Address by Dr Barry Colfer and Cian Fitzgerald (IIEA) to the Oireachtas Joint Committee on Foreign Affairs and Defence on *'Hybrid threats and threats to the national infrastructure',* 09 May 2023, 3.15pm

Opening remarks by Dr Barry Colfer, Director of Research at the Institute of International and European Affairs (IIEA).

Good afternoon and thank you for the opportunity to address this committee.

The IIEA is a public policy and international affairs think tank in Dublin.

Through a coordinated programme of research and events, we seek to contribute to public discourse across a wide range of matters and subjects that are of public interest.

This relates to, but is not limited to, EU policy and relations, economics, digital policy, development matters, climate & energy policy, foreign policy, health policy, justice policy, disability policy, UK-Irish relations, and security & defence policy to make a few.

Within the IIEA's security & defence programme, we consider issues including: the EU as a security actor, the future of defence capability, future force design, and the implications of all this for how conflicts happen and wars are fought.

This work also relates to the changing character of warfare, including the use of artificial intelligence (AI), drone technology, quantum computing, the future of nuclear proliferation and more.

Our security & defence programme resides within the broader geopolitical context that all of our work relates to, including: Russia's war in Ukraine, EU-UK relations following the UK's withdrawal, the future of NATO, the scramble for rare earth metals and scarce resources, the rise and repositioning of China and India, the politics of and relations with Africa, climate change, populism, demographic change and much more.

Given our particular interest in Irish-EU relations, and the future of the EU and Ireland's role within it, the changing security & defence context within the EU and its neighbours is particularly salient for our work in this area, and raises questions relating to relations with the UK and NATO, the EU's attempt to be a security actor (through, for example, the promulgation of the EU's Strategic Compass, essentially the EU's Security Strategy), and how the resources of the Ukraine's forces can be replenished.

Our recent IIEA paper that Cian Fitzgerald will present now -Black Swans in the Grey Zone: Defending Ireland's Energy System Against Cyber Threats – examines the threat posed to critical energy infrastructure and Irish society by hostile cyber activities. As Russia's armed forces continues to get bogged down in its war against Ukraine, Russia may increasingly seek to utilise other means to achieve its political aims by targeting European states such as Ireland.

In this context, the Russian Federation may increasingly seek to undermine Western support for Ukraine through the use of Grey Zone activities – that is to say, the spectrum of threats that operate above the threshold of normal global politics, but that falls short of kinetic warfighting - such as cyberattacks on services crucial for the normal functioning of society in Europe. Ireland, due to its importance in global technology and communications coupled with its limited defence capabilities, may be a target of this form of aggression.

This paper explores how Russia conducts cyberwarfare operations, often cloaking them so that they appear to be run of the mill cybercriminality, and the threat that it poses to Ireland's energy infrastructure and society.

Finally, this paper examines how Ireland could enhance its resilience against these attacks using a whole-of-society approach to national defence which could enhance the ability of the State to respond to, and deter, Grey Zone aggression.

We hope that a discussion and better understanding of this topic can help to inform a debate in Ireland regarding future security and defence policy.

Remarks by Cian FitzGerald, Security and Defence Researcher, IIEA

Good afternoon, it is a pleasure to be here to share the IIEA's work on hybrid and Grey Zone threats to Ireland. At the outset, I would like to state that Ireland's national security is the basis for its national and social prosperity. However, at present, we are seeing the rise of a growing type of threat to our security and prosperity – one which you may be familiar with already – 'Grey Zone threats' which are transnational, incremental, and operate below-the-threshold of conventional conflict and which do not respect borders, sovereignty, or delineations between civilian and military targets.

Since December of 2022, the IIEA has been conducting a project that reflects on the changing character of warfare as a consequence of increasing international competition and tensions. Notably, revisionist actors such as the Russian Federation, who are dissatisfied with the present geopolitical status quo and seek to tilt the balance of power in their favour at the expense of European states, are using a variety of instruments generally understood to be 'Grey Zone' techniques. The Grey Zone as a concept is the spectrum of hostile and aggressive activities which exists above the peaceful normal activity of international politics but below the threshold of kinetic warfighting. They are generally low cost and low risk for the perpetrator but have a significant destabilising effect on the target state and its society. Grey zone activities include the use, either in isolation or combination, of disinformation, election interference, espionage, intellectual property theft in key industries such as defence, life-sciences and technology – but it also includes the use of military manoeuvres designed to intimidate target states such as was planned in February 2022 or cyberattacks designed to disrupt the normal functioning of society such as the attack on the HSE in 2021. Though occasionally, some of the more high-intensity forms of Grey Zone activities do attract headlines, these forms of activities are designed to be incremental and difficult to detect with

the overall goal of changing the strategic landscape before the target state has realised what is happening. They are designed to sap the political and economic strength of the target state, to undermine social cohesion, and ultimately to leave them unable to respond to the revisionist states increasingly assertive international posture.

Moreover, we expect to see a greater proliferation of the use of Grey Zone activities against European states – in particular those originating from the Russian Federation in connection to its war in Ukraine. Activities such as cyberattacks, and most recently the reported presence of Russian vessels mapping cable infrastructure are designed to intimidate Europeans, to highlight their vulnerabilities and most importantly to undermine European support for Ukraine.

Ireland is increasingly and demonstrably at risk of such Grey Zone activity. Its ever-growing role in the interconnected economies of the Euro-Atlantic area, its importance in global technology and communications, its position in the EU and its relative diplomatic power, coupled with its limited capacity to protect itself makes it a prime and under-defended target.

Russia has shown its willingness and preference for targeting civilian critical infrastructure as part of its Grey Zone campaigns to maximise disruption in target societies. I think what should be clear is that not only is the monetary cost of state backed cyberwarfare operations high, but the potential societal cost in terms of loss of confidence in the State's ability to protect its citizens from harm is significant. As a second order consequence of cyber-attacks, the effect on public trust in institutions could also leave societies more vulnerable to the disinformation campaigns which often accompany these types of attacks.

Cyber and the Electricity Grid

The paper published by the IIEA, *Black Swans in the Grey Zone,* which was circulated in advance of today's discussion, focuses on threats posed to Ireland energy infrastructure as a part of Grey Zone activity. Examining the potential escalation trajectory, we believe that it is possible that as Russia military campaign continues to stall – in particular as it faces increasing amounts of western supplied military hardware - the Russian Federation may choose to carry out cyberattacks against electricity infrastructure in Europe in order to try and erode Europe's willingness to continue to support Ukraine.

Russia has already demonstrated that it has the capability to carry out such an attack on energy grid infrastructure when in December 2014, Russia, after months of targeting and preparation, carried out a devastating cyberattack on Ukraine's power grid causing nearly a quarter of a million customers to lose power following a synchronized attack on three regional electric power distribution companies. Furthermore, the signalling from the Kremlin itself indicates that European energy infrastructure could be a target of some form of attack. In Vladimir Putin's own words, *'any critical infrastructure in transport, energy or communication infrastructure is under threat — regardless of what part of the world it is located, by whom it is controlled, laid on the seabed or on land'.*

With this in mind, the IIEA has identified that Ireland's energy grid may be a preferred target for a cyber-attack, either through repeated small-scale attacks or from a single large-scale attack. As a host to some 30% of all European data as well as cable infrastructure critical to global communications, sustained, and large-scale power outages would not only likely disrupt Irish communications, society, and undermine Ireland's image as a safe and stable place to do business, but it would also have the potential to disrupt life in other EU Member States.

Recommendations

So what options are available to us to counter Grey Zone aggression? Though most of our recommendations focus specifically on protecting Ireland's energy infrastructure, successful implementation would make Ireland's society more resilient and better protected against the broader spectrum of Grey Zone threats. As a collective, our recommendations focus on how we can either make best use of, or augment, already existing structures.

Overall, we believe that the best means of defending Ireland against this form of aggression will require a mindset shift in how we approach national security. Ultimately, as Irish businesses, resources, people and society are the targets of Grey Zone activities, the security services of the state alone are not enough to deal with these threats. Instead, it will require a whole-of-society approach to defence which includes industry, NGO's, think-tanks, academia as well as individual citizens in protecting their society from harm by antagonistic state actors.

Our first recommendation is that **Ireland could enhance its resilience through greater cooperation between the public and private sectors**. With private sector actors and government having access to different data, in what we term the **cyber security data gap,** greater information sharing between the public and private sectors when it comes to cyber incidents would be mutually beneficial.

Second, the State needs to Continue to Build awareness in critical industries about cyber risks to operational technology and their role in national security.

Thirdly, the state could enhance the resilience of Ireland's electricity grid though greater redundancy and a focus on micro-generation programmes such as the €2,400 grant for households to install solar panel. Not only would this assist the State in meeting its climate targets, but it would also enhance the State's resilience to outages which may arise from a cyber-attack against the national grid.

We should consider the development of a Threat Lead Penetration Testing Framework, modelled on the existing TIBER-EU/IE Framework for our energy system. The TIBER EU Framework, is an EU framework developed by the European System of Central Banks to stress-test individual banks readiness in case of a cyber-attack. Intelligence on cyberthreats and best practices are shared across the framework's EU network. Such a framework for the energy system would enable operators in Ireland to stress-test their ability to respond to cyber-attacks in a systematised and regularised approach.

Our fifth recommendation is that Ireland should develop its Intelligence capabilities to counter hybrid threats. At present, Ireland's intelligence capacities are not in line with comparator countries. In short, they are insufficient for the present hybrid threat environment. By developing the state's intelligence capacities, both in the Defence Forces and An Garda Siochana, the State would be able to make better and more rapid decisions in the instance of a crisis. This coupled with a greater ability to attribute either hybrid or cyber-attacks should enable the state to deter this type of aggression and will potentially reduce the likelihood of an attack happening in the first place.

Our final recommendation is that the Irish government should examine the implications of the development of offensive cyber capabilities for defensive purposes to increase costs for perpetrators of cyber-attacks. This would also be in line with 2022 CoDF's recommendations for the development of a Joint Cyber Defence Command in the DF who would be able to conduct limited offensive cyber operations. We believe exploring the use of offensive cyber for defensive purposes would play an important role in changing the cost/benefit calculus of potential aggressors.

Conclusion

To conclude, we find ourselves in a changing and more threatening security landscape. Ireland faces a degree of threats which it likely has not faced before in its history as potentially everything from social media to globalisation, international trade and the internet can now be weaponised.

Though before I close, I would like to emphasis there is cause for optimism. A mental shift to a whole-of-society approach to national defence would not only allow the full strength of the nation's resources to be harnessed but it would also give all stakeholders - government officials, NGO's, the military, universities, business and most importantly the public - agency in the states future national security strategy ultimately creating a more resilient and more robust society which is best positioned to deter would be aggressors' hybrid warfare campaigns. Thank you for your attention and I look forward to your questions.