# THE AZURE FORUM

# Newsletter

January-March 2022

*The Azure Forum Newsletter features announcements on applied policy research, seminars and public engagement activities on peace, security, transnational crime and defence.*

In this Issue:

# Latest Research Seminars and Briefings

[Joint High-Level Azure Forum-Finnish Embassy Roundtable on "Cyber, Hybrid and Intelligence: Lessons from the Finnish Experience | 24 February 2022](#)



The Azure Forum for Contemporary Security Strategy and the Finnish Embassy Dublin co-hosted a high-level expert roundtable on cyber, hybrid and intelligence with Finnish Ambassador for Cyber Affairs Jarmo Sareva and Finnish Ambassador for Hybrid Affairs Liisa Talonpoika. The roundtable was chaired by Ambassador Raili Lahnalampi.

# The Ukraine-Russia Crisis: Regional and Global Implications? | Azure Forum International Security Dialogues, 25 February 2022



**Dr. Bettina Renz,** Professor of International Security at the School of Politics & International Relations at the University of Nottingham and **Edward Lucas,** British writer, security specialist and non-resident Senior Fellow at the Center for European Policy Analysis discussed how the security situation in Eastern Europe has developed, noting the complex history between Ukraine and Russia, the conflicts in Crimea and Donbas and recent troop build-ups. Conflict has severe regional implications and the discussion focused on what this means for the evolving European security order, and in particular for NATO and the EU. In 1914, British Foreign Secretary Sir Edward Grey famously remarked that "the lamps are going out all over Europe". Grey's phrase has more recently acquired a literal meaning alongside its symbolic one. Questions raised included: What would be the impact of conflict on European energy security given its reliance on Russia? And more broadly, what would the impact be globally amidst the pandemic trade and supply issues and on other regional hotspots such as the Arctic? The roundtable was co-moderated by Caitríona Heinl and Adjunct Fellow Ruth Casey.

[Joint British Embassy Dublin-Azure Forum Report Launch: 'Exploring Serious and Organised Crime across Ireland and the UK: Towards a Shared Understanding of a Shared Threat' | 30 March 2022](#)



The Azure Forum for Contemporary Security Strategy, with the support of the British Embassy Dublin, launched a new report: "Exploring Serious and Organised Crime across Ireland and the UK: Towards a Shared Understanding of a Shared Threat" on Wednesday 30 March 2022. At the event, report author **Senior Fellow** [Dr Alexander Chance](#) discussed the report's findings with experts **Paul Thornton, Head of Western Europe SOCnet at the Foreign, Commonwealth & Development Office** and **Detective Chief Superintendent Angela Willis, Head of Bureau, Garda National Bureau of Criminal Investigation**.

[Changing State Behaviour: Can International Law Deter Further Aggression in Ukraine? | Azure Forum International Security Dialogues, 31 March 2022](#)



This roundtable was **hosted in partnership with the Irish Rule of Law International (IRLI) and moderated by Aonghus Kelly, Executive Director of IRLI** in order to examine the intersection of security and rule of law questions. Expert discussants including **Dr. Ray Murphy**, Professor at the Irish Centre for Human Rights, NUI Galway and **Jennifer Trahan**, Clinical Professor at NYU's Center for Global Affairs addressed international law mechanisms that are now at the forefront of efforts to counteract the ongoing aggression against Ukraine with a view to bringing about a change in state behaviour. International law mechanisms such as the International Criminal Court; International Court of Justice; European Court of Human Rights; universal jurisdiction cases in domestic courts; and a putative international tribunal for the crime of aggression, were discussed. Some [scholars even argue](#) that [additional concrete](#) steps include ratification by more countries of the crime of aggression amendment to the [Rome Statute](#) (or the amended Rome Statute) and legislating for the crime in their domestic criminal codes. From a geostrategic perspective, key questions included whether such laws can [currently deter aggression](#)? And why did they fail to do so in the first place? What are the likely next steps required to continue safeguarding

the rules-based public international order from being further undermined when the outcome of the invasion of Ukraine is yet unclear?

---

## Research and Policy Reports

### Taking Stock of Ireland's Defence Industry | January 2022



The Azure Forum for Contemporary Security Strategy was commissioned by the Irish Defence and Security Association (IDSA) to produce an independent report on the Irish defence industry. The report, the first of its kind in Ireland, was designed to provide the IDSA with a high-level, state-of-play overview of the industry in Ireland. Authored by Research Associate Neil Dee, this report provides foundational research on several key questions such as the size and sectoral scope of the Irish Defence Industry as well as the economic value and impact of the industry.

**Read more**

---

[Commission on the Defence Forces Report | February 2022](#)
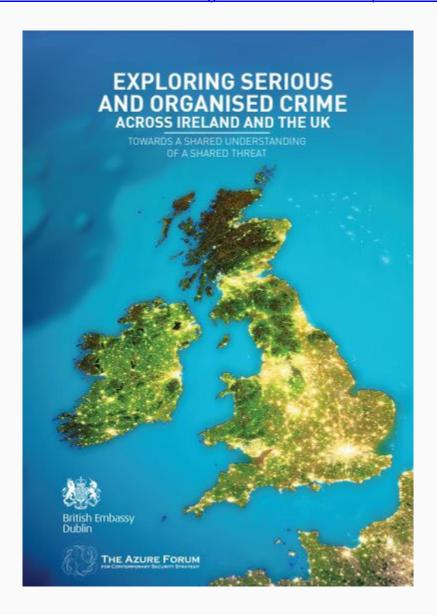


[Caitríona Heinl](#) was appointed as a member of the Irish government's Commission on the Defence Forces which began its work on 15 December 2020. Over a period of 13 months, the Commission focused its work on considering the appropriate capabilities, structures and staffing of both the Permanent Defence Force (PDF) and Reserve Defence Force (RDF) with a view to the immediate future, and the uncertain period beyond 2030. [The final report, which was released in February 2022, can be found here](#). This is a seminal report on the current status, capability requirements and potential future trajectory of the Irish Defence Forces. The report makes a number of recommendations on funding, diversity, capabilities, structures and more for the Army, Irish Air Corps, Naval Service, and Reserves. Its relevance will be felt both domestically and internationally as one of the most significant strategic documents on defence in the history of the State.

**Read more**

---

[Exploring Serious and Organised Crime across Ireland and the UK: Towards a Shared Understanding of a Shared Threat | 30 March 2022](#)



The Azure Forum for Contemporary Security Strategy, with the support of the British Embassy Dublin, published a new report on Serious and Organised Crime across Ireland and the UK. Authored by Senior Fellow [Dr Alexander Chance](#) with research assistance provided by Research Associate Neil Dee, the report, "Exploring Serious

and Organised Crime across Ireland and the UK: Towards a Shared Understanding of a Shared Threat" provides a strategic-level, qualitative assessment of serious and organised crime as it operates within and between Ireland and the UK. The report focuses on three key criminal activities that impact individuals, communities and societies in both countries: modern slavery and human trafficking, drug trafficking, and economic crime. The report also examines the cross-cutting 'enablers' that facilitate most contemporary forms of serious and organised crime.

**Read more**

## Commentaries & Azure Forum *Strategic Insights*

[Paddy McGuinness, Azure Forum Advisory Council Member, 'Deterring ransomware attacks as an international security priority: Treat ransomware as criminality', *Strategic Insight* | 16 February 2022](#)

Paddy McGuinness, Senior Advisor at the Brunswick Group and Former UK Deputy National Security Advisor for Intelligence, Security and Resilience writes that an Azure Forum seminar on "Deterring ransomware attacks as an international security priority" in September 2021 prompted four key recommendations for actions by Nation States which draw on his current work advising listed companies on their cyber resilience and past experience as UK Deputy National Security Adviser and Cyber Programme lead. First, treat ransomware as criminality and address it separately from the conflicted and glacial diplomacy to address state cyber action. Second, make it consequential for the criminal perpetrators, by attacking their wellbeing, their tools and dependencies. Third, support those who are attacked rather than blaming them, and in particular make business needs central to states' response. And fourth, develop resilience disciplines including more effective response and recovery, data sets as Critical National Infrastructure (CNI), and Public Interest communications.

**Read more**

[Jarmo Sareva, Ambassador for Cyber Affairs and Liisa Talonpoika, Ambassador for Hybrid Affairs at the Ministry for Foreign Affairs of Finland, 'Maturing national responses to hybrid influencing and cyber threats: A primer on Finland's approach',*Strategic Insight* | 2 March 2022](#)



The current geopolitical situation has highlighted the need for a comprehensive response to both cyber and hybrid threats. Finland's model of comprehensive security also supports overall resilience against these threats. The goal is to protect all of society's vital functions through a collaborative approach involving authorities, the private sector, civil society organisations, academia, and private citizens. In this regard, a high educational level, cyber skills, media literacy, social trust and cohesion as well as low corruption are important. Our legal framework further supports this whole of government approach whereby new legislation is adopted as needed to raise preparedness. During the last several years alone, Finland has updated its legislative tools in areas such as intelligence, network security, ownership of real estate, dual nationality and international assistance.

**Read more**

The war in Ukraine has so far seen very little engagement from the cyber diplomatic community. While the international community focuses on stopping Russia's invasion and ending the conflict, the contribution of cyber diplomacy to these efforts has been limited to the usual offers of assistance to deal with cyber incidents. This is surprising, given the number of cyber diplomacy-related questions raised by the conflict. In particular, the war challenges the effectiveness of the tools developed to date and asks how the framework for responsible state behaviour in cyberspace applies in this situation. Activity by non-state actors acting as proxies on both sides of the conflict is also raising new dilemmas. What does the war in Ukraine tell us about the state of cyber diplomacy today?

**Read more**

As the EU strives to strengthen its cyber resilience, it becomes ever more important for its institutions to have coherent advice on the cybersecurity implications of legislative and regulatory decisions. Current practice, including in the context of the Digital Market Act (DMA), suggests action is needed to establish a policy-agnostic technical mechanism to generate such advice, develop important partnerships and create a dynamic process that reviews regulatory decisions and their implementation as threats evolve. The EU should define what makes up a properly constituted decision on technology risk.

**Read more**

## Strategic Advisory Services



Alongside research support, the Azure Forum for Contemporary Security Strategy continues to be commissioned by the Irish Defence and Security Association (IDSA) to provide secretariat services since its establishment in 2021. The IDSA is a trade body representing the defence and security industry in Ireland with members spanning Irish SMEs, multinational corporations and research performing organisations.

---

## Public Engagement, Outreach and Awareness-Raising



Caitríona Heinl continues to be Co-Editor-in-Chief alongside Patryk Pawlak for the *Directions platform* running since 2020 under the EU Institute of Security Studies'

EU Cyber Direct project. *Directions* is an independent platform for exchanging and discussing ideas on Europe's place in the digital world and world views on digital Europe. Through analysis, commentaries and interviews, *Directions* aims to stimulate a European debate and showcase the diversity of voices about the present and future of cyber and digital policies – at the national, European and global level.

Latest EU Cyber Direct *Directions* articles can be found here.



Vice Admiral Mark Mellett DSM (Rtd), **Chair of the Advisory Council,** took part in a seminar on European Strategic Autonomy hosted by UCD, the French Ministry of Defence and the French Embassy Dublin on 26 January 2022.
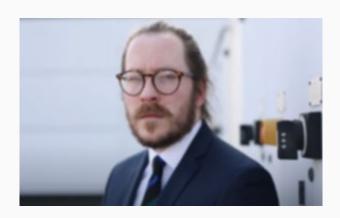
# New Members of the Azure Forum Network

## Paddy McGuinness, Advisory Council Member



Paddy McGuinness advises businesses and governments globally on data and cyber issues, business resilience and geopolitical and regulatory risk. He is a senior adviser at the Critical issues firm Brunswick Group providing counsel to clients across the firm's regions and specialisms. He sits on the advisory committee of the UK's reinsurance pool for Terrorism risk PoolRe. From 2014 – 2018, Paddy was the UK's Deputy National Security Advisor for Intelligence, Security and Resilience advising two successive British Prime Ministers on UK Homeland Security and Government Security policy. This included the National Risk Assessment and ability to respond to and recover from all hazards and threats, National crisis coordination, Cyber strategies and programmes, Counter Terrorism, Counter Hostile State Activities, resilience of Critical National Infrastructure and issues with inward investment. Through Hudhud Associates Paddy also supports Private Equity funds on a range of transactions, and works with technology start and scale ups as an adviser and investor. He is a co-founder of Oxford Digital Health and 2020Partners and is on the advisory Boards of Venari Security, Glasswall Solutions, Blackout Technologies and Kazuar-Tech.

## Matthew O' Neill, Research Fellow



Matthew O' Neill is a Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) postgraduate research student in Political Science at the Senator George J. Mitchell Institute for Global Peace, Security and Justice at Queen's University Belfast. His research explores the European Union Digital Single Market. His area of focus has been on Artificial Intelligence policy examining the political, legal, and technical relationships surrounding intellectual property rights and relationships among member states. Matthew's research area interests include EU Politics and Institutions, EU Integration, EU Security Policy, The EU Digital Single Market, Artificial Intelligence Policy, Border Studies, and British and Irish Politics.

## Mark Williams, Research Fellow



Mark Williams is a Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) postgraduate research student at the Senator George J. Mitchell

Institute for Global Peace, Security and Justice at Queen's University Belfast. His research explores the interface between the social sciences and electronic engineering and computer science focusing primarily on the criminal use of social media. This research includes examining ways of detecting and preventing inappropriate and criminal behaviour in social media, with particular emphasis on the mitigation, policing, and prosecution of offensive online expressions. Mark's research interests include online hate, extremism and disinformation; cybercrime and criminality; internet/tech regulation; cyber warfare and peacekeeping; strategic communications and digital information operations.

---

# In the News

- [Russian war games show the need for joint defence strategy](#)
- [Retired Defense Forces Chief of Staff Mark Mellett about the war in Ukraine](#)
- [Mellett: Ireland's best answer to Russian power is renewable energy](#)
- [Brexit to significantly alter flow of illegal drugs into Ireland, says think tank](#)
- [Foreign gangs may muscle in on drug trade, researchers warn](#)
- [Corrupt transport workers are key link in Irish/UK crime network, report finds](#)
- [Corrupt port and airport workers 'central' to operations of organised crime gangs in Ireland](#)