European Security Threats

Clodagh Quain and Ben Tonra

This briefing paper summarises discussions from the first of a series of three research-based, half day seminars organised by the IIEA with the support of the ERASMUS+ - funded and NORTIA academic network. The series aims to further debate in Ireland on defence policy with the input of leading scholars, experts and practitioners on i) threats to small states in Europe ii) the contribution of small states to European security and defence iii) strategy building for small states in European security and defence.

The Security & Defence of Small European States

What are the broad threats?

EXISTENTIAL

Threats to our physical existence

- CLIMATE CHANGE
- RESOURCE DEPLETION
- PANDEMICS

SYSTEMIC

Things that threaten our own security and that of our neighbours

- POLITICAL & ECONOMIC INSTABILITY
- HUMAN RIGHTS VIOLATIONS
- CIVIL CONFLICTS

STATE AND NON-STATE

- TERRORISM
- HUMAN TRAFFICKING
- ORGANISED CRIME
- DARK MONEY

What are the threats facing small states?

- Geographical location
- Development of regional cooperation and alliances
- Decline of the rules-based international order
- Exposure to global economic shocks

What are the threats facing Ireland?

- Cyberattacks and capacity to defend
- Online influence, disinformation campaigns and external political manipulation
- Weaker national security capabilities outside the cyber realm

Threats facing Europe

Today European states face a wider and more complex set of threats to their security and defence than at any time in the last 30 years.

Those threats can be grouped in different ways. In the first category are what are sometimes described as **'existential' threats**, that is threats to our very physical existence. These include issues such as climate change, resource depletion, and the threat of pandemics.

In a second category are what we might see as **'systemic' threats** – things that threaten our own security and that of our neighbours, but which are not consciously directed by other actors. In this category we might think of political and economic instability, human rights violations, civil conflicts within Europe and at its borders, and the impact of sudden migration or refugee flows which may result from instability, injustice and conflicts.

Finally, we have also to consider the kinds of **threats that are deliberately posed by other actors** – which may be other states, but which can also be **non-state actors** – such as terrorists. These actors have used a variety of tools to threaten, to intimidate or to attack Europe. While the traditional image of armies invading across borders is rare today, it has occurred in recent years in Georgia and in Ukraine. In both cases Russian troops have invaded, occupied and in some cases annexed the territory of other European states. Today, however, we are more likely to see such threats come in 'non-traditional' forms – sometimes called 'hybrid' warfare.

Some of these threats include terrorism, assassination, organised crime and human trafficking. Armed groups or individuals, sometimes with the covert backing of states, use largely **low-tech** violence against civilian populations, minorities or against individuals.

Other threats, such as attacks on critical infrastructure are designed to undermine the politics, economics and-or social cohesion of European states. Here, threatening actors deploy a variety of tools from a new and often **high-tech** toolbox. They have, for example, attacked the computer systems and IT infrastructures of electricity, banking, health care, and public security systems. Such attacks – and attempted attacks – have become an everyday reality for cybersecurity professionals in Europe. Furthermore, the use of **dark money**, **social media** and **disinformation** campaigns designed to undermine confidence in, and the free practice of, democratic politics, have emerged in recent years The rise of political extremism at home and authoritarian regimes overseas have also weakened global institutions designed to protect peace and prosperity.

All European states face the same range of threats but from different perspectives, based on their geography, their neighbours, their history and their unique strengths and weaknesses. Europe has also had to adjust to a shifting balance of power as other global regions and actors seek to reshape a world which has for so long been defined by structures set up at the end of the Second World War. Many European states too, must take account of the bitter and bloody legacy of colonialism and imperialism across Africa, Asia, the Middle East and the Pacific.

What are the particular vulnerabilities facing smaller European states in relation to the above-mentioned threats?

While all states face the general run of threats in Europe today, there are useful particularities to highlight. For example, scale matters and the national capacity of smaller states – at least in terms of material resources- are by definition, less than those of larger states. By the same token, smaller states may have greater societal resilience to threats than larger, more complex states by virtue of the size of the polity, political cohesion or sense of identity born of existing in a dangerous world.

Threats facing small states

In general, there are more particular factors that determine threats facing smaller states. These include:

First, **geography** is a particularly strong driver in terms of proximity to larger players. A cluster of states, such as the Baltics, Sweden and Finland, can produce a sense of solidarity, which may be useful in response to threats. By contrast, Ireland's peripheral location is unique in shaping its approach on defence cooperation.

A second determining factor is the development of regional cooperation and alliances. Small states tend to be more vulnerable to asymmetries of power. As a result, they are compelled to rely more on the force of law rather than the law of force in international relations. Within the EU, smaller Member States can rely more on the collective strength of much larger states in a rules-based system of governance. However, smaller states must also balance the trade-off between their interests and those of larger states with a wider global exposure to threats and more complex global agendas. Conversely, it is in the interest of larger states to seek alliances with other small and medium-sized states. However, small states in the EU have been quite successful in the pursuit of their own security priorities.

Third, the **decline of the rules-based international order** and multilateral institutions is a particular threat to small states who are best protected by the shared international rules and norms. Multilateral institutions provide a platform on which small states can assert their interests, influence and participate in decision-making, and find like-minded partners. This platform can also allow small states demonstrate leadership in areas such as climate change where their impact on the ability to mitigate the threat is limited.

A fourth driver of threats particularly facing small states is the question of **capacity**. Small states tend to grapple with constraints in terms of resources and infrastructure. Cybersecurity, for example, requires considerable investment in finance, technology and human resources. A resource-weak national security and defence capacity can entail greater dependence on larger partners and thus less direct control over some critical national security and defence issues.

In addition, small states are exposed to a certain extent to **global economic developments and shocks**. Smaller states may rely more heavily on international trade, open transport networks, access to markets and resources and inward investment. All of these can be manipulated by larger actors as a tool to gain influence over smaller states.

Threat levels in each of these areas can fluctuate considerably over time and depending on the context. This highlights the need for smaller states to carefully monitor the threats that they face and to plan accordingly, with a focus on rapid adaptation as threats evolve. In security and defence policy, smaller states need engaged leadership, cross-government collaboration, a vibrant national discourse and a wide awareness of the scale and nature of threats. The pace of change in the threat landscape also means that small states are facing an ever-moving target, particularly in the areas of cybersecurity, digital and data.

The challenge to smaller states is that while the sense of proximate territorial threat fades, cyber threats multiply. Smaller states will often be acutely aware of geographic threats – by virtue of their historic experience of larger neighbours. They may risk, however, missing the significance of threats posed in the cyber realm – especially as they are more vulnerable to the unintended consequences of ongoing cyber conflict between larger powers.

Threats: An Irish Perspective

Ireland has been relatively secure from territorial threats in the last few decades due to its geographic distance from centres of ongoing or potential conflict The peace process on the island of Ireland has also contributed to a public perception of more guaranteed security, a fact which is misleading in light of the nature of new unconventional cross-border threats.

Ireland is a host to many multinational companies, including many large social media platforms. This has afforded it a reputation as a digital hub with economic interests to defend, a topic that has featured prominently in public discourse on foreign direct investment (FDI). Ireland's resilience to cyberattacks, direct or indirect, and the capacity therefore to defend its interests is questioned by cyber experts.

The Irish Government published its first Cyber Security Strategy in 2015 and founded the National Cyber Security Centre (NCSC) in 2011 within the Department of Communications, Climate Action and Environment (DCCAE). The current National Cyber Security Strategy was published in December 2019. Taking account of efforts to date, there is an ongoing need for investment in resources and technology to forestall potential attacks that may have considerable economic, political and societal implications. This includes the defence of critical national infrastructure in areas such as energy, health, finance and banking and government services.

Cyber can also pose threats to Irish parliamentary democracy through online influence, disinformation, disruption and political manipulation. Some observers consider Ireland to be a potential backchannel for actors who wish to disrupt the EU and the UK, feeding political extremism, disrupting politics and potentially undermining democracy at home and overseas.

Inattention to these threats in Ireland carries a further hidden risk. Without acknowledgement of the threats faced as well as an informed national debate on a state strategy, Irish security and defence policy is dependent on the goodwill of other states.

Ireland's exposure to its larger neighbours has shaped its security outlook. Brexit will entail serious economic and security implications for Ireland. With the UK outside the EU, Ireland will face new challenges in managing its security interests with partners in the EU. The UK's departure from Europol for example will also create a considerable gap in data and capacity. Unpredictable politics in the US is likely to question established transatlantic security relations with implications for Ireland as the EU's own security and defence identity further develops.

International observers have noted Ireland's weaker national security capabilities outside the cyber realm. In traditional air and sea defence, Ireland lacks technologies necessary to identify and track potentially hostile aircrafts or submarines and subcontracts this out to other states. Ireland also has traditionally had a more limited capacity in gathering and analysing intelligence, which relies on foreign services to identify certain potential threats.

In a multilateral context, Ireland has the potential to pursue its security interests and values – with the EU offering the strongest rules-based framework for doing so. Other institutions such as the UN, OSCE, OECD and Council of Europe also have their own strengths, each of which contributes to the security puzzle though are limited in scope in serving the unique security challenges facing Ireland. Without public debate on the strategies needed to address security threats and in the absence of national resources devoted to making those strategies a reality, Ireland's security and defence is left in the hands of others.

A robust Irish security and defence policy requires a clear identification of what assets Ireland needs to defend and the specific threats faced by the state. This also involves greater public awareness and engagement on the range of threats faced from climate change, to terrorism and cyberattacks. A broader political debate would prioritise and contribute to shaping a response to those threats in such a way as is consistent with Ireland's values and interests.

The view expressed in this brief are those of the authors and participants in the Nortia defence seminar, and not the IIEA.

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

The IIEA is independent of government and all political parties and is a not-for profit organisation with charitable status. In January 2017, the Global Go To Think Tank Index ranked the IIEA as Ireland's top think tank.

The IIEA acknowledges the support of the Europe for Citizens Programme of the European Union.

European Security Threats

Clodagh Quain and Ben Tonra

Nortia
Jean Monnet Network
EU Foreign Affairs

Co-funded by the
Erasmus+ Programme
of the European Union

IIEA
The Institute of
International &
European Affairs