Commission on the Future of Policing in Ireland - Submission:

An Opportunity for Change: A Review of the National Security and Intelligence Function of An Garda Síochána
31 January 2018

Dr Edward Burke
Assistant Professor in International Relations
School of Politics and International Relations
University of Nottingham
Law & Social Sciences
University Park
Nottingham, NG7 2RD
UK

+44 (0) 115 951 4791
Edward.burke@nottingham.ac.uk

Summary
1. State security and intelligence – for which An Garda Síochána (AGS) is the lead agency - requires more political priority and investment in capabilities. A stretched AGS prioritises criminal investigation over long-term intelligence gathering and threat analysis. A National Security Adviser should be appointed to work as the Principal Secretary to the Government Security Committee, chair Quadrennial Reviews of national security, devise and monitor implementation of multi-agency plans to enhance security and produce all-source intelligence assessments. He or she would lead a National Security Secretariat situated in and reporting to the Department of the Taoiseach (DOT). In the medium-term, the National Cyber Security Centre (NCSC) should evolve into a signals intelligence (SIGINT) agency. The Government should also create a new intelligence service dedicated to counter-terrorism and counter-intelligence, including acting as a liaison with European Union (EU) and foreign intelligence services. Both agencies should be funded by a single intelligence account through the DOT. Finally, the Government should introduce legislation for a National Security Act to enhance intelligence capabilities and improve oversight over the national intelligence function. Such reforms are an appropriate and necessary response to the growing number of threats to national security.

Background
2. Almost 100 years since the foundation of the State, Ireland faces fundamental challenges and questions relating to its sovereignty. The threats that emerged in the 20th century – particularly on-island violence from Republican and Loyalist terrorist organisations – have not entirely gone away. But they have been surpassed in scale by others, including transnational criminal and terrorist networks who increasingly use the cyber domain as a means of targeting Irish citizens or residents and attacking critical national infrastructure (CNI).[1]

3. Ireland's membership of the EU is critical to its security. The State can draw upon agencies such as Europol and Eurojust, among other Justice and Home Affairs (JHA)

[1] Critical National Infrastructure is here defined as comprising the following: Communications, Emergency Services, Energy, Finance, Food, Government and Public Service, Health, Transport and Water.

institutions and mechanisms to counter serious crime and terrorism. But these coordinating, information sharing agencies rely in turn upon the policing and intelligence capabilities and operations of EU Member States.

4. Since 2015, the European Commission has expressed its growing concern that Ireland has been too slow to link up with critical EU crime and intelligence databases including the Schengen Information System II (SIS II). In early 2017 the Commission announced that it was initiating proceeding against Ireland for its failure to connect with SIS II. The current Government understands the urgency of doing so – but the delay in implementation appears to have confirmed other EU Member States' concerns that Ireland's priorities are elsewhere.

5. Brexit will exacerbate threats to Irish security. According to the Police Service of Northern Ireland (PSNI), 43 per cent of Northern Irish organised crime gangs' activities, including paramilitaries, have a cross-border dimension; they use Dublin based criminals to connect to European and international crime networks. The UK's likely withdrawal from the Single Market and/or the Customs Union will mean the imposition of some physical infrastructure at the border after Brexit. A customs border creates an obvious market for criminal evasion; an over-stretched Irish police and security infrastructure - currently trying to contain an escalation in gang related violence in Dublin - will struggle to adapt and respond to an expected increase in an already worrying level of border smuggling and terrorism. Securing the Common Travel Area (CTA) after Brexit will require significantly increased political attention, intensified bilateral security relations and an investment in capabilities. The UK terror threat level is at 'Severe' – the future of the CTA may depend on trust in the security infrastructure and data sharing of both States.

6. The UK appears likely to exit some JHA agencies and mechanisms if it refuses to abide by European Court of Justice (ECJ) oversight and rulings. This is particularly alarming since the UK contributes large amounts of information to EU crime and counter-terrorism databases; the UK is also involved in 40 per cent of all Europol cases. The recent impasse over the EU-Canada Passenger Name Records (PNR) agreement – essentially blocked by the ECJ due to concerns over citizens' privacy – stands as a warning of potential headaches for Ireland when it comes to sharing intelligence with the UK, if post-Brexit the UK diverges from EU standards. Britain's ability to opt back into the European Arrest Warrant arrangements are also in question. A return to some form of problematic bilateralism between Ireland and the UK appears likely.

Foreign Intelligence and Cyber Security

Even Good Friends Spy on Each Other

7. It is a relatively open secret in some European capitals that AGS relies heavily upon the UK for much of its intelligence, particularly when it comes to monitoring the internet or other signals intercepts relating to jihadi activity by Irish citizens or residents. Ireland has a limited capability – in AGS, the new NCSC and the Defence Forces (DF) - to detect and monitor networks of international criminals or terrorists who operate in Ireland. The extent of reliance upon agencies such as Government Communications Headquarters (GCHQ) in Cheltenham, the National Crime Agency (NCA), the Security Service (MI5) in London, Belfast confirms an impression of excessive dependency, a trend noted by other European countries and international partners.

8. Ireland is also at a disadvantage when it comes to countering intelligence gathering by States with sophisticated SIGINT capabilities. Cyber security in Government departments and agencies has not always been sufficiently prioritised. For example, in recent years

Irish embassy communications networks overseas often relied upon international private security companies for cyber security. Sub-contracting such tasks to these companies, often staffed by foreign nationals with previous/current military or intelligence ties, is far from optimal.

9. The NCSC is located in disparate locations, including a university campus, some of which are very possibly insecure. In the early 1970s a Secret Intelligence Service officer (MI6) infiltrated the Garda Crime and Security Branch (CSB) by recruiting an agent; given still relatively low encryption practices across Government departments it is arguably much easier to access sensitive Government communications today than it was historically. However, AGS still lacks sufficient resources to undertake extensive vetting of personnel in sensitive posts.

10. Ireland lies between three of the 'Five Eyes' (the UK, Canada and the United States. The other two are Australia and New Zealand. Five Eyes is the most integrated and sophisticated intelligence sharing relationship in the world; they generally do not conduct intelligence operations against one another). These countries have constant, senior official dialogues on how to optimise information from, and protect, transatlantic fibre optic cables that pass through Ireland including Hibernia Express Project – a superfast internet cable that links North America to Europe via Cork. Despite such conversations relating to Irish sovereignty, Ireland is mostly not included in these dialogues since it is not in Five Eyes and does not have a similarly sophisticated and secure SIGINT agency with which to consult.

11. The days of innocence – epitomised by Chancellor Angela Merkel's surprise when it was revealed that the US National Security Agency accessed her mobile phone – should gave way to a sustained, focused investment in Irish capabilities to frustrate foreign monitoring of Government communications. Ireland has sensitive policy differences relating to ongoing discussions with even its closest allies such as the UK and France. These must remain secret.

The Threat from China and Russia

12. Ireland has occasionally been used as a country of convenience either for the acquisition of false passports, routing of finance or as a location for intelligence officer-led meetings by States such as Russia, China and Israel – indeed, Russian and Israeli diplomats have been expelled from Ireland during the last decade.

13. A more active and alarming area of concern is the targeting of Irish and foreign multinational companies by criminals, sometimes linked to foreign state intelligence services, that attempt to hack businesses to extort money and/or steal intellectual property. In future a State's ability to protect the private sector from such attacks will likely be seen to be as important as other structural factors, such as corporation tax or a skilled labour market, in deciding where a multinational will locate its business. Ireland is currently the European hub for many US multinationals; the Government will come under increasing pressure to help keep their infrastructure/business activities secure.

14. The increasing frequency of cyber-attacks on Irish based businesses by hackers, particularly in China and Russia, is clearly of significant concern. The Taoiseach has moved to address this problem by establishing and resourcing the NCSC as well as introducing new legislation to allow for a more proactive Irish cyber security role. But much more needs to be done if Ireland is to meet the future requirements of multinational and Irish companies as well the EU's new general data protection regulation. Recent attacks on the National Treasury Management Agency (NTMA) underline what a potential threat this activity is to CNI. Ciaran Martin, the Head of the UK NCSC has warned that a

Category One (C1) attack – crippling an area of CNI for a period – is highly probable in the next few years. Responding to and containing a C1 attack on the UK will be a significant challenge for both States; the risk of contagion is obvious.

International Terrorism

15. The State is not immune from the threat from extremist jihadi groups. Supporters of Islamic State (IS), as their attacks in Sweden and Finland underline, are often blissfully unaware and uninterested in countries' neutrality, position on the Middle East Peace Process etc. Ireland faces a moderate but enduring threat of attack by IS sympathisers, particularly as foreign fighters return to Europe after defeat in Iraq and Syria.

16. AGS is clearly aware of the rising threat from Islamist extremism and has moved to reach out to Muslim communities to build partnerships and offer reassurances regarding the State's policing and justice aims, including through the Garda Bureau of Community Diversity and Integration. But the Security and Intelligence component of the CSB remains under-resourced. The personnel and budget of the National Surveillance Unit, for example, was significantly cut during the recent economic crisis. These and other cuts to specialised units are now being reversed but some experienced personnel have already left AGS.

17. The number of suspected jihadis on a dedicated AGS watch list has doubled in the last year, standing now at close to 70 – up to half of these are linked to broader European jihadi networks. Despite more funding, Garda specialist resources – including in surveillance and in armed support – are stretched due to the ongoing priority of dealing with the increasing violence of the Kinahan-Hutch gang war in Dublin. Active surveillance on a suspected terrorist often requires a minimum of 30 AGS personnel. Limited AGS resources mean that they can consequently only monitor a handful of suspects at a time.

18. Security officials in other EU Member States, including the UK and France, are concerned that AGS are so pre-occupied in dealing with the fall-out from gang crime that they do not have sufficient resources to focus on medium to long-term intelligence horizon scanning and analysis. Rachid Redouane, one of the IS sympathisers who carried out the June 2017 London Bridge attacks may be a case in point. Redouane was refused asylum in the UK and was later arrested on immigration offences (using a false passport) when he tried to board a ferry to Northern Ireland from Scotland. He subsequently married a British citizen and gained residency in Ireland. The lack of any other information on Redouane, who spent substantial periods in Ireland, prompted reflection on the part of AGS and in London on possible missed opportunities for detection. Either Redouane was radicalised unusually quickly or important information was not picked up. The other two attackers, one of whom was on an EU terror watch list and the other was reported to a UK anti-terror hotline, had come to the attention of British and Italian intelligence officers even if subsequent opportunities for effective threat analysis and interception were missed.

19. Another recent account of how an Algerian national, who had been arrested and convicted of organising terrorist attacks, was allowed to subsequently claim and retain asylum status in Ireland for a prolonged period also prompted concern in other EU Member States. During his time in Ireland he continued to support and plan acts of jihadi terrorism across Europe. The case of Khalid Kelly, who loudly pronounced his support for violent jihadi extremists, but was able to travel to blow himself up as a suicide bomber in

a village in Iraq in 2016 compounds a somewhat worrying picture of an under-resourced and/or constrained police, intelligence components of the wider State justice system.[2]

20. The potential terrorist threat to CNI was further underlined by the recent plot at Kerry Group by IS sympathiser Munir Mohamed, who planned to put ricin in food products at the factory in the English Midlands where he worked. Although the attempted poisoning took place at Kerry Group UK, it has important CNI implications for Irish multinationals at home and abroad.

What to do? The differentiated value between Criminal Investigation and Intelligence

21. The CSB has many competing tasks. Crime detection, evidence collection for the purposes of prosecution/conviction are rightly often the criteria by which Government Ministers and the public judge the performance of their police service. Security intelligence is more focused on collecting information, often secret, that informs policymakers about possible or emerging threats - threats that may not yet warrant a major police investigation, operation or arrests. It is often about cultivating long-term relationships and/or covert human intelligence sources (CHIS) that may one day prove useful, or may not, depending on the escalation or diminution of a potential threat. This can involve acquiring or investing in distinctive cultural and linguistic skill sets over many years. Asking an Assistant Commissioner to assume responsibility for both these distinctive, if complementary roles - investigating serious crimes and analysing possible future threats – is excessive.

Looking at the New Zealand Model

22. New Zealand is a similarly sized country to Ireland with an arguably lower security threat profile. Nonetheless, Wellington has invested in establishing and maintaining small but robust intelligence services to lead on counter-intelligence, counter-terrorism (the New Zealand Security Intelligence Service or NZSIS) and cyber security (Government Communications Security Bureau or GCSB). NZSIS collects and analyses intelligence on critical issues relating to New Zealand's national security, including protecting citizens/CNI from terrorism, foreign espionage and subversion. They are also the lead vetting agency for public agencies and on security matters relating to immigration and citizenship matters. GCSB helps to counter the growing threat to the New Zealand public and private sectors from state sponsored and individual hackers. The combined New Zealand intelligence budget per annum comes to just over €25 million per annum. However, on top of this budget, Wellington recently announced a major, €71 million upgrade of Government high-grade cryptographic infrastructure.

23. A Minister for National Security and Intelligence in New Zealand's Department of the Prime Minister and Cabinet drives intelligence coherence and evaluation, overseeing a committee of senior officials from relevant departments and agencies. He or she is assisted by a Director for Intelligence and Assessments who leads the National Assessments Bureau (NAB), an agency that offers a constantly updated national security threat analysis based on all-sources intelligence. New Zealand is in the Five Eyes network, which gives Wellington global reach on emerging threats and intelligence that may relate to the safety and interests of New Zealand citizens. Because of its regular investment in cryptographic infrastructure, other countries believe that they can share the most sensitive of material with their New Zealand counterparts relating to inter-State espionage as well as terrorism.

[2] Meanwhile, the recent vandalism/attack on a mosque in Galway and a rise in online Islamophobia indicates that the State will also have to counter a small but growing threat from far-right extremism/terrorism.

Appointing a National Security Adviser / Upgrading Security Intelligence

24. The Taoiseach has already taken very welcome steps to improve Ireland's security infrastructure including establishing the Government Security Committee (GSC) and the NCSC. However, at the operational level significant inter-departmental or inter-agency gaps remain when it comes to national security. For example, the distinctive functions of the NCSC require further political elaboration, oversight and legislation (including how they will relate in future to the Garda National Cyber Crime Bureau).

25. The Government should appoint a National Security Adviser (NSA) in DOT, with direct responsibility for whole-of-Government security and intelligence planning/assessment would be a positive step. The National Security Adviser would act as a Principal Secretary to the GSC. This senior official would also oversee a National Security Secretariat (NSS) that would assume functions equivalent, or similar, to the NAB in New Zealand.

26. The National Security Adviser would chair an Intelligence and CNI Protection sub-committee of the GSC, with the participation of senior officials from AGS, DF, the NCSC, the Department of Foreign Affairs and Trade and other departments and agencies as required.[3] He or she would develop and implement Government policy and plans as set out by the GSC. The NSS would aid the work of this sub-committee by providing all-sources threat analysis and specific subject area, cultural or linguistic expertise. The National Security Adviser would also provide a much needed whole-of-government national security link to the Oireachtas.

27. While drawing upon experiences elsewhere, the model of NSA/NSS chosen should reflect specific national concepts and requirements, rather than a generic model adopted from elsewhere. There are scale, scope and legal differences across states and no two share the exact similar structure. However, regardless of the model, the defining characteristic is an aim for better-informed decision making at executive level, encompassing a whole of government approach.

28. The transformation of NCSC into a full SIGINT agency is a sensible medium to long-term ambition to keep pace with the cyber security demands and threats that Ireland faces in the coming decades. The NCSC should receive the bulk of any future intelligence budget. It should also complement the work of the DF overseas operations – cyber capability and resilience is increasingly a key component of peacekeeping operations.

29. The option to establish a dedicated counter-terrorism and counter-intelligence service should be explored, especially if it is deemed desirable to appoint foreign nationals to key posts in AGS. Short-term crime investigation/operational tempo often trumps medium to longer-term intelligence collection and threat analysis. A new security intelligence service would liaise with EU/European intelligence services similarly engaged in drafting evolving threat assessments, assigning priorities for investigation and surveillance; furthermore, it would lead on vetting. Establishing a dedicated intelligence service funded from a pooled intelligence budget that would also fund the NCSC, and a line of authority that runs directly from the DOT, would be an appropriate response to the increasing challenges to the State's most important function, protecting Irish citizens' lives and critical interests. Such an agency would also work with AGS and the NCSC to ensure that sensitive government communications are secure.

[3] These may include the Department of Communications, Climate Action and Environment, the Department of Housing Planning and Local Government, the Department of Health, Revenue Commissioners, among others.

Time for a National Security Act

30. The debate, legal challenges that preceded the publication of the Government Communications (Retention of Data) Bill 2017 highlights both Government concern over escalating security threats and public anxiety over the potential infringement of intelligence and policing on constitutional rights and civil liberties. A National Security Act would provide an opportunity for the Government to set out its case for i) increased security vigilance and ii) more effective oversight (including by the judiciary) over the national intelligence function. Again, the Government should reflect upon other countries' experiences (even if a final Act will of course reflect Ireland's specific political, security and legal context). For example, recently proposed Canadian legislation including (Bill C-59) offers useful proposals and instructive debate on ensuring executive, judicial and legislative accountability in the management/conduct of intelligence activity.