Deloitte.
Together makes progress

IIEA
Sharing Ideas
Shaping Policy

Secure Together
Enhancing Ireland's Security and Resilience in a Time of Heightened Geopolitical Risk

December 2025

Deloitte Foreword

Arising from our work across both Government and industry, Deloitte has increasingly recognised in recent years that there is a need for an additional perspective on the topic of national security and defence in Ireland.

Too often media commentary and public debate overly pivots to emotive topics such as neutrality. But fundamentally, as a small island nation in an important geographic location, and an EU Member State we need the ability to protect our economy, society and democracy, and meet obligations to our European partners.

Resilience is *the* absolutely critical consideration for Ireland. This includes the protection of critical infrastructure and services; economic, energy and supply chain resilience; protection of assets in our territorial lands and waters; civil protection; and cybersecurity. Multiple recent examples from across Europe show how these are threatened in a hybrid warfare environment, and any lack of resilience in these areas pose significant risks to our economy and our people.

National security and defence, including the critical element of resilience, is a multi-faceted issue requiring a whole-of-government and indeed a whole-of-society approach to address. The role of and impact on private industry and services sectors are highly significant. The State relies heavily on the private sector for critical energy, communications, financial and transport infrastructures and services; and in a time of national emergency a highly joined up approach between Government and the private sector is essential. How well these interdependencies are understood across society at large is questionable. Additionally, industry and Irish based SMEs are well placed to not only contribute to the security and resilience agenda, but to also bring economic benefit to Ireland by leveraging the increased spending across Europe on defence and security.

The need to action at pace the Report of the Commission on the Defence Forces is widely acknowledged and is progressing, but the material changes in the geopolitical landscape since the report was published also require agility and adaptability in its delivery. The points above need to be underpinned by a robust capability to identify threats, provide an appropriate level of deterrence, and if necessary, defend effectively against these threats.

Deloitte is pleased to have supported this project, and we trust that this Whitepaper, developed in conjunction with the Institute for International and European Affairs, will contribute constructively to the advancement of national security, defence and resilience in Ireland.

Shane Mohan
Partner and National Government & Public Services Leader, Deloitte

Kieran O'Neill
Partner and Defence, Security & Justice Sector Leader, Deloitte

IIEA Foreword

We find ourselves in a more dangerous world. Russia's continued aggression against Ukraine threatens the security of Europe, including our own. Since 2022, we have seen an increase in disinformation campaigns, incidents of sabotage, cyberattacks and threats of military force being used against Ireland and other EU Members.

The IIEA's research on security and defence seeks to understand Ireland's changing security environment, and what we can do to protect ourselves in a more dangerous world. We seek to enable an open and honest discussion about the potential costs of inaction, the options for Ireland, and the future of our security policy and relationships with our neighbours.

The IIEA provides a platform for informed debate, providing resources on security and defence terminology, as well as hosting a series of events to promote open dialogue.

Building on our previous work with Deloitte, we were pleased to convene two important roundtables, assembling business leaders, representatives from the civil service, and academics to discuss the areas of most concern to them. These roundtables, supplemented by interviews, have enabled us to gather the perspectives of over 30 leading businesspeople, thinkers, and actors in Ireland's national security to identify how we can work together to make Ireland a safer place.

Security, in all of its forms, provides the foundation for Ireland's prosperity, social vibrancy, and national harmony. Ensuring that Ireland is a place where people feel safe and secure in their daily lives will remain of vital importance.

We are pleased to have had this opportunity to contribute to the discussion and to our national dialogue on how to protect ourselves. While this discussion may have a diverse range of positions, an area of agreement is that Ireland - and the chance for its people to live in peace, prosperity, and dignity - is worth protecting.

Alex White SC
Director-General of the IIEA

Table of Contents

Executive Summary

Ireland's security environment is at its most complex, most challenging, and most dangerous point in recent history. Marked by escalating hybrid threats, geopolitical instability, and emerging risks to critical infrastructure, economic prosperity, and societal cohesion, Ireland will have to adapt to the risks of a now dangerous world. Of greatest concern is that the possibility of an armed attack on an EU Member State, and its reverberating consequences for Ireland, are no longer outside the bounds of possibility.

This paper examines Ireland's geopolitical risk environment, including the risks to Ireland's society, prosperity, and the stated risks of most importance to Ireland's corporate and business community. However, preparations for crisis, such as unprecedented levels of defence expenditure also present opportunities for Irish business organisations and SMEs to contribute to Irish and European security and prosperity.

To gather data for this paper, the IIEA and Deloitte hosted two roundtables engaging senior representatives from Government agencies, financial services, communications, energy infrastructure operators, technology sector, aviation, think-tanks, and academic representatives. Using prepared questions, the moderator led a semi-structured discussion among the participants. Broken into two parts, each roundtable first examined Ireland's security context, while the second part explored the challenges and opportunities for public and private sector organisations to enhance Ireland's security. The roundtables were held under the Chatham House Rule.[1] Following the roundtables, the IIEA and Deloitte conducted a series of interviews with stakeholders from a range of Irish Government Departments and Agencies with responsibility for different aspects of Ireland's national security architecture.

This paper makes a number of recommendations, which the authors believe would enable Ireland to enhance the State's security and position Irish organisations to avail of the opportunities presented by the unprecedented level of investment being made in defence across Europe. This paper groups them under three overarching headings: leadership and direction, building a whole-of-government/ whole-of-society approach to security, and unlocking opportunities for Ireland. Under leadership and direction, this paper recommends that Ireland should expedite the development of a National Security Strategy, and that there is a need for ongoing political leadership and alignment on national security. It recommends that Ireland should also enhance support capacity and capability at Government level for national security. To build a whole-of-government / whole-of-society approach to security, this paper recommends that Government should examine means to increase public awareness and build a shared understanding of the threats which Ireland faces. Coupled with this, it recommends that Ireland should enhance the support to and dialogue with the private sector from the State's security architecture. Finally, this paper also recommends that the State should encourage the fostering and maintaining of peer-to-peer relationships, in particular between public and private sector stakeholders. In order to unlock the emerging opportunities for Ireland, this paper recommends that Government should examine the development of a strategy to support Ireland's defence industry / dual-use sector. Additionally, it recommends that Ireland should expedite the creation of a security clearance system for non-government officials. Coupled with this, Ireland should also amend the Science and Technology Act, 1987 to remove the restrictions placed on Enterprise Ireland's engagement with Ireland's dual-use sector. Finally, the Savings and Investment Union (SIU) provides a generational opportunity for Ireland to play a constructive role in European security.

Introduction

> "I don't think the concept of geopolitical volatility begins to capture the scale of what we are facing... I fear these issues will not be crystalised until we see a crisis – and by then it will be too late."
>
> **Roundtable Participant**

Ireland is now in a deteriorating European security environment that is unlikely to improve in the short-term. The State finds itself at a point where its people are now at increased exposure to geopolitical risks. Furthermore, these geopolitical risks endanger Ireland's reputation as a safe and stable place to do business, threatening Ireland's economic and social wellbeing. In this environment, inaction may quickly lead to social, economic, diplomatic, political, or financial costs, and will require the whole of Ireland's society to navigate our more insecure world.

Intensifying in the previous five years in the build-up to, and commencement of, Russia's full-scale invasion of Ukraine, EU Member States, including Ireland, are increasingly the targets of 'hybrid warfare' activity such as disinformation campaigns, cyberattacks, breaches of airspace and threats to critical subsea infrastructure, and espionage and sabotage. The volatility of the 21st century security environment is now directed at our societies and economies, with individual citizens and organisations in danger. Most seriously, an armed attack on an EU Member State now no longer seems outside the realm of possibility. Ireland is not immune from this, and for economic and other reasons could be specifically targeted.

Ireland's defence limitations are undergoing increased international scrutiny. Ireland will take up the Presidency of the European Union, beginning in July 2026. While the Presidency is an important political opportunity for the State, as has been shown during Denmark's Presidency,[2] hostile actors may use this as an opportunity for disruption and to cause harm. There is a considerable degree of concern over whether Ireland has the capabilities required to secure and protect itself against such threats, and the State may look for help from neighbours for security assistance.[3] This would be a short-term solution that only emphasises the need for a significantly enhanced defence capability.

Yet, preparations for crisis may present opportunities for Ireland. Many Irish organisations are well-positioned to provide products and services to augment the security of the European continent. As expenditure on security and defence increases, Ireland should ensure that its high-tech sector is positioned to be able to benefit as more resources are allocated to the sector.

This paper is a holistic examination of Ireland's geopolitical risk environment, including the risks to society, prosperity, and the stated risks of most importance to the corporate and business community. To meet the challenges of a more dangerous world, private sector organisations do expect governments to take the threats seriously and to provide a security architecture that meets the threats of the 21st century. Yet, they also have an expressed willingness and desire to play an active role in supporting Government in keeping Irish society safe.

In a more dangerous European security environment, many EU Member States, including Ireland, are making significant investments in their defence capabilities in the land, maritime, air, cyber, and space domains. In March 2025, the EU launched its ReArm EU plan, announcing €800bn in support for defence and dual-use industries in Europe, creating economic opportunities for many organisations involved in all aspects of the defence supply chain, while uplifting capabilities. This paper will explore the implications of this increased defence expenditure for Irish organisations and the opportunities that might emerge, while examining how Ireland can play a role in maintaining Europe's technological edge to deter potential aggressors.

'A Pandora's Box': Public Discourse and the Challenge of Risk Perception

"If you talk about the threats, you open a whole Pandora's Box about defence. What we need is a coordinated effort on the part of Government – some form of central core that could inform people..."

Roundtable Participant

Participants noted that it remains challenging to discuss the threats to the Irish State without opening a 'Pandora's Box' of related issues such as neutrality. While the previous initiatives embarked upon by Government such as the Consultative Forum on International Security Policy, hosted in June 2023, progressed the national conversation, Europe's security environment continues to deteriorate. While anti-militarism and support for neutrality was noted as a feature of the public discourse, a lesser acknowledged factor creating fragmentation was the sense that those who are supportive of increased defence expenditure tended to be perceived, often incorrectly, as proponents of Ireland joining NATO.

This led one participant to comment, 'the messenger is the wrong messenger.' While defence expenditure and Ireland's international partnerships are interrelated topics, experts in the room expressed a desire to establish means to decouple these issues to enable more constructive dialogues. This need to separate defence expenditure and Ireland's international partnerships into discrete elements was echoed by a representative from the financial services sector noting a broader challenge that when it comes to security, we are speaking different languages. Finding ways to develop a language and means to discuss Ireland's security, in its totality, will be imperative. The creation of a National Defence Academy to promote defence and security studies within the Defence Forces and to support other national bodies,[4] may present an opportunity to bring together Government departments and agencies, to generate common approaches and language, and to engender symbiotic and holistic approaches to national security.

At the same time, more will need to be done in the domain of strategic communications with the public to ensure that they have access to trusted and impartial information. As a part of future 'Be Winter Ready' or other public preparedness campaigns, Ireland could adapt Sweden's brochure entitled 'In Case of Crisis or War' [5] a pamphlet which outlines the threats to national security, as well as what to do during times of conflict. Information includes how to seek shelter and what should be in your home during a crisis. Having this critical information in a single printable format in Irish homes could enhance civilian engagement and preparedness not only during a crisis, but also during emergencies such as floods and storms, potentially leading to better outcomes and reduced strains on critical services.

The brochure includes instructions on 'psychological defence', and how to protect oneself from the effects of disinformation during times of crisis and day-to-day.[6] It also includes important information regarding managing anxieties related to increased geopolitical risk, how to discuss these risks with young people, and the supports available to those in need of special assistance. Such a pamphlet, adapted for an Irish context, may assist with developing consensus on the risks to the State, possibly enhance individual resilience during uncertain times, and ensure that there is a shared understanding of how individuals can contribute to the safety of themselves, their families, and their communities in times of crisis.

This fragmentation of public discourse has correspondingly created a growing challenge nationally regarding the Irish public's perception of the risk, and the threats which Ireland faces. Hybrid threats such as the ransomware attack on the HSE in 2021,[7] planned Russian military exercises in Ireland's exclusive economic zone,[8] threats to critical infrastructure,[9] repeated activities by Russia's 'shadow fleet'[10], and reports of espionage[11] are being increasingly covered in the media and spoken about at the political level, assisting to shift the public perception and understanding of the nature of the threats Ireland is facing.

However, as many of the representatives from academia and industry raised, while it is positive that awareness of these issues is growing, this does not even begin to capture the danger which Ireland faces. One representative from academia noted that we are witnessing the collapse of the US-led post-Cold War order, with the United States becoming less predictable and with Russia threatening to attack EU Member States and expand its war of aggression against Ukraine. Not only does the possibility of war in Europe seem more likely, but the risk that Europe could also lose this war was seen as a potential scenario Ireland would have to contend with. While there was a sense that Europe was not yet at war, it was not at peace either. There will need to be a growing recognition of the costs of inaction and passivity in the face of a potential looming crisis. Tentative and incremental responses will leave European citizens in danger.

Against this collective backdrop, a clear desire for increased and courageous political leadership when it comes to national security was expressed by many of the senior representatives during the roundtable sessions. Private sector organisations expressed frustration that they are shouldering the burden of defending against hybrid warfare activities, with one representative from a large multinational financial services institution stating that Government has overly relied upon the capabilities of the private sector to provide the necessary expertise to address the challenges emerging from Ireland's changing geopolitical context.

To address this, many representatives from the private sector were asking for the Government to provide for additional capacity and capability within the civil and public services to guide businesses and the public at large in navigating this period of heightened risk. An element of this may also include elevating the role of the Office of Emergency Planning, granting it additional resources and capabilities for scenario planning, preparedness, and resilience building. As a participant from a business representation organisation noted, industry can only move at the pace of regulators and will need to be able to have a partner in the State. Without greater investment by Government to provide the resources and expertise required, multinationals may choose to look towards European Member States that can provide a more secure environment to locate operations.

'Volatility is the Default Setting': Geopolitical Risk Now Endangers Ireland's Society and Prosperity

> "The number of ways that you can target critical infrastructure is quite diverse and getting more brazen."
>
> **Roundtable Participant**

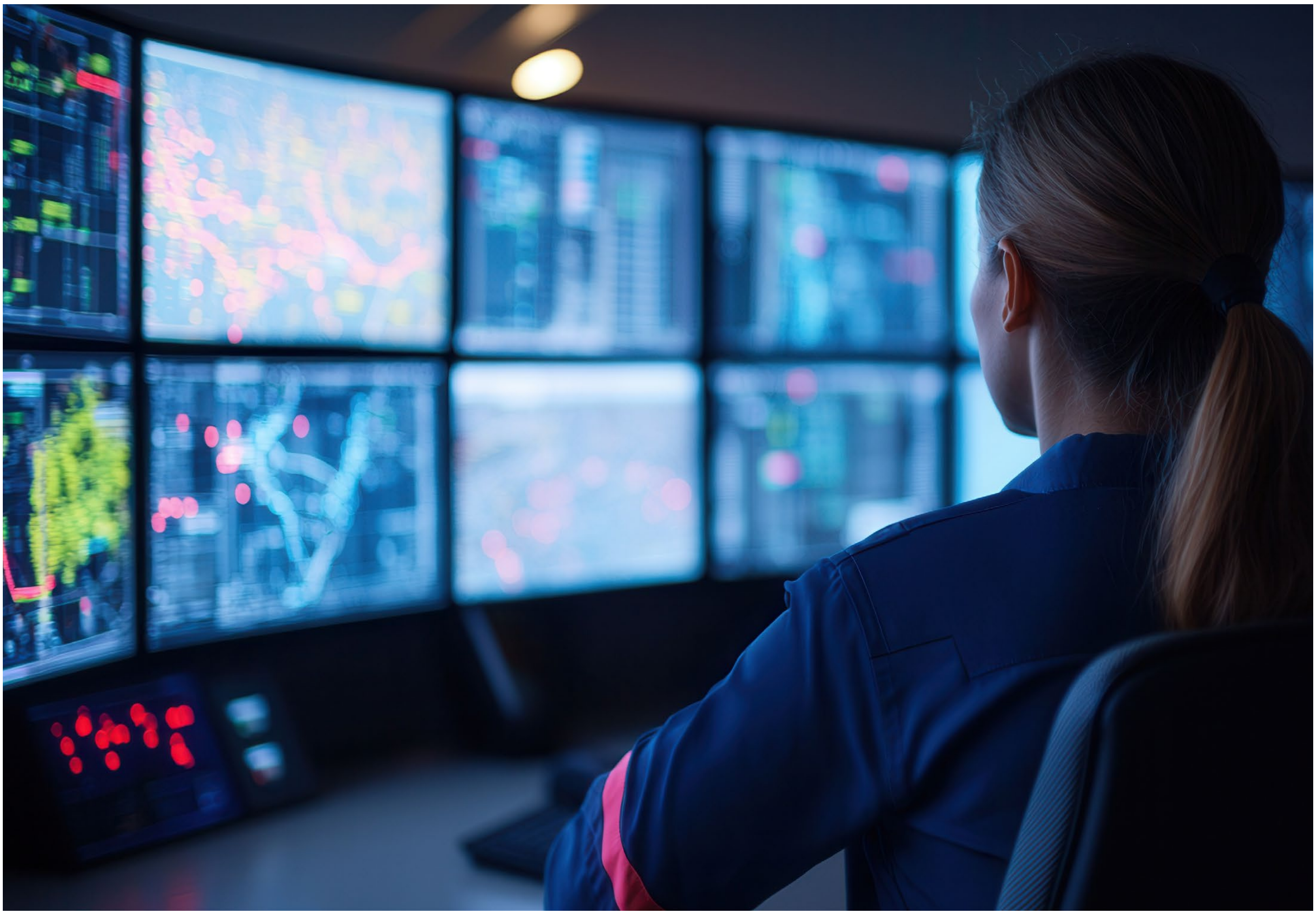
The costs of continued inaction in the face of a more dangerous world must be framed in economic terms. Private sector organisations are increasingly the direct targets of hybrid warfare such as cyberattacks, disinformation, espionage, and the targeting of critical infrastructure. It was noted by a senior representative from a leading European think-tank that the threat vectors continue to expand. Now private sector organisations and critical infrastructure operators are a primary target of State actors' hybrid warfare campaigns.

i. Energy

Many representatives from various areas of industry, including critical infrastructure, expressed concern about the cascading consequences of attacks on critical infrastructure, with attacks on electricity infrastructure noted as a leading concern. In a paper from 2023, the IIEA noted that as Russia's military aims in Ukraine become increasingly frustrated, it is likely that Russia would target European, including Ireland's energy infrastructure, via cyber and kinetic means.[12] While Ireland does conduct exercises on simulating cyberattacks, such as on the energy system,[13] the 2024 Chinese sponsored Volt Typhoon attempt to pre-position malware to enable an attack on the US grid system[14] highlights that State actors see energy infrastructure as a key target.

However, the emerging threat of a kinetic attack on gas pipelines or electricity interconnectors is seen to be particularly acute. This has grown in concern to many in the wake of sabotage of electricity and communications cables in the Baltic Sea by shadow fleet vessels.[15] It was noted that Ireland's transition to cleaner energy sources and to electrify heating and transport, while likely to create long-term energy security, has generated short-term risks for Ireland. One representative from the energy sector noted that moving from coal to importing gas via pipelines has increased Ireland's vulnerability at a time when gas pipelines are being targeted.

There was consensus amongst all representatives that increasing energy storage in Ireland, in the form of gas storage, will remain critical during a time of heightened geopolitical contestation. However, in this context, some representatives reiterated the importance of political leadership as many of these storage projects may be entangled in the broader challenges associated with the Irish planning system.



ii. Communications

The protection of subsea data cables and communications was a shared area of concern amongst the participants. Ireland plays a critical role in global telecommunications, with one representative from the renewable energy sector expressing that Ireland is a key 'communications node' globally. Ireland is home to over 30% of all EU data,[16] and approximately three-quarters of all subsea cables in the Northern Hemisphere pass near or through Irish waters.[17] While many data centres in Ireland would have temporary independent power supplies, up to 30% of all Irish electricity is expected to be consumed by the data centre sector by 2030.[18] Consequently, Ireland's energy infrastructure, in particular vulnerable undersea gas connections could be targeted in order to trigger communications outages throughout Europe.

The integrity of European data remains intimately connected to the security of Ireland's power system and the cables which transport that data. While representatives from the subsea communications cable sector did express that the majority of subsea cable outages are the result of accidents or negligence, they did acknowledge the increased geopolitical risk. Importantly, representatives from the subsea cable industry noted that severe outages to subsea cable infrastructure caused by sabotage at sea or on land have the potential for significant cascading effects throughout the Irish economy and daily life due to internet outages.

iii. Port and Food Security

Amongst the many risk vectors identified, the risks being posed in the maritime domain to Ireland's society and prosperity are seen to be of a high priority to business leaders in Ireland. Participants also expressed concern at the vulnerability of Irish port infrastructure in the context of increased geopolitical contestation. One representative commented that Irish civilians would become much more aware of threats to national supply chains, and that it would be seen as an existential risk if the country ran out of essential foodstuffs and commodities. It was noted in particular that Dublin Port represents a significant single point of failure in the national supply chain, and that food would start to disappear from shop shelves within three days if there was a material adverse event there.

iv. Cybersecurity

In addition to the above risks to critical infrastructure identified by leaders in the private sector as not only exogenous threats to their organisations, but threats to Ireland's wider society and prosperity, many of those same leaders noted concerns around direct risks to their own business particularly from cyber and espionage. Cyber risks to Irish organisations have been well documented, with almost 90% of Irish companies hit by disruption or financial loss due to cyberattacks.[19] Yet, much of this emphasis has been on the impact of cybercrime, rather than geopolitically motivated cyberattacks which can have an immediate and lasting impact on areas as diverse as our health services, utilities, internet and social media availability, and our ability to purchase basic foodstuffs.

While less publicised, many of the attendees from sectors such as financial services, aviation leasing, communications, and others all expressed concern or reported incidents regarding state-backed cyberattacks. A representative from the banking sector noted huge concerns that Russia would escalate its cyber activity in response to being removed from the SWIFT payments system in 2022. One representative from a leading financial services organisation spoke of concerns related to large amounts of financial crime emerging from North Korea to fund the North Korean Government – likely including its military operations in Ukraine. Another representative from the aviation leasing sector spoke on how they had to increase their own cybersecurity stance in response to Russia's war of aggression against Ukraine, and Russia's seizure of a number of aircraft owned by an Irish organisation, AerCap.[20] This had operational consequences for this organisation including a need to dedicate resources, invest in new technologies, and to reduce their public facing image. While cyber criminals continue to be a leading risk vector for private sector organisations, many are feeling increasingly vulnerable to geopolitical cyber risks, draining resources and capacity in these organisations. Given the sophisticated nature of the resources available to State-backed hacking organisations, private sector organisations, particularly those operating essential services, will require greater support from Government to mitigate against these risks.

v. Espionage

Many representatives during the roundtable discussion expressed concern over the growing espionage risks which private sector organisations are facing. It is well-documented that the intelligence agencies of the Russian Federation and China are interested in Ireland, and the organisations that reside here. Vice Admiral (Ret.) Mark Mellett, former Chief of Staff of the Irish Defence Forces, expressed real concern about the possibility of Russian and Chinese spies targeting Irish technology organisations at the Global Economic Summit in May 2025.[21] Although receiving less public attention, a number of private sector organisations expressed concern in relation to increased targeting by overseas intelligence services. One representative from the technology sector highlighted that they have had to increase their awareness about the potential risk posed by intelligence agencies from Russia, China, India and others attempting to place operatives in their organisations. While these activities exist at the lower end of espionage risk, assassination plots of leading European business leaders, such as the CEO of a leading German defence company supporting Ukraine,[22] have been reported. With large numbers of organisations in Ireland directly involved in countering Russian cyber threats in Ukraine, implementing sanctions on Russian officials, and involved in countering disinformation, it is not outside the realm of possibility that there could be threats to those organisations or their people. Many of the representatives expressed a clear desire for increased engagement with the State's intelligence services to better navigate the risks posed by foreign intelligence operatives attempting to target Ireland.

'A Generational Opportunity': Unlocking Opportunities during a Time of Crisis

"Over all of this, we have a reputational issue amongst our partners. We have to be seen to be pulling our weight for ourselves, but also being able to contribute something to Europe."

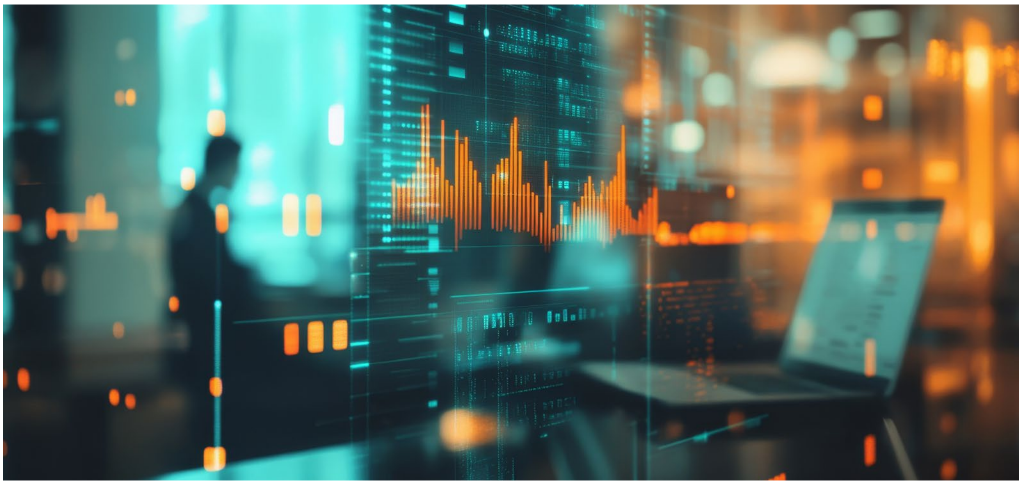
Roundtable Participant

i. Opportunities for Ireland emerging from increased defence spending

Increased investment in defence and national security at European level presents opportunities for Irish organisations to play a vital role in protecting European citizens, while also providing growth and employment. While the opportunities are great, significant obstacles for Ireland and Irish organisations persist.

For context, the EU's ReArm Europe Plan proposes to enable an additional €800 billion of defence spending by 2030. This plan is comprised of three pillars, enabling greater fiscal flexibility for Member States which is expected to create nearly €650 billion of additional funding; launching the Security Action for Europe (SAFE) instrument, a €150 billion fund which would provide long-term loans to enable investment in areas of key strategic interest from cybersecurity to missile defence; and finally supporting the European Investment Bank in broadening its lending to defence and security projects, and using the opportunities presented by completing the Savings and Investment Union to mobilise private capital.[23] In addition, the European Commission seeks to allocate €131 billion to support investment in defence, security, and space in the EU's next seven-year budget (2028-2034), the Multiannual Financial Framework (MFF), a fivefold increase from the previous budget.[24]

This unprecedented level of funding presents significant opportunities for Irish organisations working with dual-use technologies such as cybersecurity, robotics, AI, radar, satellites and other technology organisations to not only access substantial financial support, but to play a leading role in keeping Ireland and Europe safe. While Ireland may not host the large 'defence primes' found in other EU countries, this may actually give Ireland distinct competitive advantage over other EU Member States. As one representative from a dual-use technology company mentioned, Ireland does not have a 'defence prime'. Consequently, in the context of the ReArm Europe plan, much of its emphasis on cybersecurity, artificial intelligence, robotics, and advanced manufacturing, and other areas which agile organisations tend to perform better, means that Ireland does not have to contend with the embedded practices that may hamper other countries with more established defence companies. Therefore, Irish organisations and SMEs may be well positioned to benefit from this unprecedented spending, providing innovation, employment, and prosperity, while protecting their fellow citizens.



ii. Savings and Investment Union: An opportunity for Ireland to lead in Europe's Defence

While the opportunities presented by the Savings and Investment Union for Europe are known more generally, Ireland is well positioned to play a significant role in facilitating capital allocation to benefit European security and defence in this context. The Savings and Investment Union (SIU), an EU initiative to integrate Europe's capital markets and banking system to better allocate investment in European enterprises while providing better returns for European savers,[25] is a core pillar of how Europe plans to fund the long-term research, development, and innovation in defence, as well as in funding new manufacturing facilities. Playing host to nearly €5 trillion of assets, it was noted by a senior member of a multinational financial services institution that Ireland could be positioned to play a leading role in mobilising private investment to fund Europe's defence ambitions.

Domestically, Ireland's funds industry has the administrative, auditing, and legal talent as well as the structures and facilities to domicile new defence investment vehicles should they be created. Ireland's fund industry already has experience in implementing ESG-compliant strategies. Signals in changing ESG regimes directed by the European Commission's changes to the Sustainable Finance Disclosure Regulation (SFDR)[26] and European Investment Bank (EIB)[27] to better incorporate defence could enable Ireland's funds sector to become a leader in responsible defence investments.[28] As a key gateway in European capital flows, Ireland's funds sector would likely end up playing an outsized role in administering long-term investments in European defence capabilities such as new ammunition production facilities, as well as administering financial vehicles for defence start-ups. Irish policymakers have a unique opportunity to promote Ireland as a place to domicile new financial vehicles for European defence yet may need to adjust legislation to provide greater regulatory clarity for Ireland's financial services sector and encourage funds administrators to no longer voluntarily exclude security investments from their funds. Cumulatively, Ireland's key role in European funds could enable policymakers in making a case to European counterparts that it wishes to play its part in European defence through becoming the place for defence capital flows in the EU, and to utilise its existing good reputation to attract global investors, thereby improving Ireland's reputation and building new opportunities for an industry critical for Ireland's economic prosperity.

iii. Unlocking Enablers

The opportunities for Irish organisations to not only play a leading role in helping to secure Europeans from danger, but to also benefit Irish innovation and prosperity, are significant. Yet, barriers to Ireland unlocking these opportunities create risks. Ireland is the second largest per-capita contributor to the EU budget, Irish tax-payers are and will be contributing to these initiatives and funds. One representative from the dual-use sector noted that Ireland's contribution to these initiatives and funds will be very material in financial terms. A reluctance to remove obstacles or to fully engage with these initiatives will simply lead to a scenario where the Irish taxpayer will be subsidising the defence industries of other Member States, with little to no benefit to Ireland's own economy. Overall, senior politicians will be left with a choice. Either to engage with these initiatives and provide the conditions for Irish organisations to contribute to and benefit from them, or to continue with the status quo, miss the opportunities which this unprecedented expenditure provides, while paying for others.

Representatives from industry noted that Enterprise Ireland and the IDA are unable to support organisations in the dual-use space. At present, the Science and Technology Act, 1987, section 8 (5) limits Enterprise Ireland from engaging in or promoting activities with a 'primary military relevance' without the approval of Government.[29] Of note is that Ireland has no dual-use strategy, while similar agencies in Northern Ireland have clear direction and strategies from Government.[30] A representative at one of the roundtables noted that Ireland is losing investment opportunities because of these legal prohibitions and lack of political coherence in critical areas such as cybersecurity and cyber defence. Government should consider the implications of existing legislation for dual-use sectors and should provide policy coherence and direction in the form of a strategy to enable certainty for agencies such as the IDA and Enterprise Ireland.

Another critical enabler which recurred throughout the discussions was Ireland's lack of security clearance architecture. This was seen by representatives from academia, the dual-use sector, Government, and critical infrastructure as a persistent obstacle to information sharing, and critically for industry to be able to engage in EU-funded projects. One representative working in Ireland's space sector outlined the challenges in accessing funding due to the lack of security clearance infrastructure in the State. This was also reported by academics attempting to access EU grants with defence applications, and by organisations working in the dual-use sector.

The lack of security clearance also limits the ability to share information amongst key stakeholders. Industry has access to data that is of vital importance to the State, while the State could, when necessary, share information to protect private sector organisations against hybrid activity such as cyberattacks and espionage.[31] Developing the ability to provide vetting for persons or entities would provide the basis for greater transparency and exchange of vital information to truly enable a whole-of-society level of security. In 2023, Government announced the creation of a National Security Agency responsible for the issuing of security clearances for non-government persons and the classification of materials.[32] Ongoing work by the Department of Justice, Home Affairs and Migration towards establishing the Authority was welcomed.

Conclusions and Recommendations

"Not only are we heading for war in Europe, but we are heading for a war Europe might lose"

Roundtable Participant

Against a backdrop of a deteriorating geopolitical landscape and the consequences of war in Europe being felt by many, Ireland is at an inflection point. Difficult choices will have to be made. The growing deployment of the tools of hybrid warfare including disinformation, espionage, sabotage, assassination plots, and attacks on critical infrastructure by hostile States put Ireland's social wellbeing, economic prosperity, and the lives of individuals at risk.

It is now widely accepted that Ireland cannot continue with an incremental approach to national security and defence, while maintaining a reputation as a good partner in Europe, and as a safe and stable place to do business. We are at a watershed moment in European security, and there has been a paradigm shift as to how Ireland's European friends and partners approach defence. Ireland's defence deficits are increasingly being noted internationally,[33] leading to a growing perception that Ireland is putting our own security and the security of our neighbours at risk. As the mood-music in Europe shifts, and the levels of ambition of our partners regarding defence increase, Ireland will have to ensure that it stays in tune. Rapid and agile transformational change is essential to maintain our reputation and relevance.

Roundtable participants and other interviewees recognised Government's efforts around defence and security, particularly in the light of other domestic challenges such as housing and infrastructure. For example, increased defence spending, progress towards Level of Ambition 2 with a further aspiration to move to Level of Ambition 3, increased investment in the National Cyber Security Centre (NCSC), implementation of the Critical Entities Resilience Directive and other measures were all noted as progressive achievements.

Moreover, the private sector, while expecting the State to lead in the area of security, wishes to play an active role by sharing its knowledge and expertise via trusted fora, and participation in scenario planning and simulation exercises. Roundtable participants noted that the State relies heavily on the private sector for critical infrastructures and services; and in a time of national emergency a highly joined up approach between Government and the private sector is essential.

For Irish companies and SMEs that operate in the defence, security and related sectors, they want to likewise contribute, but at the same time leverage the economic benefit of increases in national defence budgets, increased funding from the European Union, as well as growing private sector investment in defence.

National dialogue on basic national security, defence and resilience needs to be decoupled from discourse on neutrality. Indeed, participants were clear that neutrality means Ireland as a nation has to be able to identify threats to our security, provide an appropriate level of deterrence, and if necessary, defend effectively against these threats.

Below, we have set out a number of recommendations based around three core themes from the roundtable discussions and subsequent interviews. Underpinning the development of these recommendations are the key principles that national security and resilience are inextricably linked to Ireland's economic prosperity and societal wellbeing; that a whole-of-government / whole-of-society approach is both optimal and essential; and given the speed of international developments, time is of the essence.

It is also noted that work in relation to some of the recommendations is underway across Government, and that further analysis and assessment of other recommendations may be required before progressing. In the spirit of the roundtables they are presented as constructive contributions to the debate on national security, defence, and resilience.

Theme 1. Leadership and Direction

In order to protect our nation and society, clear direction and leadership is critical.

Recommendation 1 – Expedite the Development of a National Security Strategy.

Ireland has developed a number of security strategies to date, including the National Cyber Security Strategy, while the development of a National Maritime Security Strategy is currently underway. While the existence of these sectoral strategies is of critical importance, enabling the allocation of resources to counter threats in specific domains, these strategies currently reside separately within the auspices of the Department of Justice, and the Department of Defence respectively. An overarching National Security Strategy would serve to create greater direction, alignment, and synergies between existing and future strategies pertaining to security and resilience. A National Security Strategy would enable the State to examine the threats it faces in their totality, increasing the ability of the State to take a whole-of-government approach to security and break down silos. The development of this Strategy would also present a critical opportunity for the creation of clear governance frameworks for all of the agencies and departments with a national security function. Importantly, this allocation of responsibilities and accountabilities would enable a greater degree of coherence between the State's national security architecture, avoiding duplication of efforts, enable a greater sharing of resources and capabilities, and lead to greater efficiencies in the ability of the State to respond to Ireland's diverse threat environment.

Finally, the process of developing the strategy, the consultation process, and the ultimate publication of a National Security Strategy could serve as a potential lodestar, providing a trusted source to continue Ireland's national conversation on security and defence.

Recommendation 2 - Need for political leadership and alignment.
Many roundtable participants noted the significantly increased political and media dialogue on national security and defence in recent months, and the leadership shown at senior Government levels. It was noted that the previous practices of avoiding questions on defence and national security as ‘too difficult’ are no longer adequate for Ireland’s changed security environment. Participants were clear that politicians across the spectrum need to provide leadership and act decisively in order to enable the diverse range of responses required to meet the scale of the challenges which the State faces.

Recommendation 3 – Enhance support capacity and capability at Government level.
Many business representatives expressed a clear desire for greater resourcing of Government departments and agencies, and the building of additional capability and capacity to address and advise on Ireland’s national security challenges. While noting that there are many good people with deep expertise across Government, they are insufficient in number. As the range of threats which the State faces continues to increase or diversify, and emphasis on resilience and preparedness grows, Ireland could, for example, increase the resourcing of the Office of Emergency Planning, enabling it to play a greater role coordinating and preparing for national responses to crises.

Theme 2. Building a whole-of-government / whole-of-society approach to security

It is important that a national dialogue around national security and defence continues and evolves engaging all of Government and society.

Recommendation 4 - Government should examine means to increase public awareness and build a shared understanding of the threats which Ireland faces.

Government should seek to communicate clearly and directly the type and scale of threats which Ireland's society faces, in particular with regard to disinformation campaigns and hybrid warfare and their potential or real impacts on people's daily lives. Building a shared understanding of the threats to Ireland's people will play a critical role in developing societal resilience in the face of increased hybrid attacks against critical infrastructure, including energy and communications infrastructure. For example, Government and the Office of Emergency Planning could consider adapting Sweden's 'In Case of Crisis or War' pamphlet which includes information on hybrid threats, psychological risks to geopolitical uncertainty and disinformation, as well as what citizens can do to keep themselves and their loved-ones safe should a crisis, such as a severe electricity outage, occur.

Recommendation 5 – Enhance the support to and dialogue with the private sector from the State's security architecture.

While the risks to nation States in Europe are well documented, the private sector is also increasingly being targeted, often as a means to create fear and anxiety within society. This targeting ranges from cyberattacks and intellectual property theft. As noted previously the State is in many cases dependent on the private sector for the provision of critical infrastructures and services and so incidents of sabotage, including the cutting of undersea cables, destruction of train lines and arson attacks impact too. The private sector should be aware of these risks and supported in their efforts to mitigate against them through routinised contact with, and education and briefings from, the State's security architecture. In particular, the private sector wants to play an active role in the security of the State and social wellbeing by sharing their expertise. Enhancing the existing means of engagement and deepening the partnership between public and private sector can produce a win-win scenario, augmenting the preparedness of both groups, and increasing the resilience of Ireland's society to hybrid threats as a whole.

Recommendation 6 - Fostering and maintaining peer-to-peer relationships, in particular between public and private sector stakeholders.

Throughout the discussions and interviews, the importance of peer-to-peer relationships were expressed as key to preparing for a crisis and building societal resilience. Knowing who to call, and being familiar with that person before a crisis was viewed as crucially important by representatives from the private sector and Government. Citing positive experiences, a desire for an increase in the number of joint exercises and simulations such as – but not limited to – those conducted via the National Emergency Coordination Centre (NECC) was expressed by a number of representatives from the private sector at the roundtables, and from security representatives interviewed. Academic institutions and think-tanks could also play a role in facilitating simulations or table-top exercises. In addition, it was noted that these exercises and the creation of contact groups also play a key role in developing person-to-person relationships enabling easier communication and familiarity during times of crisis. This approach would be consistent with a whole-of-government / whole-of-society approach where each stakeholder knows their respective roles and responsibilities.

Theme 3. Unlocking opportunities for Ireland

Significantly increased defence spend and related EU initiatives were noted as an opportunity for Irish companies and SMEs to contribute capability and technologies, and leverage the economic benefit for Ireland.

Recommendation 7 - Government should examine the development of a strategy to support Ireland's defence industry / dual-use sector.
Ireland has a growing technology sector which could play an important role in maintaining Europe's technological edge and supporting Ireland's national security and defence.

A 'Defence Industry Strategy' could seek to examine how Ireland can engage with the EU's European Defence Industrial Strategy (EDIS) and the European Defence Industrial Programme (EDIP), the latter of which allocates €1.5billion to boost investment in Europe's defence industry.[34] In addition, this Strategy could examine ways and means for the State to responsibly support Irish SMEs engaged in the dual-use sector, to remove obstacles to their success.

This Strategy could examine a whole-of-government approach to supporting Ireland's defence / dual-use sector, including coordinating the Department of Enterprise, Tourism, and Employment, Enterprise Ireland; and the IDA, with the needs of the Irish Defence Forces; the Department of Defence; the National Cyber Security Centre; and An Garda Síochána.

Recommendation 8 - Expedite the creation of a security clearance system for non-government officials.
The ongoing work by the Department of Justice, Home Affairs and Migration towards establishing a new statutory National Security Authority (NSA) to provide a security clearance system for commercial entities and their personnel is welcome.[35] While it was recognised that interim arrangements apply, a clear need for a formalised system was noted by roundtable participants. It is believed to be of vital importance that this process is expedited. The lack of an official security clearance system for non-government officials presents a significant obstacle to investment in Ireland's dual-use sector. This lack of security clearance architecture can also hinder Irish dual-use SMEs from accessing EU funding such as the European Defence Fund, an €8 billion defence research fund[36]; and limits the ability of non-government officials such as academics and businesspeople from attending classified briefings and from engaging in academic projects with a military application funded by the EU. With Ireland's upcoming EU presidency likely to create increased exposure and opportunities for Irish SMEs, this gap may be further exacerbated. Ireland contributes to many of these funds via its contributions to the EU budget, with the implicit risk that Ireland is subsidising the industries of other EU Member States, while simultaneously restraining its own companies.

Recommendation 9 - Amend the Science and Technology Act, 1987, section 8(5) to remove the restrictions placed on Enterprise Ireland's engagement with Ireland's dual-use sector.
This would provide greater clarity for Enterprise Ireland in supporting dual-use SMEs in availing of State, EU and private funding, thereby enabling Irish dual-use SMEs to scale and to support indigenous European defence capabilities, Irish enterprise, and Ireland's prosperity.

Recommendation 10 - The Savings and Investment Union (SIU) provides a generational opportunity for Ireland to play a constructive role in European Security.
In its ReArm EU plan, the Savings and Investment Union functions as one key pillar for how Europe will fund defence research and innovation, investment in manufacturing facilities, and in developing new capabilities to counter security threats.[37] Ireland's significant role in the financial services sector, with €5 trillion of assets domiciled in the State, may provide significant opportunities to play a leadership role in allocating capital to ensure that Europe can develop the capabilities it needs to protect European citizens. As a key gateway in European capital flows, Ireland's funds sector could have an important role in administering long-term investments in European defence capabilities, as well as providing start-up capital for emerging defence enterprise. With security now increasingly compatible with ESG frameworks due to direction from the European Investment Bank and the European Commission, Irish policymakers may need to adjust legislation to provide greater regulatory clarity for Ireland's financial services sector and to encourage funds administrators to no longer automatically exclude security investments from their funds.

End notes

01. The Chatham House Rule refers to a spirit of sharing information where participants are free to use the information received, but neither the identity nor the affiliation of the speaker, nor that of any other participant can be revealed.
02. Laura Sharman 29 September 2025 Denmark, rattled by mysterious UAV sightings, bans drone flights ahead of European Union summit. CNN World.
03. Martin Wall, Conor Galagher, and Jack Power 8 November 2025 Ireland may seek aid of French warship to boost security during EU presidency. The Irish Times.
04. Commission on the Defence Forces 2022: 154 Report of the Commission on the Defence Forces.
05. Swedish Civil Contingencies Agency 2024 In Case of Crisis or War.
06. Swedish Civil Contingencies Agency 2024: 22 In Case of Crisis or War.
07. Paul Reynolds 23 May 2021 The anatomy of the health service cyber attack. RTE.
08. Cian FitzGerald 31 March 2022 The Gray Zone Ireland in an Era of Renewed Great Power Competition. IIEA.
09. Romina Bandura and Thomas Bryja 23 July 2025 The Strategic Future of Subsea Cables: Ireland Case Study. CSIS.
10. Conor Gallagher 19 November 2025 Russian spy ship on course for Irish waters, with UK threatening ;military options'. The Irish Times.
11. Paul Reynolds 5 August 2024 Russia is one of the countries spying in Ireland – Assistant Commissioner. RTE.
12. Cian FitzGerald 2023 Black Swans in the Gray Zone: Defending Ireland's Energy System Against Cyber Threats. IIEA.
13. Garreth MacNamee 24 November 2022 National Cyber Security Centre carries out mock attack on nationa's energy infrastructure system. The Journal.ie.
14. Cybersecurity and Infrastructure Security Agency 7 February 2024 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure.
15. Richard Milne and Chris Cooke 11 August 2025 Finland charges captain of Russia 'shadow fleet' ship over cable cutting. Financial Times.
16. National Cybersecurity Centre 2019: 8 National Cybersecurity Strategy 2019-2024.
17. Romina Bandura and Thomas Bryja 23 July 2025 The Strategic Future of Subsea Cables: Ireland Case Study. CSIS.
18. Oonagh Smyth 21 August 2025 Government warned of rising household bills as data centres strain grid. RTE.
19. Ciara O'Brien 4 April 2025 Almost 90% of Irish companies hit by disruption or financial loss due to cyberattacks. The Irish Times.
20. Alistair Gray, Sylvia Pfeifer and Lee Harris 11 June 2025 Worlds biggest aircraft owner set for $1bn payout in Russian planes case. Financial Times.
21. Daniel McConnell 28 May 2025 Watch: 'Irish tech security is being targeted by China and Russia... we need to wake up' BusinessPost.
22. Reuters 11 July 2024 Russia tied to assassinate CEO of German arms firm sending weapons to Ukraine, reports say. Reuters.
23. European Commission Acting on Defence to Protect Europeans.
24. European Commission The 2028-2034 EU budget for a stronger Europe.
25. European Commission Savings and Investment Union Factsheet.
26. European Commission 20 November 2025 Commission simplifies transparency rules for sustainable financial products [press release].
27. European Investment Bank Strengthening Europe's Security and Defence Industry.
28. Lloyd Collier 4 October 2025 Defence and Dual-Use Technology Investment: The Evolving Role in Ireland's Funds Industry. JTC Group.
29. Irish Statute Book Science and Technology Act 1987, Section 8. :
30. UK Ministry of Defence 8 September 2024 Defence Industrial Strategy 2025: Making Defence and Engine for Growth.
31. Cian Fitzgerald 2023 Black Swans in the Gray Zone: Defending Ireland's Energy System Against Cyber Threats. IIEA.
32. Conor Gallagher 3 March 2023 Agency to handle security clearances and classification of sensitive information set to be established. The Irish Times.
33. Marcus Solarz Hendriks and Harry Halam 5 February 2024 Closing the Back Door: Rediscovering Northern Ireland's Role in British National Security.
34. European Commission 2024 European Defence Industry Programme Factsheet.
35. Jim O'Callaghan 2 July 2025 National Security. Dail Eireann Debate, Wednesday – 2 July 2025. Houses of the Oireachtas.
36. European Commission EDF | Developing tomorrow's defence capabilities.
37. European Commission Acting on Defence to Protect Europeans.

Bibliography

01. Bandura, Romina and Thomas Bryja 23 July 2025. The Strategic Future of Subsea Cables: Ireland Case Study. CSIS.
02. Collier, Lloyd 4 October 2025. Defence and Dual-Use Technology Investment: The Evolving Role in Ireland's Funds Industry. JTC Group.
03. Cybersecurity and Infrastructure Security Agency 7 February 2024. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure.
04. European Commission Acting on Defence to Protect Europeans.
05. European Commission 20 November 2025 Commission simplifies transparency rules for sustainable financial products [press release].
06. European Commission EDF | Developing tomorrow's defence capabilities.
07. European Commission 2024 European Defence Industry Programme Factsheet.
08. European Commission Savings and Investment Union Factsheet.
09. European Commission The 2028-2034 EU budget for a stronger Europe.
10. European Investment Bank Strengthening Europe's Security and Defence Industry.
11. FitzGerald, Cian 2023. Black Swans in the Gray Zone: Defending Ireland's Energy System Against Cyber Threats. IIEA.
12. FitzGerald, Cian 31 March 2022. The Gray Zone Ireland in an Era of Renewed Great Power Competition. IIEA.
13. Gallagher, Conor 19 November 2025. Russian spy ship on course for Irish waters, with UK threatening 'military options'. The Irish Times.
14. Gallagher, Conor 3 March 2023. Agency to handle security clearances and classification of sensitive information set to be established. The Irish Times.
15. Gray, Alistair; Pfeifer, Syvia; and Harris, Lee 11 June 2025 Worlds biggest aircraft owner set for $1bn payout in Russian planes case. Financial Times.
16. Hendriks, Marcus Solarz and Halam, Harry 5 February 2024. Closing the Back Door: Rediscovering Northern Ireland's Role in British National Security.
17. Irish Statute Book Science and Technology Act 1987, Section 8.
18. MacNamee, Garreth 24 November 2022. National Cyber Security Centre carries out mock attack on nation's energy infrastructure system. The Journal.ie.
19. McConnell, Daniel 28 May 2025. Watch: 'Irish tech security is being targeted by China and Russia... we need to wake up'. BusinessPost.
20. Milne, Richard and Cooke, Chris 11 August 2025. Finland charges captain of Russia 'shadow fleet' ship over cable cutting. Financial Times.
21. National Cybersecurity Centre 2019. National Cybersecurity Strategy 2019-2024.
22. O'Brien, Ciara 4 April 2025. Almost 90% of Irish companies hit by disruption or financial loss due to cyberattacks. The Irish Times.
23. O'Callaghan, Jim 2 July 2025 National Security. Dail Eireann Debate, Wednesday – 2 July 2025. Houses of the Oireachtas.
24. Reynolds, Paul 5 August 2024. Russia is one of the countries spying in Ireland – Assistant Commissioner. RTE.
25. Reynolds, Paul 23 May 2021. The anatomy of the health service cyber attack. RTE.
26. Reuters 11 July 2024. Russia tied to assassinate CEO of German arms firm sending weapons to Ukraine, reports say. Reuters.
27. Sharman, Laura 29 September 2025 Denmark, rattled by mysterious UAV sightings, bans drone flights ahead of European Union summit. CNN World.
28. Smyth, Oonagh 21 August 2025. Government warned of rising household bills as data centres strain grid. RTE.
29. UK Ministry of Defence 8 September 2024 Defence Industrial Strategy 2025: Making Defence and Engine for Growth.
30. Wall, Martin; Gallagher, Conor;, and Power, Jack; 8 November 2025 Ireland may seek aid of French warship to boost security during EU presidency. The Irish Times.

About the Authors

Cian FitzGerald (Principal Investigator) is a Senior Researcher at the IIEA, specialising in Defence and National Security Policy. His research focuses on hybrid warfare, societal resilience and the role of the private sector in national defence planning. Additionally, he works on EU Common Security and Defence Policy (EU CSDP), and matters pertaining to Ireland’s national security. In 2023, Cian 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.

Dr Barry Colfer 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 spent two years in student politics studied at University College Dublin and he 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 the consequences of Brexit for Ireland. Barry is a fellow of the UK Royal Society of the Arts (RSA).

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.

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

IIEA
Sharing Ideas
Shaping Policy

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

Deloitte.

Together makes progress

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with over 450,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients.

In Ireland, Deloitte has over 3,000 people providing audit, tax, consulting, financial advisory, and risk advisory services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients taking them wherever they want to go.

This document has been prepared by Deloitte Ireland LLP for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte Ireland LLP to supply the proposed services.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment and no reliance may be placed for any purposes whatsoever on the contents of this document.

Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC001499 and its registered office at The Ewart, 3 Bedford Square, Belfast, BT2 7EP, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

The Deloitte Ireland LLP privacy notice is available at www.deloitte.ie/privacy