enhance the preparedness of critical services including telecommunications.

Regularising crisis scenario simulations would enable Government and the private sector to test and develop plans for dealing with specific crises,³⁸ to identify gaps in risk mitigation measures, and to identify unforeseen risks and potential 'black swan' events in a 'safe-to-fail' environment.³⁹ One representative from industry noted that at present 'we don't know where our reliance on subsea cables lie', and that we don't know exactly where many of our vulnerabilities sit; noting soberingly that it could be 'one tiny bit of software located in another jurisdiction' that could cause significant

35. European Commission 2026: 8 *Proposal for a Regulation for the Digital Networks Act*. Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna>

36. Government of Ireland May 2026 *Emergency Planning*. Available: <https://www.gov.ie/en/department-of-culture-communications-and-sport/policy-information/emergency-planning/>

37. Government of Ireland 2

38. UK Ministry of Defence 2017: 9 *Wargaming Handbook*. Available at: <https://www.gov.uk/government/publications/defence-wargaming-handbook>

39. Ibid

societal issues. Not only would such crisis scenarios assist in identifying risks and gaps, but they would also play a vital role in training decision-makers in how to manage crises.⁴⁰ Such exercises, when done correctly to provide sufficient levels of engagement,⁴¹ can also have a bonding function, facilitating peer-to-peer relationships that can exist beyond any crisis simulation. This could play an important role in generating ongoing buy-in in for collaboration around building resilience, breaking down silos, and enhancing cooperation, as well as facilitating the creation of peer-to-peer networks which would overall enhance the capability to respond during a crisis.

5. Government should increase institutional and regulatory capacity and capability, including through additional resourcing for key bodies such as MARA.

A recurring theme throughout the roundtable meetings was that regulatory complexity had outpaced the capacity of the State to manage it effectively. While regulatory simplification could assist the State in better managing the implementation of regulation, it is only one piece of the puzzle. It was acknowledged that while in recent years, Ireland's population has grown so has the number of regulations, while the size of the civil service has remained largely static. In the IIEA's *Secure Together: Enhancing Ireland's Security and Resilience in a Time of Heightened Geopolitical Risk* paper, industry representatives also expressed their wish to see Government provide additional capacity and capability to the civil service to deal with geopolitical risk.⁴²

It was also identified that more State capacity is needed to engage with industry, draft better legislation, and to accelerate implementation of policy. Indeed, one senior government representative noted that this failure to increase the size of the civil service in line with the growing demands being placed on it was a major strategic risk in itself. Government should provide additional resources for the civil service and for the regulatory bodies responsible for overseeing telecommunications such as MARA (the Maritime Area Regulator Authority) and ComReg (the Commissioner for Communications Regulator). The potential role of MARA in radically improving maritime cable licencing timelines was viewed positively by participants. Increasing State capacity and capability across the board would also assist in creating the conditions for more frequent engagement between State and industry, and would enable resilience-building measures such as better regulation, faster approvals for new projects, and crisis simulations.

6. National security and resilience considerations should be explicitly reflected in the proposed 'public interest test' for judicial review reform.

Representatives from Government and industry equally stressed that the judicial review process presents a significant obstacle to the development of additional redundancy and capacity in Ireland's energy and telecommunications sector. While ensuring the right of citizens to challenge public decisions remains essential, Government should explore whether the proposed 'public interest test' for judicial reviews should explicitly include the contribution of strategic telecommunications, energy, and digital infrastructure to national security and overall societal resilience.

7. Government should integrate space-based infrastructure into national telecommunications resilience planning, and should engage in greater strategic engagement with EU programmes such as IRIS².

Digital infrastructure resilience can no longer be understood in purely terrestrial or subsea terms. Satellite communications; Earth observation; and Position, Navigation and Timing (PNT) systems; are becoming increasingly ubiquitous and essential for the operation of essential services on a day-to-day basis, but also for continuity of service in times of crisis. While Ireland is geographically well positioned to support space-based connectivity projects of European interest such as IRIS², the EU's satellite internet connectivity programme,⁴³ a well-placed industry representative once again noted that the lack of a system for security clearances continues to pose a significant obstacle to Ireland's participation in such programmes.

40. UK Ministry of Defence 2017: 8 *Wargaming Handbook*. Available at: <https://www.gov.uk/government/publications/defence-wargaming-handbook>

41. Ministry of Defence 2017: 25 *Wargaming Handbook*. Available at: https://assets.publishing.service.gov.uk/media/5a82e90d40f0b6230269d575/doctrine_uk_wargaming_handbook.pdf

42. Cian FitzGerald and Barry Colfer: 9 2025 *Secure Together: Enhancing Ireland's Security and Resilience in a time of Geopolitical Risk*. IIEA. Available at: <https://www.iiea.com/publications/secure-together-enhancing-irelands-security-and-resilience>

43. European Space Agency *EU secure connectivity programme / IRIS²*. Available at: <https://eu-space.europa.eu/programmes/secure-connectivity-iris2-and-govsatcom/eu-secure-connectivity-programme-iris2>

Finally, under the proposed EU Space Act, Ireland will be required to designate a competent authority with sufficient resources and powers to oversee Ireland's space sector.⁴⁴ A new agency responsible for space could play a critical role in creating greater policy coherence and coordinate efforts across the likes of the Department of Defence; the Department of Enterprise, Tourism, and Employment; and others with responsibility for space. In particular, it could play a key function in unlocking the potential for space-based systems to support Ireland's society during crisis events such as extreme weather or a hybrid attack on critical telecommunications infrastructure.

44. European Union 1.28-39 *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety, resilience and sustainability of space activities in the Union*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0335>

6. Conclusion: ‘When we work together, it works’

**Connectivity is the nervous system of our society...
it is never more important than during a crisis.**

- Roundtable Participant

Ireland’s telecommunications infrastructure ecosystem is a foundational layer of public life and a critical node for Europe’s security and resilience. The cables, data centres, radio spectrum, internet exchanges, satellite systems, and energy infrastructure that make up Ireland’s telecommunication system underpin the functioning of public services, financial systems, healthcare, defence, and day-to-day social life across the continent. Ireland’s open economy has led to a growing role in European and transatlantic digital infrastructure in particular, which has contributed to Ireland’s prosperity for decades. Yet against the backdrop of a radically deteriorating security environment, where telecommunications infrastructure is now seen as something to be targeted in a conflict to maximise civilian disruption and harm, this infrastructure is now under strain and is increasingly exposed. That the spectrum of threat vectors is increasing at a time when our societies are most dependant on telecommunications connectivity means that a serious incident would have cascading consequences throughout Irish society and economy. Thus, in this context, the resilience of telecommunications infrastructure should be understood as a core element of national security and societal resilience.

Ireland’s exposure to geopolitical risk is broader than public debate often suggests. Subsea cable security remains of high strategic importance, given Ireland’s geographical position, limited naval capabilities, and the growing pattern of hybrid activity across Europe. However, the roundtables convened as part of this project demonstrate that this vulnerability is not only a risk to Ireland’s telecommunications system but simultaneously to Ireland’s society and prosperity. Terrestrial networks, data centres, supply chains, energy systems, and space-based assets now function as part of the same essential system. Disruption to one part can easily spillover to others, with the impact felt across wider society in a number of ways.

Moreover, resilience is becoming increasingly expensive and challenging to implement and maintain. Throughout this project, participants repeatedly returned to the questions of who pays for redundancy, who pays for supply chain derisking, and who pays for security? Telecommunications operators are being asked to deliver more security, more investment, more resilience, more decarbonisation, and more innovation, at a time when regulation is becoming ever more complex. This has created a moral hazard whereas resilience is now essential for society, yet it is delivered via infrastructure that is owned and operated by the private sector. If the costs of resilience are left solely to the private sector, lower investment, reduced redundancy, and weaker competition may result, thereby reducing resilience rather than enhancing it.

At the same time Ireland’s planning and regulatory systems are not moving at the pace required by the State’s present risk environment. This presents significant obstacles to building the redundancy required to have a resilient telecommunications system. Delays in permitting, grid connection, judicial reviews, and regulations can make essential projects unviable or can encourage investors to locate elsewhere. Moreover, potential policy uncertainty regarding radio spectrum licencing continues to deter long-term investment from telecommunications providers. This matters for Ireland. If new subsea cables, AI infrastructure, satellite uplinks or data centres are stalled, not only does Ireland risk losing out on economic opportunities, but it also risks losing the additional capacity and redundancy needed to build resilience.

The paper’s recommendations attempt to point towards a model of shared responsibility and public-private partnership to mitigate these challenges. The paper argues that the State should clarify the balance between public support and private responsibility for the cost of resilience; that it should accelerate the creation of a security clearance system to allow for greater information sharing with industry on geopolitical risk; and that there should be regular joint exercises and simulations so that government and the private sector can build peer-to-peer relationships and develop a shared perception of risk. The paper argues for example that the State could provide long-term certainty on radio spectrum

policy in the context of the Digital Networks Act (DNA) to encourage long-term investment; and that it could increase capacity and capability in the civil service and regulators to enable the State to engage more effectively. While reforms regarding judicial reviews and critical infrastructure are under consideration, national security and resilience should be considered in the proposed 'public interest test'. Finally, Ireland should integrate space-based infrastructure into its resilience planning to enable better crisis response and continuity of service during crises.

Cumulatively, telecommunications infrastructure is indispensable for the functioning of Ireland's society. Essential services such as healthcare, water services, banking, transportation among much else are increasingly reliant and underpinned by digital infrastructure. Yet, this infrastructure is owned and largely operated by the private sector. Ensuring that this critical infrastructure, including subsea cables, terrestrial systems, and data centres, is protected will require a whole-of-society effort, which brings the resources and expertise of the State and private sector together. While how the State and the private sector will share the burden, share resources, and share information, remains to be seen, what is certainly clear to industry and government, is that 'when we work together, it works'.

Bibliography

BBC (2024) *Only two Irish Navy ships available to go to sea*, BBC News, Available at: <https://www.bbc.com/news/articles/cprwlpdv04lo>

Beesley A. (2025) *Data centres costing €5.6bn have planning approval but no electricity, industry warn*, The Irish Times, Available at: <https://www.irishtimes.com/ireland/2025/10/13/data-centres-costing-56bn-have-planning-approval-but-no-power-industry-warns/>

BlackRock Investment Institute (2024) *AI's big questions*, Available at: <https://www.blackrock.com/corporate/insights/blackrock-investment-institute/publications/investment-perspective/november-21-2024>

Boffey, D. (2026) *It means missile defence on data centres': drone strikes raise doubts over Gulf as AI superpower*, The Guardian, Available at: <https://www.theguardian.com/world/2026/mar/07/it-means-missile-defence-on-data-centres-drone-strikes-raises-doubts-over-gulf-as-ai-superpower>

BT (2025) *BT enters agreement with Speed Fibre Group for the sale of its wholesale and enterprise business unit in Ireland*, Available at: <https://www.btireland.com/news/article/2025/02/05/bt-enters-agreement-with-speed-fibre-group-for-the-sale-of-its-wholesale-and-enterprise-business-unit-in-ireland>

Burgess, M. (2024) *'Saboteurs cut internet cables in latest disruption during Paris Olympics'*, Wired, Available at: <https://www.wired.com/story/saboteurs-cut-internet-cables-in-latest-disruption-during-paris-olympics/>

Chiappa, C. and Ngendakumana, P.E. (2023) *Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says*, Politico, Available at: <https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/>

Central Statistics Office 7 July 2026 *Data Centres Metered Electricity Consumption*. Available at <https://www.cso.ie/en/releasesandpublications/ep/p-dcmec/datacentresmeteredelectricityconsumption2025/>

Clarke A. (2026) *EU Cybersecurity Act Review (CSA2)*. IBEC. Available at: <https://cdn.ibec.ie/-/media/documents/connect-and-learn/insights/ibec-position-on-csa2---april-2026.pdf?rev=5291574cb7f34d32aac47941452cc166>

Commission on the Defence Forces (2022) *Report of the Commission on the Defence Forces*. Available at: <https://assets.gov.ie/static/documents/report-of-the-commission-on-the-defence-forces.pdf>

Department of An Taoiseach (2024) *National Risk Assessment 2024: Overview of Strategic Risks*. Available at: <https://assets.gov.ie/static/documents/national-risk-assessment-2024-overview-of-strategic-risks.pdf>

Edwards, C. and Seidenstein, N. (2025) *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. IISS. Available at: <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure>

European Commission (2025) *EU Preparedness Strategy to Prevent and React to Emerging Threats and Crises – Press Release*, Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_856/IP_25_856_EN.pdf

European Commission (2026) *Impact Assessment – Proposal for a Regulation for the EU Cybersecurity Act*. Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>

European Commission (2026) *Proposal for a Regulation for the Digital Networks Act*. Available at: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna>

European Space Agency *EU secure connectivity programme / IRIS²*. Available at: <https://eu-space.europa.eu/programmes/secure-connectivity-iris2-and-govsatcom/eu-secure-connectivity-programme-iris2>

European Union (2025) *Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC033>

FitzGerald, C. and Colfer, B. (2025) *Secure Together: Enhancing Ireland's Security and Resilience in a Time of Geopolitical Risk*. Institute of International and European Affairs. Available at: <https://www.iiea.com/publications/secure-together-enhancing-irelands-security-and-resilience>

Gallagher, C. (2025) *Russian spy ship on course for Irish waters, with UK threatening military options*, The Irish Times, Available at: <https://www.irishtimes.com/ireland/2025/11/19/russian-spy-ship-on-course-for-irish-waters-with-uk-threatening-military-options/>

Government of Ireland (2025) *European Union (Resilience of Critical Entities) Regulations 2024*, Available at: <https://www.gov.ie/en/office-of-emergency-planning/organisation-information/critical-entities-resilience-cer-regulations/>

Government of Ireland (2026) *Minister Chambers Announces Government Approval for Development of Critical Infrastructure Bill*, Available at: <https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/press-releases/minister-chambers-announces-government-approval-for-development-of-critical-infrastructure-bill/>

Government of Ireland (2026) *Minister Jim O'Callaghan publishes Civil Reform Bill to overhaul Judicial review and streamline courts processes*, Available at: <https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/press-releases/minister-jim-ocallaghan-publishes-civil-reform-bill-to-overhaul-judicial-review-and-streamline-courts-processes/>

Government of Ireland (2026) *National Strategy for the Resilience of Critical Entities (2026–2029)*. Available at: <https://assets.gov.ie/static/documents/9222c1da/National-Strategy-on-the-Resilience-of-Critical-Entities-20262029.pdf>

Government of Ireland (2026) *Emergency Planning*, Available at: <https://www.gov.ie/en/department-of-culture-communications-and-sport/policy-information/emergency-planning/>

House of the Oireachtas (2025) *Naval Service*, Available at: <https://www.oireachtas.ie/en/debates/question/2025-05-08/184/>

- Maritime Area Regulatory Authority *Applying for a MUL*. Available at: <https://www.maritimeregulator.ie/our-work/maritime-usage-licences/applying-for-a-mul/>
- Mellet, M. (2024) *What's Past is Prologue: Ireland's Security and Defence in a New European Context*. Institute of International and European Affairs. Available at: <https://www.iiea.com/publications/whats-past-is-prologue-irelands-security-and-defence-in-a-new-european-context>
- Met Éireann (2025) *Hurricane Force Éowyn*, Available at: <https://www.met.ie/cms/assets/uploads/2025/10/Eowyn.pdf>
- Moen, B. (2026) *Brussels in move to bar Chinese suppliers from EU's critical infrastructure*, Financial Times,. Available at: <https://www.ft.com/content/eb677cb3-f86c-42de-b819-277bcb042295?syn-25a6b1a6=1>
- National Cyber Security Centre (2019) *National Cyber Security Strategy 2019–2024*. Available at: <https://assets.gov.ie/static/documents/national-cyber-security-strategy-2019-2024.pdf>
- National Cyber Security Centre *NIS 2 A Quick Reference Guide*. Available at: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- O'Doherty, C. (2026) *Data centre electricity demand could exceed power usage of the republic*, The Irish Times, Available at: <https://www.irishtimes.com/politics/2026/06/09/data-centre-electricity-demand-could-exceed-power-usage-of-entire-country/>
- RTÉ (2025) *How many of world's undersea cables pass through Irish waters?*, RTÉ News, Available at: <https://www.rte.ie/news/2025/0219/1497714-irish-undersea-cables/>
- Schia, N.N., Gjesvik, L. and Rødningen, I. (2023) *The Subsea Cable Cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?* Norwegian Institute of International Affairs. Available at: https://www.nupi.no/content/pdf_preview/26372/file/NUPI_Policy_Brief_1_23_Schia_Gjesvik_R%C3%B8dningen-FERDIG.pdf
- Total Telecom (2025) *Hyperscalers: Seizing the reins of the submarine cable industry*, Total Telecom Newsletter,. Available at: <https://totaltele.com/hyperscalers-seizing-the-reins-of-the-submarine-cable-industry/>
- UK Ministry of Defence (2017) *Wargaming Handbook*. Available at: <https://www.gov.uk/government/publications/defence-wargaming-handbook>
- Wall, C. and Morcos, P. (2021) *Invisible and Vital: Undersea Cables and Transatlantic Security*. Center for Strategic and International Studies, Available at: <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>
- Wood, J. (2025) *Arson attacks on 5G masts driven by conspiracy theories online*, BBC News, Available at: <https://www.bbc.com/news/articles/cd788lg2yn5o>

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 acts as a forum for informed debate, analysis and discussion. Views expressed in the Institute's publications, and in presentations at its events, are those of the authors alone and do not represent the views of the Institute, which is fully independent. The IIEA is a not-for profit organisation with charitable status.

© Institute of International and European Affairs, July 2026

Creative Commons License

This is a human-readable summary of (and not a substitute for) the license.

<https://creativecommons.org/licenses/Attribution-NonCommercial-ShareAlike/4.0/> 4.0 International (CC BY-NC-SA 4.0)

You are free to:

- Share - copy and redistribute the material in any medium or format
- Adapt - remix, transform, and build upon the material
- The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.



The Institute of International and European Affairs,

8 North Great Georges Street, Dublin 1, Ireland

T: +353-1-8746756 F: +353-1-8786880

E: reception@iiea.com W: www.iiea.com

