Cyber Deterrence: A Comprehensive Approach?

Dr Joe Burton[1]
Visiting Researcher, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)
Senior Lecturer, New Zealand Institute for Security and Crime Science, University of Waikato

Introduction

There are three recent examples of deterrence failure that are worth noting at the outset of this article. The first relates to the events of September 11, 2001 in New York and Washington, DC. The terrorist attacks on 9/11 were perpetrated by a group of individuals who did not fear the consequences of their actions, including any reprisals or punishment. Their fanatical commitment to martyrdom rendered them immune to one of the core dynamics that has kept the US homeland safe throughout its history – a credible deterrent based on a commitment to use military power in defence of US interests. The second, more recent, example relates to the former CIA analyst and National Security Agency (NSA) contractor, Edward Snowden. In May 2013, Snowden was responsible for one of the biggest data leaks in US history, releasing hundreds of thousands of classified national security documents. The revelations created a serious political controversy over the practice of mass surveillance by US national security agencies. Snowden made a seemingly rational calculation that the benefits associated with the release of classified data (including the public's right to know about NSA surveillance) outweighed the costs of his actions to him personally and to the reputation and national security of the United States.[2] The third example is the Russian annexation of Crimea in February, 2014. The Russian military occupied the Crimean Peninsula at a speed that caught the international

[1] I would like to thank Clare Lain, Merle Maigre, Lauri Lindström, Michael Widmann, Ihsan Tolga, Veronika Lantenhammer, and Simona Soare for their helpful comments and feedback on the paper while it was in development. I would also like to thank the CCD COE for hosting me while I conducted this research.

[2] Snowden's motivations were outlined in early reporting by the *Guardian*, in which he refers to the range of factors that influenced his decision. See: Greenwald, G., MacAskill E. and Poitras, L. (2013). 'Edward Snowden: the whistle-blower behind the NSA surveillance revelations', *The Guardian*, available online: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, accessed 11 January 2018.

community by surprise and Russian forces continue to fight a hybrid war in eastern Ukraine characterised by subversion, cyber-attacks, misinformation and propaganda, and the covert infiltration of Special Forces. The actions of the Putin government have been interpreted as a fundamental challenge to the post-Cold War European order. They also signal a failure of deterrence.[3] The control of the Crimean peninsula and the message that the actions sent about Russian interests in the region were seen by the Putin government as benefits exceeding any potential costs imposed on Russia by the government of Ukraine or Russia's perceived adversaries in the West.

Each of these cases has had a profound impact on international security and they all raise important questions. How can suicide terrorism be deterred? What measures can be put in place to deter employees of national security agencies from divulging state secrets?[4] What can be done to deter the Russian government from similar hostility towards other European states? Subsequent to each of the three cases, specific measures have been put in place to strengthen deterrence, including increased border and aviation security in the US, enhanced NSA safeguards against data leaks, and efforts by NATO to bolster its eastern flank and reassure its eastern allies. Just as importantly, the three cases illustrate the complexity of creating and sustaining effective deterrence measures in the post-Cold War era, a period in which the diversity of threats to national security has grown and the diversity of actors with the capacity to have an impact on international security and stability has expanded. Deterrence must now include actions that target a range of globalised security threats that defy borders, including threats from non-state actors such as terrorist groups and criminal gangs, insider threats from whistle-blowers within national security organisations, and threats from revisionist state actors using hybrid tactics to pursue their political and strategic goals.

When placed in the context of cyber security, this level of deterrence complexity is equally apparent and similar questions apply. Cyber-attacks are growing in frequency and

[3] Takacs, D. (2017). 'Ukraine's deterrence failure: Lessons for the Baltic States', *Journal on Baltic Security*, Vol. 3 No. 1, pp. 1–10.

[4] The US Department for Homeland Security has issued specific guidance on combating insider threats, which emphasises deterrence very prominently. See US Department for Homeland Security (2014). 'Combating the Insider Threat', available online: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf, accessed 24 January 2018.

sophistication and having an increasing impact on politics, societies and economies. In the last year, the spread of the *Wannacry, Petya* and *Notpetya* viruses caused direct and indirect damages costing billions of dollars.[5] A rapidly spiking global market in cyber crime[6] has shown that cyber criminals are prepared to use malicious cyber tools with seemingly little consideration of laws and punishment. The alleged Russian subversion of the US 2016 presidential campaign through cyber espionage and dissemination of propaganda on social media has created an ongoing political crisis at the highest levels of the US government. Despite a growing amount of scholarly and policy attention to how these kinds of activities can be deterred, little progress seems to have been made in building effective deterrence against cyber threats. State and non-state actors continue to act with an unacceptable level of impunity in using the internet for malicious purposes.

This paper addresses these issues by posing two related questions: given the diversity of actors, threats and motivations involved, is deterrence against cyber-attacks possible? And if it is, how can effective cyber deterrence be built and sustained? These questions are important to both academic and policy debates. If progress is not made on deterring malicious activity online, the costs and consequences of cyber-attacks will continue to grow and continue to cause instability within the international system. The academic debate on cyber deterrence also appears to be unresolved, with some analysts advocating the view that the deterrence concept should be stretched,[7] some that it should be ditched altogether,[8] and others that cyber deterrence should be a limited approach applicable only to state actors and high-level strategic threats.[9]

[5] Berr, J. (2017). 'WannaCry' ransomware attack losses could reach $4 billion' CBS News, available: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, accessed 10 January 2018.

[6] The Asia Pacific region has seen a 45% growth in cybercrime year-on-year. See: Markets Insider (2017), 'Global Cybercrime Levels Reach All-Time High with a 45 Percent Rise in Attacks for the Asia Pacific Region, Reveals ThreatMetrix Report', available: http://markets.businessinsider.com/news/stocks/Global-Cybercrime-Levels-Reach-All-Time-High-with-a-45-Percent-Rise-in-Attacks-for-the-Asia-Pacific-Region-Reveals-ThreatMetrix-Report-1002267756, accessed 10 January 2018.

[7] Nye, J. S. Jr. (2016/7). 'Deterrence and Dissuasion in Cyberspace', *International Security,* Vol. 41 No. 3, pp. 44–71.

[8] Fischerkeller, M. P. and Harknett, R. J. (2017). 'Deterrence is Not a Credible Strategy for Cyberspace', *Orbis,* Vol. 61 No. 3, pp.381-393.

[9] See Cycon 2017. 'Panel on Cyber Deterrence', available: https://www.youtube.com/watch?v=rvSWAJQQvSs&list=PLtUuPz3a0Gz8dihTzZ-eAuLMHMlmprrpt&index=20, accessed 24 January 2017.

The overarching argument of this paper is that cyber deterrence is possible if the concept is conceived more broadly. In particular, as these three examples illustrate, the diversity of actors, the range of emerging technologies and the range of motives behind malicious cyber activity should be considered more fully in cyber deterrence strategies. To enhance cyber security, cyber deterrence should be a comprehensive strategy that considers the full spectrum of cyber threats and moves beyond narrow conceptions of national and military security. This is not an argument that a blanket approach to cyber deterrence should be applied to all cyber security threats across all sectors, or that military-strategic cyber deterrence is redundant. Instead, deterring diverse cyber threats requires that deterrence be tailored and customised to different actors across the societal, state and international spectrum. Traditional conceptions of deterrence may still have utility in deterring high-level strategic threats (and are arguably already doing so) but will likely not have an impact in an increasingly diverse and complex cyber security landscape.

The paper proceeds in three sections. Section one presents an analysis of existing thinking and theorising around cyber deterrence and highlights aspects of the debates that are mired in Cold War thinking and burdened by comparisons to nuclear and conventional deterrence. It argues that historical analogies have clouded strategic thinking on cyber deterrence and that in some cases the wrong lessons have been learned from deterrence history, and it explains why cyber deterrence based on a limited conception of national security is too restrictive. The second section explores wider, deeper and differentiated approaches to cyber deterrence. It suggests that building cyber deterrence requires a comprehensive and tailored approach to cyber security, one which includes a range of political, social, economic, technological and legal responses that are designed to deter a broader range of threats and actors with tailored and targeted countermeasures. This section refutes the widespread view that deterrence should only be focused on state actors, and the related view that the threat from non-state actors is largely inconsequential. The third section of the article addresses Russian cyber subversion of the US presidential election campaign in 2016. The US election case demonstrates the need for a more comprehensive approach to cyber deterrence and highlights the opportunities that might stem from a broader cyber deterrence strategy.

Cold War thinking and cyber deterrence

Deterrence can be defined as ‘dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.’[10] In the cyber security sphere, ‘doing something’ equates to attacking, manipulating, exploiting and/or gaining unauthorised access to computer systems and networks. Effective deterrence is generally understood to rely on three factors: the capabilities of the affected party to respond, the credibility of that response, and the communication of that threat to the attacker.[11] The concept of deterrence has been used frequently in debates about conventional and nuclear security, and during the Cold War period a substantial body of literature on deterrence theory emerged. Perhaps its most prominent exponents were Thomas Schelling and Glen Snyder. Schelling noted that deterrence based on rational assessments of the costs and benefits had a history that predated the nuclear age and argued that a balance of deterrence in the Cold War between two fairly equally matched sides could lead to a higher degree of stability.[12] Glenn Snyder went further, outlining distinctions between deterrence by denial – measures taken to deny the Soviet Union the ability to achieve its military and political objectives, and deterrence by punishment – that Soviet aggression would be punished through retaliatory strikes, making Soviet military action, including the use of nuclear weapons, inconceivable.[13]

The Cold War was a golden age for strategic studies and the quality of the work stands the test of time in many ways. But there are various problems in applying Cold War deterrence approaches to cyber security.

First, deterrence during the Cold War may not have had the impact that scholars and policy-makers thought it did. In this sense, there is danger of drawing on the Cold War and deriving the wrong lessons from deterrence theory rather than the right ones. Keith Payne argues that

[10] Nye (2017), p.44-71.

[11] Lupovici, A. (2016). ‘The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward’, *International Studies Perspectives*, Vol. 17 No. 3, pp. 322–342.

[12] Schelling said, ‘… governments throughout history have undoubtedly been deterred from military attack and attempted conquest by the possibility of military defeat or the prospect of a war too costly to make even victory seem attractive.’ Quoted in Ayson, R. (2004), *Thomas Schelling and the Nuclear Age: Strategy as Social Science* (Frank Cass: London).

[13] Snyder, G. H. (2015), Deterrence and Defense: Toward a Theory of National Security, Princeton University Press, p.14.

deterrence hinges on an expectation that actors will act rationally, and highlights various Cold War crises where they did not, including the Cuban Missile Crisis where US policy-makers were caught by surprise by Khrushchev's decision to place nuclear weapons in Cuba. In this and other Cold War cases, US foreign policy-makers 'failed to take seriously the prospect for, and thus to prepare for, what seemed in Washington to be highly unreasonable foreign behaviour'.[14] The diversity of actors involved in cyber security suggests that rational, cost benefit approaches to decisions to use cyber capabilities may not always be present, and other motivations may take precedence, including ideological considerations, a desire to cater for internal domestic audiences rather than external ones, and national honour and sovereignty.[15]

A related problem with deterrence thinking during the Cold War was that the effects of deterrence and its reliability were difficult to test empirically. That the Soviets did not invade West Berlin may have been due to deterrence (both nuclear and conventional), but that cannot be proven in absolute terms. It is arguably more difficult to prove the effects of deterrence strategies in cyberspace. Evidence of cyber-attacks and malicious presence on the web is transitory and temporary, with malicious code concealed, adapted, modified, and diffused in ways that are not easy to track and trace.[16] The tendency of governments to overclassify information pertaining to cyber threats and reluctance in the private sector to report malicious cyber activity have further compounded the problem of determining cyber effects and their strategic outcomes.[17]

There are various other practical and conceptual reasons why deterrence thinking is not so easily translated to new cyber security debates and technologies. On the deterrence by punishment side, the problem of attribution is a perennial one. Simply stated, if an attacker cannot be identified they cannot be punished. Cyber deterrence by this line of argument is not impossible, as will be discussed later in this article, but is limited by a number of factors, including that actors can easily deny involvement in cyber attacks, that evidence is difficult

[14] Payne, K. (2003). 'The Fallacies of Cold War Deterrence and a New Direction', *Comparative Strategy*, Vol. 22 No. 5, p. 412.
[15] Ibid., p. 413.
[16] See Valeriano B. and Maness R. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. (Oxford University Press: Oxford).
[17] Kello, L. (2013). 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security*, Vol 38 No. 2, pp. 7-40.

and slow to gather, analyse and disseminate, and that convincing wider audiences that attribution is exact and accurate is problematic, especially when publicising intelligence analysis can harm sources and reveal methods.[18] In the deterrence by punishment paradigm, communicating the credibility of punishment threats is integral to deterrence success. If an attacker cannot be convinced that its target's ability to strike back is credible, then deterrence will not be effective. If a cyber response or countermeasure is deployed through cyberspace to signal displeasure and to communicate a message, and that retaliation is not visible (an internet outage is reported, for example, but not seen or heard), then the deterrence effect is harder to achieve. The right lesson from history is that if nuclear deterrence was effective it was partly due to the visual horror of nuclear explosions and the damage they wrought. Cyber effects are not visible and do not create the same shock value.

Conducting cyber attacks as responses can also cause significant collateral damage. This is a danger inherent in the use of many offensive cyber capabilities. The *Stuxnet* virus, for example, spread to some 100,000 computers beyond Iran[19] and there are derivatives and variants of the code still in use today.[20] Malware can also be reverse engineered after being used, and hackers have learned how to infiltrate, attack and exploit computer systems based on deployed code.[21] Creating cycles of damaging malware duplication is a danger inherent in the deterrence by punishment paradigm. A further problem is the possibility that deterrence by punishment may lead to escalation by dragging in third parties (both state and non-state actors) who respond to the punishment measures by coming to the defence of the target. As Herbert Lin argues, escalation in cyberspace may be less easy to manage and mitigate due to the lack of transparency in cyber activity, the uncertainty about the extent and damage of cyber attacks,

[18] Ibid., p. 26.

[19] Langner, R (2013). 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve', available: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, accessed 10 January 2018.

[20] Symantec (2011). 'W32.Duqu: The Precursor to the Next Stuxnet, Symantec Security Response Symantec Employee', available online: https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet, accessed 10 January 2018.

[21] Langner (2013), p. 19.

the lack of cyber confidence building measures currently in effect between states, and the potential involvement of non-state actors in the escalation of cyber conflict.[22]

The ability to craft a proportional cyber response to an attack is also problematic. A cyber response or retaliation at a low threshold is unlikely to be effective in deterring attacks. This has led some authors to argue for a form of cross-domain deterrence, in which states respond in the other operational domains of land, sea, air and space.[23] But it is hard to see what threshold an attack would need to reach to be met with a kinetic military response. Defining and signalling a threshold also creates the problem that hackers may feel they have a licence to conduct attacks below that threshold. This relates to the idea of strategic ambiguity; the US strategy for the defence of Taiwan, for example, hinges on China's uncertainty about whether and how the US will respond to an attack or occupation. The argument here is that keeping an attacker in the dark about the response threshold creates a deterrent in itself. A state that fails to strike back may also lose stature in the eyes of the attackers, and this may undermine the credibility of deterrence based on ambiguity of response. As Martin Libicki explains, 'If a state leans too far forward in promising reprisals in response to cyber attacks and cannot deliver, its ability to deliver against all other threats may be further doubted'.[24]

A further problem with the deterrence by punishment approach is that cyber-attacks used as retaliatory measures (a so-called 'hack back') may erode the normative environment around the use of cyber capabilities and further legitimatise cyber attacks as a tool of statecraft. In this sense, the adoption of an offensive cyber strategy may hinder progress towards cooperative cyber security measures and present opportunity costs to other cyber security strategies. Chris Macintosh has argued that the military responses to the threat posed by Al Qaeda and its affiliates undermined the legal ones.[25] In the same way, preparing for a long-term militarised cyber deterrence posture may incur the same opportunity costs and undermine civil and

[22] For the fullest exposition of the dangers and escalation resulting from offensive cyber-attacks, see Lin, H. (2012). 'Escalation Dynamics and Conflict Termination in Cyberspace', *Strategic Studies Quarterly*, Vol 6 No. 3, pp. 46-70.

[23] Gartzke, E and Lindsay, J. (2014). 'Cross Domain Deterrence: Strategy in an Era of Complexity', available: http://deterrence.ucsd.edu/_files/LindsayGartzke_ConsequencesofComplexity_Draft.pdf, accessed 10 January 2018.

[24] Libicki, M. C. (2011). 'The Strategic Uses of Ambiguity in Cyberspace', *Military and Strategic Affairs*, Vol. 3, p. 9.

[25] McIntosh, C. (2015). 'Counterterrorism as War: Identifying the Dangers, Risks, and Opportunity Costs of U.S. Strategy Toward Al Qaeda and Its Affiliates', *Studies in Conflict & Terrorism*, Vol. 38. No. 1., pp. 23-38.

criminal approaches that could yield greater benefits. Such an approach could also lend momentum to the emerging cyber security dilemma; as Ben Buchanan argues, states that invest in both defensive and offensive cyber capabilities may exacerbate fear and mistrust in the international system, which could lead to greater proliferation pressures and cyber arms races.[26]

The problems associated with creating strategies founded on deterrence by punishment have created a preference in many quarters for cyber deterrence by denial. This is reflected in the massive investment in defensive cyber security measures throughout the developed world, and this approach has been a central part of NATO's emerging cyber security strategy.[27] But is denying an attacker the ability to achieve their aims achievable in cyberspace? Just as with the deterrence by punishment approach, several problems emerge. First, it is a largely passive strategy that does little to address the actions and motivations of the attacker. The political need to be proactive in responding to cyber security threats runs counter to deterrence by denial approaches. A second and more fundamental problem is the large 'attack surface' the internet presents. It is difficult in many advanced, democratic states to achieve deterrence by denial due to increased vulnerability caused by high levels of internet penetration, the presence of digitally reliant economies, and a high proportion of critical infrastructure being in the private domain and outside government control. As Jamie Shea has recognised:

> 'This vastly complicates the task of defenders, who can rarely know in advance that an attack is being launched, where it will strike or where it will originate. So the defender has to try to protect every important part of the national economic or military infrastructure all the time, while the attacker can choose the individual segment or vulnerable fault line that he wishes to disrupt'.[28]

Relatedly, the number of internet connected devices is projected to grow from 21 billion today to around 75 billion by 2025.[29] The rapid growth in the Internet of Things (IoT) brings security implications and new vulnerabilities across the governmental, military, and societal sectors.

[26] Buchanan, B. (2016). The Cybersecurity Dilemma: Hacking, Trust and Fear Between nations (New York: Oxford University Press).

[27] Burton, J. (2015). 'NATO's cyber defence: Strategic challenges and institutional adaptation', *Defence Studies*, Vol. 15 No. 4, pp. 297.

[28] Shea, J. (2016). 'Resilience: a core element of collective defence', available online: https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm, accessed 11 January 2018.

[29] Statistica (2018). 'Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)', available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed 11 January 2018.

Securing a vast array of hardware, software, cables, connections and devices is an ambitious task. This is especially true when we recognise that humans create an enlarged attack surface through our use and misuse of internet connected technologies. In general terms, humans are prone to error and laziness, are unwilling to invest funds in cyber security, and suffer from the belief that 'it won't happen to us'. Many of the high-profile cyber security incidents of the past decade, including the Snowden case, have human as well as technological causes. Eliminating malfeasance, carelessness or error in working with computer networks is an unrealistic aspiration.

New thinking: building a comprehensive approach to cyber deterrence

Cyberspace has presented a challenge to strategy and policy because it is difficult to think about a radically new technology without analogies to the security environment of the Cold War, where territorial and geopolitical considerations were paramount to policy-makers. Modern deterrence theory was founded in debates about the control and defence of physical territory from a geographically proximate security threat (the Soviet Union) and not a globally connected system of computer networks with both physical and virtual layers. This is particularly evident in the deterrence by punishment and denial paradigms, in which cyber deterrence is viewed as a binary strategy to be applied to state actors within a context of geopolitical competition. Much of the recent cyber deterrence debate has occurred in a particular historical context, moreover, in which Russian hostility in Ukraine has raised the spectre of the Cold War and in which China has used cyber capabilities to advance its geopolitical interests. This may have encouraged path dependency – a tendency to stick with old strategies because of the perception that they have worked before in deterring similar threats. However, the use of Cold War analogies and state-centric thinking in the scholarly and academic fields may constrain new thinking and reinforce previously held views about security.[30] The presence of groupthink, with academics from the security and strategic studies

[30] Betz, D. and Stevens, T. (2013), 'Analogical Reasoning and Cyber Security', *Security Dialogue*, Vol. 44 No. 2, p. 149.

disciplines dismissing other perspectives and talking with each other inside a ‘walled garden’, is also a concern.[31]

Given the limitations of traditional deterrence thinking when applied to cyber security, can cyber deterrence ever be achieved? Despite the issues outlined above, there remains considerable hope that cyber deterrence can be a useful and effective strategy, especially when conceived of more broadly. Several recent analyses of cyber deterrence have attempted to move the debate forward in such a way. Amir Lupovici, for example, argues that current research has too limited a view of what cyber deterrence is, and seeks to redefine the concept as a socially constructed process that relies on intersubjective interpretations of motives, means and actions.[32] Through an analysis of the *Stuxnet* attack, Lupovici contends that cyber deterrence is not based on the characteristics of cyberspace – anonymity, for example – but on adherence or disobedience to social norms. When attributing cyber-attacks, the identity of the attackers can be derived from social context: in the *Stuxnet* case, the historical relations between Iran, Israel and the US. According to this line of thinking, attribution can be determined technically, but it can also be established through an examination of the history, culture and politics of the attack and its causes and consequences.

Technology may also evolve in a way that makes attributing cyber-attacks less problematic. Attribution could become easier by limiting the anonymity of web traffic, for example. The United States government has suggested that the internet could be redesigned and engineered to make it an ‘identified and attributed network, where logging in entails specific personal verification.’[33] It is outside the scope of this article to examine the likelihood or implications of such a fundamental change to the way the internet operates, but this is indicative of a wider range of thinking about how one of the central problems with cyber deterrence might be resolved.

The level of investment in attribution technologies also suggests progress in attempts to close the attribution gap. The US government is funding research that could address some of the

[31] Ibid., p. 159.

[32] Lupovici (2016).‘The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward’, *International Studies Perspectives*, Vol. 17 No. 3, p. 338.

[33] Ibid., p. 330.

main issues involved in cyber attribution, particularly the speed and accuracy of the attribution process.[34] The last budget of the Obama administration in February 2016 assigned $19 billion for cyber security, including long term (7-15 year) investment to develop science and technology for 'effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution'.[35] This built on the 2015 Department of Defence strategy for cyberspace, which placed a premium on the importance of attribution to cyber deterrence of both state and non-state actors.[36]

There are various other compelling arguments for maintaining cyber deterrence as a concept and strategy and widening deterrence theorising and application to a less binary and more comprehensive range of threats and actors outside the military and strategic sphere. The first and most obvious is that cyber vulnerabilities are society-wide, and attacks on critical infrastructure, often in private hands, can have immediate and consequential national security implications. Deterring attacks against banking and financial institutions, energy facilities, transport infrastructure and other vital public services has become as important as deterring state-based attacks against military-strategic targets. If the targets of attacks are wider, then it is logical that deterrence strategies should be too.

Malicious cyber activity also exists across a broad spectrum of activity and almost invariably falls below the threshold of a 'use of force' or 'armed attack'. The targets of cyber attacks are diverse, but so too are the types of malicious cyber activity. The growing use of hybrid warfare tactics, 'grey zone' incidents that target civilian infrastructure, the growth of the use of the internet for criminal and financial gain, espionage, subversion, coercion, cyber protest and hacktivism, all suggest that deterrence needs to be focused on a broader range of activities and actors with a diverse array of motivations. Focusing on deterring military-strategic cyber security threats from state actors will only ever capture a diminutive proportion of the overall scope of malicious cyber activity. Cyber threats are also characterised by their ability to cross

[34] Toon J. (2016). '$17 Million Contract Will Help Establish Science of Cyber Attribution', available online: http://www.news.gatech.edu/2016/11/29/17-million-contract-will-help-establish-science-cyber-attribution, accessed 11 January 2018.
[35] Naegele, T. (2016). '7 Keys to President Obama's $19 Billion Cybersecurity Plan' available: https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.5Cre8GU, accessed 11 January 2018.
[36] Lindsay, J. L. (2015). 'Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, Vol. 1 No. 1, p. 62.

borders and blur the boundaries between the societal, state and international levels of analysis. Some threats will be within a state, such as in the Snowden case where an insider caused a major information security breach, some will be state-based, and some will be global and come from transnational organisations including terrorist groups and organised criminal enterprises that form complex networks of illicit international activity. To discount the applicability of cyber deterrence to this broad range of activities and actors would be extremely counterproductive.

Underpinning a more comprehensive approach to cyber deterrence is the efficacy of both domestic and international law in helping to constrain cyber threats and the corresponding development of international norms of behaviour. The pursuit of legal and normative approaches to cyber deterrence may seem counterintuitive considering the recent failure of the UN GGE to reach consensus on the applicability of existing international law to cyberspace,[37] but the prospects for legal and normative deterrence remain considerable. Legal deterrence has long been an established approach to criminal acts, and debates in the historical legal literature have mirrored those in the security field.[38, 39] More recent legal analyses of cyber deterrence have offered important insights that sit outside the military sphere, including how to break down legal obstacles to data sharing on cyber threats between government and private entities.[40] Recent cases have also demonstrated that governments see the use of legal instruments as relevant in shaping the behaviour of attackers. The US indictment of five PLA members in 2014 is a prominent example of legal measures being used to deter cyber criminality. Despite its obvious usefulness in deterrence of a variety of actions, consideration of the impact of domestic and international law has been peripheral to the security and strategic studies literature.

[37] Korzak, E. (2017). 'UN GGE on Cybersecurity: The End of an Era?', available: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/, accessed 11 January 2018.
[38] Ball, J. C (1955). 'Deterrence Concept in Criminology and Law', *Journal of Criminal Law and Criminology*, Vol. 46 No. 3, pp. 347-354.
[39] Rid, T. (2012). 'Deterrence beyond the State: The Israeli Experience', *Contemporary Security Policy*, Vol 33 No. pp. 124-147.
[40] Davis, J. E.; Brown, G. (2016). 'The Emergence of Cyber Deterrence: Implications for International Law' American Society of International Law, available online: https://www.questia.com/library/journal/1G1-493794377/the-emergence-of-cyber-deterrence-implications-for, accessed 11 January 2018.

Wider interpretations of cyber deterrence also rest on an acceptance that expanding the concept to a greater range of actors and threats may make the concept more prone to failure. Some deterrence failures should be expected. Deterrence is an imperfect strategy in law just as in military strategy. As Eric Sterner argues:

> 'Law enforcement accepts imperfect deterrence as the nature of the beast rather than dismissing the concept entirely. Deterrence is not a military concept per se.'[41]

Increasing the costs of cyber-attacks and decreasing the benefits through a variety of mechanisms can be an incremental strategy that achieves results through persistence. In this sense, deterrence is not a binary concept and imperfect deterrence is better than no deterrence at all. Again, the presence of Cold War thinking may have hindered the development of cyber deterrence strategies. During the Cold War, deterrence was *absolute,* in that even one attack by the Soviet Union would have proven devastating. While such an approach may still be relevant for high-level strategic attacks, in a more comprehensive and tailored strategy, cyber deterrence will be *restrictive*, in that it seeks to limit the overall frequency and severity of attacks, and shape the behaviour of the attacker.[42] As Uri Tor argues, cyber deterrence is about how to 'postpone, limit, and shape a series of ongoing conflicts with a variety of state and sub-state actors'[43] rather than preventing all attacks occurring at all times.

Non-state actors and cyber deterrence

Any analysis of the broadening of cyber deterrence as a concept and its application to a wider degree of challenges must consider the prospects for deterrence strategy to be effective when directed at non-state actors and the seriousness of the cyber threat they pose. The prevailing assumption has been that if deterrence is difficult when applied to nation states, then it is even more difficult with non-state actors, who are less bound by rules and norms in their international interactions, who operate under different assumptions and preferences, who accept greater levels of risk, who have a higher tolerance for punishment measures, and who

[41] Sterner, E. (2011). 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly*, Vol. 5, No. 1, pp. 62-80.

[42] Tor, U. (2017). 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies*, Vol. 40 No. 1-2, p. 93.

[43] Ibid., p. 93. Tor limits his analysis in the article to state actors, but the idea of full spectrum, non-dichotomous deterrence is prominent in his ideas.

may in some cases welcome retaliatory measures.[44] Other analyses of non-state actors and cyber security have concluded that the cyber threat they pose is minimal and should not be the focus of cyber security or deterrence strategies.[45] Jon Lindsay has argued, 'Given that most attacks tend to fall on the lower end of the value spectrum, conducted for criminal gain, surveillance, or protest rather than physical combat it is unsurprising that many are sceptical of deterrence.'[46] James Lewis takes a similar view, arguing, 'cyber attacks that do not pose existential threats or immense harm to vital interests are not deterrable. This is also true for cyber espionage or cyber crime. They fall below the threshold that would justify a military response.'[47]

But is cyber deterrence against non-state actors possible, and perhaps even more importantly, is it even necessary given the lower threshold at which attacks have occurred in the past? First, although states have certainly developed the most advanced and sophisticated cyber capabilities, cyberspace has clearly become an arena of competition and contestation between states and non-state actors, including social movements, who have used the internet to try and restrict and resist the power of the state and to exercise their own power in pursuance of diverse causes. Recent attention has fallen on relatively new organisations like Anonymous, which have sought to influence the political process through cyber attacks. The ongoing contestation and influence sought by Julian Assange and WikiLeaks is another prominent recent example. In the last several years, WikiLeaks has worked with insiders, state, and state-sponsored hackers to release troves of classified information, with highly consequential impacts on national and international security and stability. Manuel Castells has argued that 'networked social actors aiming to reach their constituencies and target audiences through the decisive switch to multimedia communications networks'[48] have become central to international

[44] Lewis, J. A. (2013). 'Reconsidering Deterrence in Cyberspace', available online: http://csis-prod.s3.amazonaws.com/s3fs-public/131015_Reconsidering_Deterrence_in_Cyberspace.pdf, accessed 11 January 2018.

[45] Through an analysis of the Cyber Gaza, Syrian Electronic Army, and Red October operations, Valeriano and Maness (2015) argue that the impact and long-term damage on targets from attacks by non-state actors is minimal to non-existent.

[46] Lindsay (2015). p. 54.

[47] Lewis (2013).

[48] Castells, M. (2009). *Communication Power*, (Oxford: Oxford University Press) p. 49.

security, and should not be seen as low-level threats. Other analysts have taken a similar view, arguing that:

> ‘states envisaged defending themselves against other states because they were seen as the main threats, whereas ‘hacktivists’ were not perceived to be as dangerous. In hindsight, that assessment was wrong. Non-state hacking is much nearer the top of the threat’.[49]

Some states, most notably Russia and China, have tended to outsource or privatise their cyber-attack capabilities to affiliated groups who will conduct cyber-attacks on their behalf, including patriot hackers or netizens. In this sense, the threat comes not from non-state actors but actors who have connections with the state and are directed by it. This may change the deterrence dynamic in unknown ways and pose questions that are underexplored by cyber security scholars; how do we deter states from outsourcing cyber operations, for example? The recent spread of the *Wannacry* virus shows that state and non-state actors are combining to present a threat to international security and it is the complex relationship between the two that may determine the effectiveness of any cyber deterrence strategy. Analysis of the *Wannacry* code suggests links to the Lazarus group of hackers, which has ties to the North Korean regime.[50]

Some research has begun to address these linkages and their implications for cyber deterrence. Forrest B. Hare, for example, argues that the outsourcing of cyber attacks by states may lead to difficulties in synchronising the private actors’ actions with government objectives, lead to escalation in cyber conflicts, and pose risks to the states themselves, as hackers redirect their activities against domestic and friendly targets.[51] In this scenario, a form of ‘self-deterrence’[52] may emerge within states because of fears of the unintended consequences of encouraging non-state actor activity and the risk that the actions of non-state actors could constitute breaches of international law and lead to sanctions. Recent developments through the NATO CCD COE Tallinn Manual 2.0 process suggest the emergence of a variety of legal measures to deter non-

[49] Quoted in Betz and Stevens (2013), p. 152.

[50] The attacks have now been formally attributed to North Korea by US authorities.

[51] Hare, F. B. (2017). ‘Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?’, *Asian Security*, Online Version: p.6.

[52] For an interesting discussion of this concept as it pertains to nuclear weapon, see: Paul, T. V. (2015), ‘Self-deterrence: Nuclear weapons and the enduring credibility challenge’, *International Journal*, Vol. 71 No. 1, pp. 20-40.

state actors, including tying their activity to states through international legal mechanisms.[53] If non-state actors are seen as operating not in isolation but in connection and interaction with the long-established nation state system, then cyber deterrence may not prove so elusive.

A further common assumption is that non-state actors' motivations and level of rationality make them harder to deter. This view emerges from the post 9/11 era and the wave of suicide terrorism that has plagued international affairs. Terrorist groups' use of the internet for planning, operations, radicalisation and other activities is certainly guided by the fanatical viewpoints of the individual involved and their commitment to extremist ideology. President George W. Bush's words are worth recalling here. In 2006, he said:

> 'The enemies we face today are different in many ways from the enemy we faced in the Cold War. Unlike the Soviet Union, the terrorist enemies we face today hide in caves and shadows … have no borders to protect, or capital to defend. They cannot be deterred'.[54]

Recent research in the counterterrorist literature suggests the level of terrorists' imperviousness to deterrence may be overstated, however. As John Klein has argued:

> 'Some strategists and policy makers believe that acts of cyberterrorism, especially by non-state actors, may prove to be undeterrable. Yet the leadership of both state and non-state actors tend to act rationally and function strategically, and therefore they can, in fact, be deterred to some degree'.[55]

The key to deterrence in Klein's analysis is that the deterrence concept is 'considered holistically' and that 'all available means' are used as deterrence measures, including legal tools and the use of military force. Alex Wilner, in another insightful analysis of the applicability of deterrence to terrorist actors, takes a similar view:

> 'By expanding the scope of traditional deterrence theory and pairing it with more nuanced understanding of contemporary terrorism, a variety of deterrents can be constructed and levied against terrorist organisations. When tailored appropriately, states can use the logic of deterrence to influence, coerce and

[53] See: NATO CCD COE, *Tallinn Manual 2.0*, available online: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html, accessed 11 January 2018.
[54] Bush, G. W. (2006). 'Commencement Address at the United States Military Academy in West Point', available online: http://www.presidency.ucsb.edu/ws/?pid=83, accessed 11 January 2018.
[55] Klein, J. J. (2015). 'Deterring and Dissuading Cyberterrorism', *Journal of Strategic Security*, Vol. 8 No. 4, p. 22.

> deter terrorist groups, delimiting the type and ferocity of the violence those groups are willing to use, and influencing their behaviour more generally'.[56]

A recent cyber example of the types of activity Wilner refers to are efforts to counter radicalisation, particularly relating to social media. Much research is now addressing this important challenge and there have been reports that targeted removal of ISIS twitter accounts has been effective in nullifying the level of activity involved.[57]

When considering threats from terrorist groups, cross domain deterrence (responding to cyber attacks with physical attacks) might also be considered more fully and, under certain circumstances, be more ethically acceptable. In this sense, a particular deterrence strategy would be tailored to groups like ISIS based on the extent of the threat. It is notable that the ISIS hacker who was killed in 2015 by a US airstrike was responsible not only for radicalisation online, but also for the release of details of US personnel in the form of a 'kill list', thus posing a direct threat to US armed forces.[58] This was not an inconsequential or illusory threat. The debate about targeted killings is an ongoing one and outside the scope of this article, but the killing of an ISIS hacker (and the subsequent FBI operation targeting the group's online efforts)[59] communicated a clear message that ISIS manipulation of computer networks and attempts to obtain data on US personnel would be countered with kinetic force if necessary. It would be wrong to assume terrorist groups are impervious to these types of actions.

Deterrence through resilience

The other non-state actors that are pivotal to wider conceptions of cyber deterrence exist within the private sector and are often outside of direct government control (and often under-considered as 'deterring actors' within cyber security strategies). The importance of public-private partnerships in achieving cyber deterrence is receiving greater attention in academic

[56] Wilner, A. S. (2015). *Deterring Rational Fanatics*. Pennsylvania: Pennsylvania University Press), p.2.
[57] Conway, M. et al. (2017). 'Disrupting Daesh: measuring takedown of online terrorist material and its impacts', available online: http://www.voxpol.eu/download/vox-pol_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf, accessed 11 January 2018.
[58] Daftari, L. (2017). 'ISIS hacker who published 'kill lists' reportedly killed in U.S. drone strike', available online; http://www.foreigndesknews.com/world/middle-east/isis-hacker-published-kill-lists-reportedly-killed-u-s-drone-strike/, accessed 11 January 2018.
[59] Goldman, A. and Schmitt, E. (2016). 'One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program', available online: https://www.nytimes.com/2016/11/24/world/middleeast/isis-recruiters-social-media.html, accessed 11 January 2018.

and policy circles. The Obama administration's cyber security strategy referenced plans to use 'partnerships with the private sector to deter, detect and disrupt threats', for example.[60] Cyber deterrence may require a degree of private sector responsibility that has not been in abundant supply to date. Nevertheless, Internet Service Providers and internet content creators may be able to deter cyber-attacks by self-policing and making their networks resilient to malicious use. In this sense, and as Madeline Carr has argued, 'It might be more appropriate to develop a national cyber-resilience strategy instead of a national cyber-security strategy'.[61] 'De-securitising' cyber security in this way may help to emphasise reputational and commercial incentives for companies to make their products safe, secure and free from attack and manipulation. In the absence of independent actions by the private sector to secure computer systems from manipulation, new domestic legislation may also be needed; the Estonian government is considering introducing new laws that would enable the Estonian Information System Authority (RIA) to disconnect malicious actors from using Estonian ISPs, for example.[62]

A wider concept of cyber security based on computer network and societal resilience may also bring benefits to cyber deterrence efforts. This would involve a broad range of actors, including internet service providers, critical infrastructure providers, operators of social media platforms, the military *and* government in a wide and deep effort to ensure service continuity (and the continuity of basic societal functions) in the event of major cyber disruption. If measures can be put in place to keep the internet running, minimise the impact of cyber-attacks, and quickly replace core services, then the perceptions of cyber attackers that they are able to achieve their objectives could be eroded considerably. Inherent to this approach is that deterrence measures become decentralised and involve a broad range of stakeholders. As one recent report notes:

[60] Obama, B. (2016). 'Protecting U.S. Innovation from Cyberthreats.' Available online: https://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003, accessed 11 January 2011.

[61] Carr, M. (2016). 'Public-private partnerships in national cyber- security strategies', *International Affairs*, Vol. 92, No. 1, p. 62.

[62] Lõugas, H., (2017). 'RIA peadirektor saab õiguse ohtlik arvuti Eesti internetist välja lülitada', available online: https://geenius.ee/uudis/ria-peadirektor-saab-oiguse-ohtlik-arvuti-eesti-internetist-valja-lulitada/, accessed 24.01.17.

> 'The concept of resilience replaces the measurement and control of risks with the decentralised and flexible ability to resist varied disruptions and often unforeseen shocks'.[63]

Such a strategy will rely on effective communication and efficient information sharing between government and the private sector, and resilience strategies should not be viewed as replacements for other cyber deterrence approaches, especially as resilience processes are at an early stage of development. Illustrating this point, Tim Ridout has argued for combining resilience with other forms of cyber deterrence:

> 'resilience could play a critical dissuasive role by reducing the utility of cyber offense, especially when joined with the credible threat of punishment. If you demonstrate that you can absorb a blow, bounce back quickly, and then hit back, resilience and deterrence can be a potent combination'.[64]

Resilience may also have more utility in certain sectors than others, such as in transport and energy supply. Critical infrastructure providers with no authority or capability to implement cyber countermeasures may find cyber deterrence based on resilience appealing, especially when supported by government efforts. The US Computer Emergency Response Team's (CERT) *Cyber Resilience Reviews* (no-cost, voluntary, non-technical assessments to evaluate an organisation's operational resilience and cybersecurity practices)[65] are but one example of the sorts of measures that are emerging that could enhance cyber deterrence.

The relevance of resilience to deterrence is receiving more traction within the international community too. The EU's most recent cyber security proposals are titled, *Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*,[66] suggesting a clear interrelationship between the resilience and deterrence concepts. NATO officials have recently recognised that Information Technology 'represents a fundamental pillar of resilience and a critical enabler of decisions taken at Warsaw to strengthen NATO's deterrence and defence

[63] Bendiek, A., Bossong R. and Schulze, M. (2017). 'The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-Reaching Challenges', available: https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf, accessed 11 January 2011.

[64] Ridout, T. (2016), Building a Comprehensive Strategy of Cyber Defence, Deterrence, and Resilience, *The Fletcher Forum of World Affairs*, Vol. 40 No. 2, p.80.

[65] See for example: US CERT (2018). 'Assessments: Cyber Resilience Review (CRR)', available online: https://www.us-cert.gov/ccubedvp/assessments, accessed 22 January 2018.

[66] European Commission (2017). 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' available online: https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf, accessed 11 January 2018.

posture.'[67] If these efforts by international organisations can be complemented at the sub-state level, then significant cyber deterrence progress could be made.

Comprehensive cyber deterrence

What would a comprehensive cyber deterrence strategy look like? Some existing policy documents provide indications. The 2015 DoD Cyber Strategy calls for the Department of Defence to contribute to 'the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests'. The policy refers to 'a range of policies and capabilities to affect a state or non-state actors' behaviour' and highlights that cyber deterrence will be achieved through a:

> 'totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.'[68]

A similar approach is taken in the US Army Special Operations Command White Paper, 2016, which says that:

> 'Comprehensive Deterrence seeks to expand upon traditional concepts of deterrence to account for the totality and the variety of the threats we face in the early 21st Century security environment'.[69]

The strategy suggests constructing a grand strategy for deterrence, based on a wider focus than just high-end conflict by nation states, countering grey zone challenges, recognising trans-regional competition, the necessity for new ways of thinking, and nuanced inter/intra-governmental multi-year campaigns.[70]

[67] Fertasi, N. and De Vivo, D. (2016). 'Cyber resilience: protecting NATO's nervous system,' available: https://www.nato.int/docu/Review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm, accessed 11 January 2018.

[68] Department of Defence (2015). 'The Department of Defence Cyber Security Strategy', available online: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed 11 January 2018, p.10.

[69] US Army Special Operations Command (2016). 'Comprehensive Deterrence White Paper', available: http://www.soc.mil/Files/ComprehensiveDeterrenceWhitePaper.pdf, accessed 11 January 2018, p. 2.

[70] Ibid., p. 2.

In academic circles, the long-established concept of comprehensive security provides some insight into how a comprehensive cyber deterrence strategy might be established. As Gebhard and Norheim-Martinsen explain, comprehensive security concepts have tended to:

> 'focus on widening the conventional perspective on security towards a not purely military, territorial and state-centric understanding, but one that includes other security-relevant aspects such as civilian operations in various areas (police, security sector reform, rule of law, civil protection and civil administration), development, environmental issues, humanitarian aid, structural cooperation and diplomacy'.[71]

More recently, Scott Jasper has outlined some of the necessary attributes of comprehensive cyber deterrence, stressing the importance of 'continuity of purpose not command' between the private sector and government, and the corresponding need to overcome a 'clash of self-interests – where one party strives to maintain economic or military advantage – that might prevent cooperation in deterring cyber aggression.'[72]

Figure 1 suggests a tentative and collaborative framework for cyber deterrence that recognises the range of threats involved in cyber security and the range of targets, makes distinctions between actors who need to be deterred and deterring actors (those engaged in formulating and implementing deterrence strategies), and highlights the variety of measures that can be used depending on the type of threat, target and actor involved. Deterrence measures include a range of existing policies that have deterrent value, including punishment for higher level strategic threats, and denial for lower spectrum activity. The approach recognises that targets will be diverse and the application of deterrence measures will vary accordingly. It also recognises that deterrence measures will be tailored and chosen according to the type of actor to be deterred, the organisations involved in the deterrence activity, and their capabilities and authority.

[71] Gebhard, C. and Norheim-Martinsen, P. (2011). 'Making sense of EU comprehensive security towards conceptual and analytical clarity', *European Security*, Vol. 20 No. 2, pp. 225.
[72] Jasper, S. (2015). 'Deterring Malicious Behavior in Cyberspace', *Strategic Studies Quarterly*, Vol. 9, No. 1, p. 75.

Fig. 1 A comprehensive cyber deterrence framework

Deterring Actors	Deterrence Measures	Threats	Targets	Deterrable Actors
International Organisations Nation states and government agencies Police, Judiciary Private sector, ISPs	*Punishment* Kinetic retaliation, cyber retaliation, legal prosecution, economic sanctions, diplomatic isolation. *Denial* Norms, Societal denial, Technical denial *Resilience* Recovery, contingency, and continuity planning	(absolute deterrence) Cyber warfare Cyber espionage Cyber terrorism Cyber crime (restrictive deterrence)	Military Government, political institutions, values Corporate Critical infrastructure Individuals, public	Nation states, military and security agencies State affiliated hackers Terrorist groups Insider threats Criminals and organised crime

The US election hack, 2016: lessons for cyber deterrence

The use of cyber espionage and subversion by the Russian state during the US presidential election 2016 has clearly demonstrated the destabilising effects that hostile cyber campaigns can have at the highest levels of national and international politics. The investigation into Russian subversion of the election, and the extent to which members of the Trump campaign were involved in that effort, is ongoing. Nevertheless, there have been clear evidence-based indications from the US national security agencies of the extent of the cyber-attacks, the motivations behind them, and their impact. The Office of the Director of National Intelligence (ODNI),[73] in a declassified summary of its investigation, concluded that President Vladimir Putin ordered Russian intelligence agencies to conduct an 'influence campaign' to disrupt the US election, undermine faith in the US political system, denigrate Secretary Hillary Clinton, harm her campaign, and undermine her future presidency.[74] The methods involved in the

[73] Incorporating views from the three main US intelligence agencies, The Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA)

[74] Office of the Director of National Intelligence (2017). 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', available: https://www.dni.gov/files/documents/ICA_2017_01.pdf, accessed 11 January 2018, p. II.

campaign were some of the most highly coordinated in recent history and constituted a 'significant escalation in directness, level of activity, and scope of effort compared to previous (Russian) operations.'[75]

While the election hack could be interpreted as a clear case of cyber deterrence failure, that would be too simplistic an assessment. There are some important lessons to be learned that relate to the arguments for a comprehensive approach to cyber deterrence outlined in this article. The case also suggests several opportunities for the development of cyber deterrence strategy and policy.

First, the attacks were not directed solely at the US state and its governmental actors, and used and targeted non-state actors to achieve political effects. The attacks were directed at both the main US political parties (including the primary campaigns), think tanks and lobbying groups, and hackers infiltrated the Democrat National Committee (DNC) networks from June 2015 to July 2016. Attempts were made to gain and sustain access to electoral systems, including US state and local election boards. Those involved in the attacks included both Russian state actors and intermediaries or proxies, including 'state funded media, third-party intermediaries, and paid social media users or "trolls"'.[76] The attacks were also based on the manipulation of private sector organisations within the US and internationally, most notably Facebook and Twitter. Julian Assange's Wikileaks organisation was used to disseminate materials that had been obtained illegally and covertly from various US sources. The ONDI report notes that Wikileaks actively collaborated with Russia Today (RT), the main propaganda outlet of the Russian state, and that RT executives met with Julian Assange to discuss further partnership between the organisations. It also suggests that, after election day, Russian hackers began a 'spear fishing' campaign targeting a wide range of government and non-government actors, including 'US Government employees and individuals associated with US think tanks and NGOs in national security, defence, and foreign policy fields'.[77] The election hack thus demonstrates that cyber deterrence across both the government and societal sectors will be necessary to prevent and deter future such activity. This may have been a state orchestrated

[75] Ibid., p. II.
[76] Ibid., p. 2.
[77] Ibid., p. 5.

campaign of cyber subversion, but it was implemented by and targeted actors beyond conventional state based structures and agencies.

The second related lesson is that preventing and deterring the manipulation of social media has grown in importance and should be seen as a cyber security issue, and new strategies are needed to enhance the security of social media platforms from manipulation. The social media providers themselves may need to take greater responsibility in this area or risk seeing public trust in their platforms eroded. Since the election, executives from Facebook, Google and Twitter have testified to the US Congress, and have taken some first steps to protect their networks from covert manipulation. This suggests that private sector and social media deterrence by denial is at least on the agenda. It has been estimated that content produced by Russian operatives may have reached as many as 126 million Facebook users, with 36,000 Russian bots responsible for 1.4 million tweets during the election period, and 1,108 videos with 43 hours of content distributed on YouTube relevant to the aims of the Russian operation.[78] Limiting the overall scope of this malicious activity is achievable with tailored deterrence strategies. Various aspects of the role of these content providers relates to the efficacy of a broader approach to cyber deterrence. First, the advertising that appeared on social media that was targeted at undermining Secretary Clinton's campaign was paid for in roubles, a fact recognised by Senator Al Franken at the recent congressional hearings: 'American political ads and Russian money, roubles: How could you not connect those two dots?'[79] This indicates that some changes in practice by social media operators could bring simple deterrent results. One proposed measure currently before the Congress is to require digital service providers to provide publicly listed databases of those purchasing election ads. This would create a degree of transparency that may serve as a deterrent. Another proposal by academics Dan Jerker B. Svantesson and William van Caenegem involves making the covert algorithmic manipulation of social media platforms for dishonest political gain a criminal offence.[80]

[78] Shaban, H., Timberg C. and Dwoskin, E., (2017). 'Facebook, Google and Twitter testified on Capitol Hill. Here's what they said', available https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/?utm_term=.7e90b0e2c269, accessed 11 January 2018.

[79] Quoted in Shaban, Timberg and Dwoskin (2017).

[80] Svantesson, D. J. B. and Van Caenegem, W. (2017). 'Faking it: we should make manipulating algorithms for political purposes a crime, March 9, 2017, available: https://theconversation.com/faking-it-we-should-make-manipulating-algorithms-for-political-purposes-a-crime-73970, accessed 11 January 2018.

Adopting or refining laws may yield enhanced legal deterrence. More proactive removal of manipulative advertising and content has also been considered and Facebook has announced the application of advanced AI technologies to combat fake news, including by de-ranking sites such as Russia Today in search algorithms.[81] Successes have been recorded with similar measures to constrain the use of Twitter by ISIS.[82]

The third lesson that should be derived from the US election hack is the unique vulnerability of democracies to hacking and the need to tailor cyber deterrence accordingly. This was not simply an attack on a nation state by another nation state, but a manifestation of identity politics and ideology, and there have been clear subsequent threats to elections in other countries including Germany, the UK and France. In this sense, a comprehensive cyber deterrence strategy would need to be tailored to protecting democratic values, institutions and systems of governance. Zoe Hawkins has argued that:

> 'to limit our understanding of the cyber threat to physical damage would be to overlook the integral role that cyber technologies play in less tangible elements of national security: democratic elections and supporting public information flows'.[83]

Conversely, in achieving effective cyber deterrence, more attention may need to be placed on what costs are taken seriously by authoritarian leaders who are more insulated from internal democratic constraints on their power than leaders in democracies. The Obama administration in its last months in office expelled Russian diplomats and new sanctions were imposed on Russia's two leading intelligence services, but the coherence and continuity of the US response has been affected by the wider political controversies surrounding the Trump administration during its first year in office.[84] Subsequent to the US sanctions, the EU has announced it will impose sanctions in response to cyber attacks against its members' democratic processes, including travel bans, assets freezes and blanket bans on doing business with a person,

[81] BBC News (2017). 'Facebook promises new fake news measures', available: http://www.bbc.com/news/technology-40812697, accessed 11 January 2018.
[82] Conway et al. (2017).
[83] Hawkins, Z. (2017). 'Securing Democracy in the Digital Age', available online: https://www.aspi.org.au/report/securing-democracy-digital-age, accessed 12 January 2018.
[84] Sanger, D. E. (2016). 'Obama Strikes Back at Russia for Election Hacking', available online: https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html, accessed 12 January 2018.

company or government.[85] This is part of new EU cyber security proposals that place more emphasis on broader conceptions of cyber deterrence and resilience than usually adopted.[86] Another more practical aspect of this problem is the vulnerability of electoral systems to interference and some new research is already emerging on this important aspect of cyber security and deterrence.[87] Recent proposals that could create significant deterrence by denial and resilience involve ensuring supply chain integrity (e.g. voter rolls, voting machines, software, and results) and efforts to ensure that voting systems are backed up by paper ballots or are secured through distributed or duplicated systems that can continue to function in the event of infiltration and manipulation.[88] In a recent report on deterring attacks against election systems, David Fidler concludes that 'layered state, federal, and international actions would deter cyberattacks on election systems by making such attacks more difficult, costly, and ineffective'.[89] Comprehensive approaches to cyber deterrence thus appear to be gaining heightened attention in the wake of the US election hack of 2016 and innovative new approaches to cyber deterrence may emerge as a result.

Conclusion

This article has proposed a comprehensive approach to cyber deterrence that is wider and deeper than many current conceptions and which addresses the diversity of actors, threats and motivations involved in malicious cyber activity. Its central argument has been that relying on binary Cold War conceptions of deterrence (most notably deterrence by denial and punishment) and state-centric conceptions of cyber security is likely to prove ineffective. A tailored approach that recognises the role of a diverse range of deterring actors and deterrable threats,

[85] Reuters Staff (2017). 'EU agrees to use sanctions against cyber hackers', available online: https://www.reuters.com/article/us-eu-cyber-sanctions/eu-agrees-to-use-sanctions-against-cyber-hackers-idUSKBN19A115, accessed 12 January 2018.

[86] Minárik T. and Alatalu S. (2017). 'EU Cybersecurity Package: New Potential for EU to Cooperate with NATO', available online: https://ccdcoe.org/eu-cybersecurity-package-new-potential-eu-cooperate-nato.html

[87] See for example, https://www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-infrastructure-vulnerabilities-solutions/, accessed 12 January 2018.

[88] Zarate, J. C. (2017). 'The Cyber Attacks on Democracy', available online: http://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html, accessed 12 January 2018.

[89] Fidler, D. P., 'Transforming Election Cybersecurity', available: https://www.cfr.org/sites/default/files/report_pdf/CyberBrief_Fidler_Elections_OR_2.pdf, accessed 12 January 2018.

and which includes legal, social, normative and technological approaches to deterrence, could yield greater benefits. A preliminary analysis of the US election case has shown the potential benefits and opportunities that may stem from the adoption of this type of approach.

There are various potential pitfalls and costs to adopting a comprehensive approach to cyber deterrence. The first is time. Embedding norms and laws and achieving resilience will be a lengthy process and require sustained attention. Socially constructed, normative approaches to cyber deterrence will be slow to establish and part of a complex life cycle that includes periods of advocacy, contestation, acceptance, diffusion and localisation. To paraphrase Tim Stevens, cyber security is an inherently temporal proposition.[90] A comprehensive cyber deterrence strategy focused on both state and non-state actors will also need to be well resourced at the societal, state and international levels. Measures to enhance cyber deterrence will be pursued in an environment of economic scarcity and a political and bureaucratic competition for resources. Stretching the deterrence concept to include non-military aspects of cyber security may also dilute the concept. It should be noted, however, that this kind of critique has been levelled at other broader conceptions of security. The 'human security' approach, for example, which emerged in the mid-1990s and sought to include insecurity caused by economic deprivation and environmental degradation, attracted the same types of criticism. Yet it also made an important policy and theoretical contribution to security in the post-Cold War era. In this sense, a concept of comprehensive cyber deterrence will be part of:

> 'a long line of neologisms [that have sought to] encourage policymakers and scholars to think about international security as something more than the military defense of state interests and territory'.[91]

What is certain is that more research is required. If cyber deterrence is going to be tailored to different threats and involve a broader range of deterring and deterrable actors, then a more nuanced understanding of what types of deterrence might work in different contexts is needed. This indicates a rich and varied future research agenda for the emerging cyber security discipline. Short-term areas of focus could be deterring state-sponsored or affiliated hackers, deterring the manipulation of social media, and enhancing deterrence through resilience in the

[90] Stevens, T. (2015). *Cyber Security and the Politics of Time*, (Cambridge: Cambridge University Press).

[91] Paris, R. (2001). 'Human security: Paradigm Shift or Hot Air?', *International Security*, Vol. 26 No. 2, pp. 87-102.

private sector and in democratic systems and governance. More multidisciplinary research is also needed. Deriving insights from the behavioural sciences, psychology, law, criminology, crime science, computer science, and political science will likely yield more nuanced results and more effective cyber deterrence measures. In this sense, the concept of ‘deterrence’ needs to be reclaimed from the realist-based military-strategic studies sphere. In the final analysis, and to use the terminology of deterrence itself, the costs of not putting in place strategies to deter a broader range of cyber threats may exceed any benefits accrued from limiting the concept to state actors and high-level strategic attacks.