Nimmons Consulting Ltd

Strategic Thinking in a Complex World
Web: https://www.nimmonsconsulting.com

Assessing Ireland’s Cyber Security Strategy

Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA

Nimmons Consulting, London, December 2017

Introduction

Ireland is a thriving modern European state with a buoyant technology sector and ambitions to become a digital world-leader. Favourable corporate tax rates, high quality science, technology, engineering and mathematics (STEM) graduates (European Commission, 2017a, p. 5), access to European markets and other cultural and socio-economic factors have attracted technology giants including Google, Facebook, Amazon, Apple and Twitter to headquarter in Ireland. Ireland has significance in the data centre market with Amazon (O’Brien, 2017), Microsoft (Mulligan, 2016) and others having established footprints and growth plans. Ireland’s digital ambitions demand robust national cyber security response. In examining the efficacy of the existing cyber security strategy, a brief profile of Ireland’s digital capabilities is explored against which risks from threat categories, including crime, cyberterrorism and cyberwarfare are considered. Potential weaknesses are highlighted and 5 key recommendations proposed for improvement of Ireland's digital security posture.

Ireland's Digital Profile – a brief overview

96% of Irish households have fixed broadband coverage, although only 69% have taken this up (European Commission, 2017, p. 3). Mobile saturation in Ireland is 127% (European Commission, 2017b, p. 2) and mobile broadband uptake of 96 (subscriptions per 100 people) is significantly above the European Union (EU) average. There is something of a rural / urban connectivity divide and fixed broadband costs are high compared with other EU countries (European Commission, 2017a, p. 3).

Ireland ranks lowest in the EU for online news consumption (just under 50% of the population). Online entertainment, shopping, banking and social networking patterns are in line with EU average (European Commission, 2017a, p. 7). 58% of Irish citizens use eGovernment services (the 4th highest in the EU). The Irish Government is committed to the European Single Digital Market as well as open eGovernment (Department of Public Expenditure and Reform, 2017). The Irish state relies on technology to deliver digital public services (such as MyGovId and Public Services Card), drive economic growth (particularly in tech, pharma and banking), transact with trading partners in the EU and beyond and to preserve national security through defence, intelligence, policing, customs, border, critical information and critical infrastructure protection. Ireland, although a leader in some areas could see progress significantly impeded by low levels of digital skills within its citizenry (European Commission, 2017a, p. 10) and workforce (PwC, 2017, p. 7).

National Cyber Security Strategy

Ireland's National Cyber Security Strategy is written and owned by the Department of Communications, Climate Action and Environment (DCCAE) (until 2016 known as the Department for Communications, Energy and Natural Resources). The latest version (2015) sets out the strategy to the end of 2017. In broad terms it focuses on cyber security of the citizenry, protection of critical information infrastructure (across health, transportation, utilities), digital public services, and economic wellbeing. It is a cross-government strategy and contextualises cyber security initiatives with other government programmes and strategies including the National Digital Strategy (Department of Communications Energy and Natural Resources, 2013), eGovernment strategy (Department of Public Expenditure and Reform, 2017) and Public Service ICT Strategy (Department of Public Expenditure and Reform, 2015). It spans public, private sectors and academia, recognising the essential contribution that multi-sector stakeholders make to national cyber defence. Linking upwards into an overarching National Risk Assessment (Office of the Taoiseach, 2017), further contextualises cyber response within the national security framework. It is important to recognise the influence of EU cyber strategies, directives and doctrines and (as an integral EU nation) it is unsurprising to find Ireland in close and closing alignment.

Strategy Delivery

Delivery of the National Cyber Security Strategy involves a range of government departments and agencies, closely allied with partners in the EU and other states. Domestically, ownership sits with the DCCAE, within which the Computer Security and Incident Response Team (CSIRT-IE) and the National Cyber Security Centre (NCSC) have key operational roles (Edwards, 2017). The criminal justice system (under the Department for Justice and Equality) involves management of legal frameworks, policing (An Garda Síochána) with preventative and investigatory roles in crime and counter-terrorism, the Courts Service and Criminal Assets Bureau. The

Irish Defence Forces have a lead role in defending the defence network against cyber-attack and work closely with CSIRT-IE, the NCSC and other agencies. The Department of Defence chairs the Government Taskforce on Emergency Planning, with key accountabilities assigned to DCCAE for cyber related issues. EU and other transnational co-operation with the European Network and Information Security Agency (ENISA) and Europol (Calnan, 2014) have importance.

Irish and EU legal framework

In Ireland's legal framework, the key counter-terrorism instruments are the Offenses against the State Act (Government of Ireland, 1998) and the Criminal Justice Act (Government of Ireland, 2005). Neither provide definitions of cyberterrorism or cyberwarfare. The transposition of EU cybercrime directive 2013/40/EU into Irish law (Government of Ireland, 2017) provides legal clarity and additional powers, but missed the EU transposition deadline by two years (European Commission, 2015). The legal framework (as it relates to cyber security) in Ireland is arguably somewhat slow to adapt. It is therefore important to critically question the adequacy of legal powers and the extent to which Ireland treats cyberterrorism and cyberwarfare as strategic threats to the state.

Threat Actors and Motivations

In assessing cyberterrorism risks to Ireland it is helpful to enumerate likely threat actors. In terms of domestic terrorism, dissident Irish republican splinter groups present some challenges (Department of Defence, 2015, pp. 18-19). Loyalist paramilitaries operating in Northern Ireland have previously threatened the Irish state, but it seems unlikely that they have either motivation or cyber capability of significance. With the United Kingdom (UK) leaving the EU, the nature of the Northern Ireland / Republic of Ireland border has been debated. Instability could be exploited by paramilitary actors, including cyberattack on electronic border controls. Ireland's military neutrality might arguably distance it from certain transnational terrorism threats, although as a member of the Global Coalition against Daesh and the NATO Partnership for Peace, this distancing may be somewhat tenuous. Furthermore, Ireland does not take a neutral stance on counter-terrorism or cybersecurity. Ireland could find itself in the cross-hatches of far-right groups (if it overplays its position on the N. Ireland border), republican groups (if it appears too acquiescent to the UK) or radical Islamist actors seeking retribution against Western (particularly EU) states. The shock factor of an attack against Ireland might define its attractiveness. With a high density of data centres, international technology companies and banks, a large scale cyber-attack against Ireland could have significant world impact.

Cyberterrorism

In exploring this further, taking likelihood, capability, motivation and impact into consideration it is helpful to assess goals of radical Islamists (Al Qaeda or ISIS directed or inspired) against potential targets in the state's digital landscape. Although Ireland has no nuclear sites, control systems for utilities (water, electricity, gas) and transport (air, rail, port and road) could be significant targets. Bringing down the banking system, digital public services or causing a major outage or loss at an internationally significant data centre could have catastrophic effect. There could be significant economic and reputational damage. The possibility of a hybrid attack, combining kinetic and cyber assault cannot be discounted. Perhaps the most realistic scenario however is Ireland being attacked as it hosts (what terrorists might consider) strategic economic assets of other states.

Cyberwarfare

The threat profile from cyberwarfare has similar characteristics. Threat actors including North Korea, Russia and China may have cyber-espionage ambitions. With a handful of major companies providing 40% of Ireland's corporation tax returns (Office of the Taoiseach, 2017, p. 33), economic destabilisation of a strategically important sector seems plausible. It seems unlikely that Ireland would face cyberwarfare alone, but rather it would be attacked as part of more complex hostilities between Europe and other world actors. With plans to expand EU defence integration across member states (Bielenberg, 2017), Ireland must balance neutrality with defensive strength. Otherwise, in cyberwarfare it may be a prime target for compromise and exploitation.

Sufficiency of Preparation

This raises a key question, how prepared is Ireland to meet a cyberterrorism or cyberwarfare attack? Key policies, legal frameworks, agencies and working agreements are in place. These span numerous aspects of the public sector including eGovernment, policing, defence, critical infrastructure protection and emergency response. There are established links with industry and academia (including the Centre for Cybersecurity & Cybercrime Investigation at University

College Dublin) and Ireland benefits from close relationships with leading global technology firms. Ireland also benefits from extensive EU partner support from nation states (including UK policing and intelligence) and transnational institutions including ENISA and Europol. Alignment with the EU cybercrime directive harmonises Irish and EU legal frameworks.

WannaCry and Petya ransomware attacks in the summer of 2017 impacted some Irish businesses (Donnelly, 2017), but seemed to have little impact on government systems or services. Hygiene factors (such as patch management, intrusion protection and detection, anti-malware) may therefore be sufficient against some threats. Complacency must be avoided however, as legacy systems may be more susceptible to attack. With General Data Protection Rules (GDPR) coming into force in May 2018, cyber threats could rise, with rogue actors motivated by the infliction of punitive damages against their targets. It is unclear if Ireland's cyber capabilities would scale to meet a significant elevation of hostile activity. Inflection points such as Brexit, introduction of GDPR, or events including state visits or international summits could provide significant stress tests. Although Ireland's National Risk Assessment mentions the risk of nuclear contamination through accident (Office of the Taoiseach, 2017, p. 53) it might also be prudent to consider a broad set of risks posed to Ireland through catastrophic attack on a ‘near neighbour’.

There are significant strengths in Ireland’s cyber posture and readiness. CSIRT-IE has been in place since 2011. The establishment of the NCSC and transposition of the EU cybercrime directive into Irish law mark key milestones. The national cyber strategy is comparable with other national strategies including those of Canada (Ministry of Public Safety, 2010) and Estonia (Retel, 2014) which were used as additional reference points in this analysis. Ireland’s strategy aligns with a National Risk Assessment, which contextualises the importance of cyber-security within a broader national security context. This helps ensure that cyber initiatives are aligned with national priorities. Accountabilities and responsibilities across departments and agencies have been clearly articulated and the role of the NCSC as cyber lead within DCCAE provides co-ordination. Strategic focus on co-operation with domestic and international partners, cyber exercising, collection and reporting of key metrics signals both the importance of cyber security and its increasing professionalism.

Possible Weaknesses

Ireland has several apparent weaknesses that warrant further evaluation and discussion. Firstly, lack of digital skills across society is injurious not only to economic growth and public sector efficiency, but also to national security and combatting cybercrime. Cybercrime is a significant challenge and business capacity to combat it is seemingly weak (PwC, 2017a). Fostering greater resilience in the private sector is important to ensure that government resources are not needlessly focused on solving problems that others could and should own. Secondly, the economy has over-reliance on corporation tax returns from large technology firms. A concerted attack against Ireland's technology sector may be difficult, but would have obvious strategic appeal for an enemy. Thirdly, the national security role of An Garda Síochána (Garda) could be questioned. Whether there is sufficient capacity and specialism within the Garda to provide services across low and high policing, intelligence, counter-terrorism and cyber is debatable. In other nation states these functions are divided among several specialist agencies. Fourthly, Ireland's 'military neutrality' must be counter-balanced with transnational co-operation on counter-terrorism and cyber security. Beyond the EU, Ireland must also consider its alignment with the US government (Donnelly and Lynott, 2017) ensuring symbiosis. Ireland could benefit from US government and tech sector 'know how', but at the same time become a proxy target for enemies of the US. Finally, in light of recent warnings from the UK chief of defence staff (BBC News, 2017) Ireland may need to consider protection of transatlantic data cables in its territorial waters. Its cyber strategy and contingency planning should look at resilient communications in domestic and international contexts.

Suggested Focus Areas

5 areas of focus are suggested to improve cyber capabilities and readiness to meet extant and future threats. Firstly, the question of the soft border controls between Northern Ireland and the Republic of Ireland must be assessed. Electronic border controls could be targets for multiple actors with grievance against the UK, Ireland or the EU. Border destabilisation would weaken integrity and create tension between the UK and Ireland. Maintaining the free flow of goods, services and people between Northern and Southern Ireland is important for economic prosperity and détente. Rogue actors may seek to exploit transition.

Secondly, technological and sociological trends such as Smart Cities, the Internet of Things (IoT), Artificial Intelligence (AI) and driverless vehicles present great development opportunities. As Ireland's digital maturity grows, it should seek to lead in research and development of emerging technology. Infrastructure fragility and other capacity issues could be exploited and Ireland should seek novel solutions. This may extend the attack surface and the pace of innovation must be matched with a corresponding 'pace of safety'. Examples such as "remote tower technology" (Percival, 2017) at Irish airports or the implementation of traffic optimisation solutions in Galway demonstrate ambition. Systemic fragility, particularly in urban transportation could be exploited in attacks against control systems. Research focus on AI and IoT is important to ensure Ireland keeps pace with other nations. The National Cyber Security Strategy should be updated with reference to specific disruptive technology trends.

Thirdly, the potential for data science and big data solutions should be examined across all aspects of emergency response. CSIRT-IE, the NCSC, Defence Force capabilities and public sector bodies may be well co-ordinated through the Office of Emergency Planning, but the national Framework for Major Emergency Management

(Ireland's National Steering Group, no date) makes no explicit reference to cyber capabilities. What is also unclear is the availability of decision support systems and crisis management solutions with 'real time' analytical capabilities. The ability to make nimble decisions at pace and communicate clearly and accurately is essential during a national emergency. A technological review of crisis management capability (across all of government) should be considered with clear articulation of cyber-related dependencies laid out in major emergency management documentation.

Fourthly, regular counter cyberterrorism drills should be conducted within and between government departments, policing, defence and emergency services. Cyber exercising is a key objective of the NCSC. This should ensure scenario testing of systems, processes and procedures to ensure clarity, understanding and interoperability of cyberterrorism and cyberwarfare response across agencies, including situations of hybrid attack. Through regular drilling and performance evaluation, a continuous improvement cycle can be established that will improve cyber defence capabilities across process, organisation, technology and information domains. Ideally, performance data would be open for public scrutiny and subject to independent review.

Finally, upskilling the public in basic digital skills and online safety is vital. Digital skill level in Ireland is a significant human capital weakness. This weakness could be exploited by cybercriminals, terrorists and rogue state actors. Paradoxically, as less than 50% of Irish citizens use online news as a primary source, fake news and propaganda may have diluted impact on national opinion. Poor understanding and digital hygiene could however be exploited through ransomware, social engineering, or large-scale botnet compromise. Ireland must ensure its citizenry cannot be criminally exploited or even weaponised against the state by a controlling rogue actor.

Conclusion

Ireland is a confident modern state and has been extremely successful in high-tech industries. As a non-nuclear state that prizes military neutrality, some threats (such as attacks against nuclear power-plants) can be discounted or downgraded. While neutrality may somewhat reduce threats, it does not entirely eradicate those from indigenous nationalist or transnational terrorists. Cyber criminals and hostile governments (particularly those motivated by cyber espionage) will pay little heed to the State’s foundational doctrines. As Ireland hosts key economic assets of global firms, it may find itself caught up in cyber or other attacks against ‘hosted foreign assets’. Reliance on digital public services is increasing and significant lack of confidence in government could be caused by successful cyber-attack. Urbanisation and population concentration are creating transportation difficulties in major centres. Ireland needs to embrace innovative smart city and traffic management solutions but must ensure this is achieved safely. The digital divide and lack of digital skills in the population is both an economic and security weakness. Education, cyber challenges and coding challenges are good practices to engage and enthuse future digital leaders. Capabilities within the law enforcement and intelligence communities should be continually reviewed to ensure Ireland contributes to European and global cyber defences at the highest levels.

Bibliography

BBC News (2017) ‘Russia a “new risk” to undersea cables’, *BBC News*, 15 December. Available at: http://www.bbc.co.uk/news/uk-42362500 (Accessed: 18 December 2017).

Bielenberg, K. (2017) ‘Explainer: Ireland joins PESCO... is it the start of an EU army?’, *Irish Independent*, 17 December. Available at: https://www.independent.ie/irish-news/explainer-ireland-joins-pesco-is-it-the-start-of-an-eu-army-36409443.html (Accessed: 18 December 2017).

Calnan, D. (2014) ‘An Garda Siochana team up with Europol in largest crime-targeting operation in EU history’, *Irish Independent*, 24 September. Available at: https://www.independent.ie/irish-news/an-garda-siochana-team-up-with-europol-in-largest-crimetargeting-operation-in-eu-history-30612195.html (Accessed: 18 December 2017).

Department of Communications Energy and Natural Resources (2013) *National Digital Strategy for Ireland - Doing more with Digital*. Available at: https://www.dccae.gov.ie/en-ie/communications/publications/Documents/63/National Digital Strategy July 2013 compressed.pdf.

Department of Communications Energy and Natural Resources (2015) *National Cyber Security Strategy 2015-2017*. Available at: http://www.dcenr.gov.ie/communications/SiteCollectionDocuments/Internet-Policy/NationalCyberSecurityStrategy20152017.pdf.

Department of Defence (2015) ‘White Paper on Defence’, (August), pp. 1–143. Available at: http://www.defence.ie/WebSite.nsf/WP2015E.

Department of Public Expenditure and Reform (2015) *Public Service ICT Strategy Overview*. Available at: http://ictstrategy.per.gov.ie/ictstrategy/files/Public Service ICT Strategy.pdf.

Department of Public Expenditure and Reform (2017) *eGovernment Strategy 2017 – 2020*. Available at: http://egovstrategy.gov.ie/wp-content/uploads/2017/07/eGovernment-Strategy-2017-2020.pdf.

Donnelly, E. (2017) 'Irish firms increase cyber security after WannaCry attack', *Irish Independent*, 8 August. Available at: https://www.independent.ie/business/technology/irish-firms-increase-cyber-security-after-wannacry-attack-36011128.html (Accessed: 18 December 2017).

Donnelly, E. and Lynott, L. (2017) 'US urges greater global co-operation in protection of cyber-security', *Irish Independent*, 5 November. Available at: https://www.independent.ie/business/technology/us-urges-greater-global-cooperation-in-protection-of-cybersecurity-36290364.html (Accessed: 18 December 2017).

Edwards, E. (2017) 'State's cyber security centre launches major recruitment campaign', *Irish Times*, 25 July. Available at: https://www.irishtimes.com/news/ireland/irish-news/state-s-cyber-security-centre-launches-major-recruitment-campaign-1.3166209 (Accessed: 17 December 2017).

European Commission (2015) *Combating Cybercrime: EU-wide rules against cyber attacks come into force*. Available at: https://ec.europa.eu/home-affairs/what-is-new/news/news/2015/20150904_1_en (Accessed: 17 December 2017).

European Commission (2017a) *Country Profile Ireland. Europe' s Digital Progress Report 2017*. Available at: https://ec.europa.eu/digital-single-market/en/scoreboard/ireland.

European Commission (2017b) *EU Digital Progress Report Ireland - 2017 Telecoms chapter*. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=44447.

Government of Ireland (1998) *Offences Against the State (Amendment) Act 1998*. Available at: http://www.irishstatutebook.ie/eli/1998/act/39/section/9/enacted/en/html#sec9.

Government of Ireland (2005) *Criminal Justice (Terrorist Offences) Act 2005*. Available at: http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/html.

Government of Ireland (2017) *Criminal Justice (Offences Relating to Information Systems) Act 2017*. Available at: http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/index.html.

Ireland’s National Steering Group (no date) ‘A framework for major emergency management’. Available at: http://www.mem.ie/memdocuments/a framework for major emergency management.pdf.

Ministry of Public Safety (2010) *Canada’s Cyber Security Strategy*. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Mulligan, J. (2016) ‘Microsoft given the green light for four Dublin data centres in €900m project - Independent.ie’, *Irish Independent*, 13 May. Available at: https://www.independent.ie/business/jobs/microsoft-given-the-green-light-for-four-dublin-data-centres-in-900m-project-34710317.html (Accessed: 16 December 2017).

O’Brien, T. (2017) ‘Amazon’s €900m Dublin data centre to run on renewable energy’, *Irish Times*, 26 September. Available at: https://www.irishtimes.com/news/ireland/irish-news/amazon-s-900m-dublin-data-centre-to-run-on-renewable-energy-1.3234995 (Accessed: 16 December 2017).

Office of the Taoiseach (2017) *National Risk Assessment 2017 Overview of Strategic Risks*. Available at: https://www.taoiseach.gov.ie/eng/Publications/Publications_2017/National_Risk_Assessment_2017_–_Overview_of_Strategic_Risks.html.

Percival, G. (2017) ‘Remote air traffic control systems set for Irish airports’, *Irish Examiner*, 3 February. Available at: http://www.irishexaminer.com/business/remote-air-traffic-control-systems-set-for-irish-airports-441932.html (Accessed: 18 December 2017).

PwC (2017a) *Economic crime: A rising threat in Ireland - PwC 2016 Irish Economic Crime Survey*. Available at: https://www.pwc.ie/publications/2016/pwc-irish-economic-crime-survey.pdf.

PwC (2017b) *Irish Digital IQ Survey - 2017*. Available at: https://www.pwc.ie/publications/2017/irish-digital-iq-survey.pdf.

Retel, S. (2014) *Estonia's Cyber Security Strategy (2014-2017)*. Available at: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

Nimmons Consulting Ltd

Strategic Thinking in a Complex World
Web: https://www.nimmonsconsulting.com

About the Author

Steve Nimmons is consultant and writer.

He is a

- Patron of the Royal Institution of Great Britain (Electric Circle)
- Chartered Fellow of the British Computer Society (FBCS CITP)
- Fellow of the Institution of Engineering and Technology (FIET)
- Certified European Engineer (Eur Ing)
- Chartered Engineer (CEng)
- Fellow of the Royal Society of Arts (FRSA)
- Fellow of the Linnean Society (FLS)
- Fellow of the Society of Antiquaries of Scotland (FSA Scot)

His interests include:

- Digital Innovation and Digital Transformation in Defence, Security and Policing
- Complex Problem Solving
- International Relations
- Counterterrorism & Smart Cities
- Cyber Security