Crossed Wires: International Cooperation on Cyber Security

Madeline Carr

Senior Lecturer in International Politics and the Cyber Dimension

Introduction

Cyber security is a compelling problem for scholars of International Politics. Internet technology is so thoroughly integrated into civil society, commerce, governance, critical infrastructures, intelligence collection and law enforcement that the stakeholders necessary to cyber security practices and policies are diverse and complex. This produces a collision of interests, agendas and expectations – that can often be incompatible or even in direct conflict. And of course, some aspects of the Internet can be quite independent of geographic and political borders. Although cyber security is quite clearly a 'post-state' problem, it has actually proven very difficult to move beyond a Westphalian conception of either the problem or the possible solutions. This leads to a central paradox about cyber security as we currently conceive it: on the one hand, it appears to be a problem that can not be dealt with effectively by state instruments like the military or law enforcement but despite that, there remains a strong expectation that the state retains responsibility for providing security in this realm. This paradox has lead to an emphasis in cyber security policy documents on the imperative for international cooperation. [1]

At first glance, it might appear intuitive that states would seek to cooperate on cyber security. In the context of the globalisation literature of the past two decades, transnational and non-traditional security concerns have frequently been discussed as transcending state capabilities[2] and even as a catalyst for enhanced cooperation.[3] However, despite this clear emphasis on international cooperation on cyber security and the assertions that not only is the threat imminent but a solution is in everyone's best interest, progress on this front has been slow. Analysis of the impediments to greater cooperation has largely been the domain of the technical and legal sectors. However, after 25 years of looking for solutions through these two lenses (often in isolation of one another) it is becoming clear that cyber security is not simply a technical problem. Rather, there are considerable political elements to this that need to be much more closely examined and understood.

In order to highlight some of the political factors that impede greater progress on international cooperation in this context this paper provides a brief overview of two mechanisms for state to state cooperation on cyber security; NATO and the Council of Europe Convention on Cybercrime. These two mechanisms are useful for this analysis for two reasons; first, both have been in existence long

[1] Maude, F. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, (London, Cabinet Office, 2011). Obama, B. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* (Washington DC, The Whitehouse, 2011).

[2] This literature spans a broad range of issues but environmental politics has been particularly active. See Death, C. (ed.), *Critical Environmental Politics,* (London, Routledge, 2014).

[3] de la Chapelle, B. 'Towards Multi-Stakeholder Governance – The Internet Governance Forum as Laboratory', in *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment,* Kleinwachter, W. (ed.), (Marketing for Deutschland GmbH, 2007).

enough to provide a platform for discussion of the range of political factors that might help to explain the reasons why states have not cooperated more comprehensively on this issue. The second reason why they are useful examples if because of their very different origins. NATO is a pre-existing security arrangement that is working to adapt to the Information Age. The 2007 attacks on Estonia made it clear that Article Five of the NATO charter is ill-equipped to address cyber attacks and it prompted a concerted effort to explore the implications of cyber security for future cooperation between member states. Looking at NATO provides some insight into the challenges of incorporating concepts of 'cyberwar' into conventional military based security arrangements. In contrast, the Council of Europe Convention on Cybercrime (also referred to as the Budapest Convention) is an example of a more recently established mechanism for state to state cooperation specifically on cyber security.[4] It is open to ratification by any country – in or outside of Europe. Predominantly a mechanism for aligning legal regimes, its uptake has been slow and limited. While technical capability and legal factors are certainly part of the explanation for this, this paper argues that a lack of political will has also been a significant impediment to greater cooperation.

This is a question that warrants significant research and it cannot be dealt with in a short paper like this one. Instead, this article sets out the problem of international cooperation through both pre-existing and purpose built security arrangements and proposes some of the factors for consideration and further research. Most significant here is the need to consider more carefully the implications of attribution problems for international relations, the utility of conceptualising cyber security as 'war' and the expectations of less powerful states that they have a greater role in the promotion of values through international law.

NATO

In April 2007, a diplomatic stoush between Russia and Estonia resulted in a Distributed Denial of Service (DDoS) attack on Estonian critical infrastructure. Involving over a million computers around the world, primary targets were the websites of the Estonian President and Parliament, three of the country's six news services, two of its largest banks and several communications firms.[5] Estonia's Defence Minister Jaak Aaviksoo declared a national security situation which could "effectively be compared to when your ports are shut to the sea".[6]

Relations between Russia and Estonia deteriorated quickly with Estonia turning to its NATO allies for assistance in what they believed was an act of state-to-state belligerence. NATO responded by acknowledging that the attacks fell within the purview of the alliance relationship and should elicit support.[7] However, Article Five of the NATO treaty – the 'tripwire' for collective response by NATO

[4] The treaty was introduced in 2001 and entered into force in 2004. As of 2015, 47 states have ratified the treaty while an additional seven have signed but not ratified. For a full list of participating states, see the Council of Europe website at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures .

[5] DW Staff Writer, 'NATO Probes Cyber Attacks on Estonia', *Deutsche Welle*, 18 May 2007, http://www.dw-world.de/dw/article/0,,2542756,00.html?maca=en-rss-en-all-1573-rdf and Traynor, I. 'Russia accused of unleashing cyberwar to disable Estonia', *Guardian Unlimited,* 17 May 2007, http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

[6] 'Cyber Warfare – Beyond Estonia-Russia, The Rise of China's 5th Dimension Cyber Army', *Asymmetric Threats Contingency Alliance (ACTA) Briefing,* 30 May 2007, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/300507.php.

[7] Applebaum, A. 'For Estonia and NATO, A New Kind of War', *The Washington Post,* 22 May 2007, p. A15 http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html . Also, 'Estonia urges firm

members to an attack on a member country – was not then understood to define cyber-attacks as military action.[8] After three weeks of sustained attacks, Estonia was forced to isolate itself from Internet traffic beyond its borders in order to restore its systems and the attacks subsequently died off (presumably as rental of the botnet being used to launch the attack expired). [9]

This incident served to highlight two important elements of conceptualising cyber security in a state security context. First, industrialised, developed states are disproportionately vulnerable to cyber threats and this disrupts longstanding beliefs in IR about the relationship between technology and power.[10] Even in 2007, Estonians relied heavily on their critical information infrastructure with many commercial, civilian and governmental functions taking place solely online. The disruption to Internet access impacted Estonia in a way that it would not (even today) impact many of the world's states where penetration rates, and therefore reliance - are too low. Additionally, in a global order with vastly uneven distribution of capabilities, there is a growing expectation that those political actors with access to few conventional military resources may be attracted to the asymmetric potential of cyber weapons. [11]

The second important element that this incident brought to the fore was the challenge for collective security arrangements like NATO of synthesising existing concepts of kinetic war to threats particular to the Information Age. Understanding these fully will be the work of a generation of scholars and practitioners (work begun in this special issue) but beginning to articulate some of the disjuncture between our conceptions of political violence pre and post Internet technology is a starting point. In this case, there are two points worth enunciating; first, the problems surrounding retaliation and second, the uneasy fit of 'war' with 'cyber'.

EU, NATO response to new form of warfare: cyber-attacks', *The Sydney Morning Herald,* 16 May 2007 http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html and 'Estonia hit by 'Moscow cyber war', *BBC News,* 17 May 2007 http://news.bbc.co.uk/2/hi/europe/6665145.stm .

[8] In response to questioning from Russian policy maker Konstantin Kosachev at an alliance planning summit in March 2015, NATO Secretary-General Jens Stoltenberg said that a cyber attack would potentially elicit a military response from NATO. Transcript from 'Zero-Sum? Russia, Power Politics, and the post-Cold War Era: Session at the Brussels Forum with participation of NATO Secretary General Jens Stoltenberg', NATO, 20 March 2015. http://www.nato.int/cps/en/natohq/opinions_118347.htm?selectedLocale=en. For media coverage of the problems with Article Five that immediately followed the Estonian attacks, see Traynor, I. 'Russia accused of unleashing cyberwar to disable Estonia', *Guardian Unlimited,* 17 May 2007 http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

[9] It needs to be acknowledged here that DDoS attacks are now regarded at the very low end of cyber security threats with some even suggesting that they should be regarded as a legitimate form of political protest. (See James, S. 'Hacktivist's Advocate: Meet the lawyer who defends Anonymous', *The Atlantic,* 2012 http://www.theatlantic.com/international/archive/2012/10/hacktivists-advocate-meet-the-lawyer-who-defends-anonymous/263202/ .) DDoS attacks do not cause damage and are not used for theft. They block access to a site by bombarding it with requests – something like a crowd of protesters preventing access to a building. The difference is that in the context of a physical protest, all of those protesters are consciously participating whereas DDoS attacks rely upon large numbers of illegally co-opted computers. However, in 2007 DDoS attacks were still regarded as an important part of the overall cyber threat matrix.

[10] Carr, M. *US Power and the Internet in International Relations: The Irony of the Information Age,* (London, Palgrave Macmillan, 2016).

[11] Wilson, C. 'Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress', (Washington D.C., Congressional Research Service, 17 October 2003), p.1.

Attribution and Retaliation:

Retaliation by use of kinetic or electronic force is deeply problematic as a response to cyber attacks. In large part, this is a consequence of the challenge of attribution – or accurately identifying the source of an attack that comes across the Internet. Although (post Snowden) we should all be familiar with how much data is collected about our online transactions and how sophisticated tracking practices are, for those who are determined and skilled, masking the origin of an attack is still possible. Despite the widespread attention it attracted from security firms, even the Estonian DDoS attack has never been conclusively attributed. It will probably always remain unclear whether that attack was initiated by a determined group of individuals (with or without some degree of support from the Russian state) or if it was a state led attack. [12] This problem of attribution means that *any* response is problematic. If we were to consider responding to states from which an attack *appears* to emerge, we would have to consider the potential for being deliberately misled. In the context of a pre-existing political tension like Estonia (or the Straits of Taiwan, the Middle East etc), those with an interest in conflict escalation could conceivably use a cyber attack to prompt a kinetic response. This creates a kind of 'digital fog of war' which has implications for trust in international relations.

The role of trust in international cooperation has attracted significant scholarly attention – often in the context of adherence to arms treaties.[13] Although much of the literature around cyber security falls back on concepts and frameworks developed in the context of kinetic weapons, the problem of attribution on the Internet seriously undermines the potential for trusting relationships because it renders transparency and accountability so difficult. Computer forensics focuses on Internet Protocol (IP) addresses. This can, if an investigation is successful, lead to the identification of a computer involved in an attack. However that does not in itself identify the person behind the attack. This means that state actors could continue to break the terms of an agreement with some hope of avoiding detection but it also means that there is potential to design attacks so that they *appear* to come from a particular state. This ambiguity of the origins of cyber attacks leads to a condition of 'plausible deniability' – states may use the difficulties of attribution to their advantage, but this makes it difficult to establish trust.

Is Cyber War 'War'?

The second important disjuncture that emerged through this challenge for NATO as a collective security instrument was how (or whether) the concept of war could be applied to cyber attacks. The literature on cyber war is polarised. Some people like Richard Clarke (former US 'cyber czar') argue that it is a matter of 'when' rather than 'if' we will experience a significant incident that can be understood as cyber war.[14] At the other end of the spectrum, Thomas Rid suggests that when we look closely at cyber attacks in the context of the state, rather than anything resembling war, we see

[12] Greenemeier, L. 'Estonian "Cyber-Riot" Was Planned, But MasterMind Still a Mystery', *Information Week,* 3 August 2007. http://www.informationweek.com/news/showArticle.jhtml?articleID=201202784

[13] Keating, V. & Ruzicka, J. 'No Need to Hedge: Identifying trusting relationships in international politics', *Review of International Studies,* 40:4 (2014), pp.753-770. Also Kydd, H. *Trust and Mistrust in International Relations*, (Princeton, Princeton University Press, 2005); Booth, K. & Wheeler, N.J. *The Security Dilemma: Fear, Cooperation, and Trust in World Politics,* (New York, Palgrave Macmillan, 2008); Ruzicka, J. & Wheeler, N.J. 'The Puzzle of Trusting Relationships in the Nuclear Non-Proliferation Treaty', *International Affairs,* 86:1 (2010), pp. 69-85.

[14] Clarke, R.A. & Knake, R.K. *Cyber War: The next threat to national security and what to do about it,* (New York, HarperCollins, 2010).

‘three activities that are as old as human conflict itself: sabotage, espionage and subversion’.[15] He argues that emphasis on these practices is reducing the reliance on physical violence. There is plenty of value in the terminological clarity that Rid insists upon but the insistence of strategic studies scholars on overlaying a Clausewitzian understanding of war on contemporary political violence suggests that there is no need – or no space – to reconceptualise war in the context of the massive technological changes of the past quarter century. In a practical sense, even if Clausewitz would not recognise cyber war, that can be of little comfort to those charged with protecting the state from attack in a globally accessible networked environment.

Essentially, both ends of this polarised literature tend to be quite conventional and rely heavily on concepts, practices and ideas developed in the context of kinetic war to try to understand cyber war. Early thinking on this was focused on coordinated DDoS attacks or attacks on critical infrastructure that would generate a level of public chaos often articulated as a ‘Cyber Pearl Harbour’.[16] More recently, the economic cost of cyber insecurity has been framed as a state of ‘war’. In this view, damage to the economy is not a *by-product* of cyber attacks but rather the economy is the *target* of attacks. Industry estimates vary wildly but some have put the global theft of public and private intellectual property and data at as high as US $445 billion per year.[17] At a Senate hearing into US cyber security vulnerabilities, one witness testified that “the Nation is under attack, and it is a hostile attack, it is a continuing attack. It has been going on for years, and we have largely been ignoring it”.[18]

These two factors; first, the challenges of attribution and their implications for retaliation and second, the conceptual ambiguity about what cyber war *is,* are two of the political impediments to greater international cooperation on cybersecurity in the context of a collective security arrangement like NATO. Both of these impediments require extensive research if we are to move beyond existing debates that are tethered to ideas about the state, about political conflict and about global security that may no longer have the same explanatory power that they did in the age of purely kinetic war.

Budapest Convention

The Council of Europe Convention on Cybercrime (The Budapest Convention) is the first international treaty on crimes committed via the Internet. The treaty came into force in November 2001 and was developed in consultation with the US, Canada, Japan and South Africa. It is open to signature by any state and at the time of writing had been ratified by 47 states (signed but not

[15] Rid, T. *Cyber War Will Not Take Place*, (London, Hurst and Company, 2013), p. xiv.

[16] Technology journalist Scott Berinator traces the use of this term back to 1991 when it was used by D. James Bidzos, the president of a computer security firm. However, the term had become common amongst many policy makers by the late 1990s and continues to resonate with experienced cyber security commentators like Richard Clarke and Robert Knake. See Berinato, S. ‘The Future of Security’, *Computerworld*, 30 December 2003 http://www.computerworld.com/s/article/print/88646/The_future_of_security .

[17] *Net Losses: Estimating the Global Cost of Cybercrime*, (Center for Strategic and International Studies, June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. Note: these estimations are acknowledged to be very difficult for a range of reasons, not the least of which is the reluctance of many in the private sector to publically discuss such losses. For an explanation of how the authors arrive at this figure, see p. 6 of the report.

[18] Spafford, E.H. testimony at *Cybersecurity: Assessing our Vulnerabilities and Developing an Effective Response*, hearing before the Committee on Commerce, Science, and Transportation, United States Senate, 19 March 2009, p. 28.

ratified by a further seven).[19] Only eight of these states are outside of the Council of Europe membership and neither Israel nor South Africa have ratified the treaty.

The Budapest Convention initially dealt with infringements of copyright, computer-related fraud, child pornography and violations of network security. The treaty calls on states to align their criminal codes in order to facilitate faster and more effective cooperation between law enforcement bodies. States that ratify the treaty have to make the following five actions illegal and authorise their domestic law enforcement agencies to investigate them: unauthorised access, unauthorised interception, data interference, system interference and misuse of devices.[20] Although states are expected to authorise their domestic law enforcement agencies to investigate these crimes, they can exempt certain cases if they regard them as inconsistent with their public policies or security.

Several problems have arisen since that have impeded ratification of the treaty. In 2006, an additional protocol was added that addressed the publication of racist and xenophobic propaganda making it a criminal offence. This interpretation of what constitutes a crime online is complex and raises a number of interesting political impediments to further cooperation on this issue. By folding in content conventions like hate speech and copyright, the treaty arguably introduces an area of broad disagreement that states are unlikely to align upon. In 2011, attempts in Brazil to pass a bill for the purpose of acceding to the Budapest Convention resulted in a backlash against what was seen as potential human rights abuses.[21] Under the proposed law, Brazilian courts could criminalise file-sharing and peer-to-peer activity. This prompted a harsh response from two quarters; intermediaries like Internet service providers and platforms like YouTube which would have become liable for the illegal content they carried objected to the proposed law. It also prompted objections from human rights activists concerned about the implications for free speech.

In discussing the challenges of global cybercrime law, Murdoch Watney raises the issue of 'paper laws' – that is laws that are in existence but that are not enforced.[22] There are several reasons why this is sometimes the case but amongst them in this context is a lack of technical or financial capability and also differing perceptions of the risk these crimes pose. Indeed, one of the primary reasons why the political will to address cyber security vulnerabilities varies from state to state is the degree to which that state is reliant on a secure, reliable network. States with low Internet penetration rates, without the comprehensive integration of critical infrastructure to network platforms that we have witnessed in many developed states, and which do not produce and market intellectual property, are much less vulnerable to attacks either on the Internet or over the Internet. Persistent security problems that are reported to be increasingly expensive are predominantly a cost to those states that have been best able to integrate Internet technology and infrastructure into

[19] Convention on Cybercrime, *Council of Europe,* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[20] Convention on Cybercrime, *Council of Europe,* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[21] Biddle, E.R. 'Brazil: Cybercrime Law Could Restrict Fundamental Rights, Internet Openness', *Global Voices Advocacy Blog,* 8 November 2011 http://advocacy.globalvoicesonline.org/2011/11/08/brazil-cybercrime-law-could-restrict-fundamental-rights-internet-openness/ . Harley, B. 'A Global Convention on Cybercrime?', *The Columbia Science and Technology Law Review* blog, 23 March 2010, http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.

[22] Watney, M. 'Cybercrime regulation at a cross-road: State and transnational laws versus global laws', *International Conference on Information Society,* 2012, p. 72.

their civil, military, commercial and government systems.[23] This asymmetry in states' vulnerability to cyber security has clear implications for the extent to which states will value international cooperation on the issue.

Finally, there have been objections to the process by which the treaty was drawn up. It has been criticised by the UN's International Telecommunications Union (ITU) chief Hamadoun Touré for being outdated.[24] Even allowing for institutional competition and jealousies, Touré makes a point that resonates with many political leaders, especially many newly independent states that see sovereignty as linked to national identity. In contrast, the Shanghai Cooperation Organization's set of principles or 'action plan' adopted in 2007 by China, Russia Kazakhstan, the Kyrgyz Republic, Tajikistan and Uzbekistan is also a law enforcement approach but it stressing the member states' intent to exercise sovereign control over content and systems. It too is open to accession by other states but the take up there has also been limited.

Conclusion

While cooperation on other transnational issues is often based around mutual interest and/or around relationships of trust, cyber security is problematic in both respects. Perhaps in part because of the broad implications of Internet technology, state interests in this context align at some times and they collide quite significantly at others. Furthermore, the attribution problem and its implications for transparency mean that trust is difficult.

In the case of a pre-existing security arrangement like NATO, the challenges of interpreting cyber security within a set of practices and policies conceived of to address kinetic conflict continue to play out and to limit clarity about possible retaliation. The ongoing problems of attribution and the interconnected nature of military and civilian systems make options for response complex and (at this stage) quite limited. In addition, there is much more work to be done on understanding the extent to which cyber security and war can be dealt with in the same conceptual, legal and practical frameworks. It is likely that extending war-related practices and policies to cyberspace will have limited utility in the long term.

For a 'purpose built' mechanism for international cooperation on cyber security like the Budapest convention, aligning laws in cyberspace equates to aligning values on issues with diverse interpretations and approaches. Values and interests have always played a role in international cooperation of any kind but in the case of cyber security, the implications are so broad that an unusually wide range of factors must be taken into account and coordinated and this has proven challenging. Perhaps as significant as this has been the expectation by states of a more equitable and inclusive process – one that is not led by powerful states but one that takes into account more fully the views of those expected to participate.

[23] This could apply to any number of developing states but it was highlighted with some force through speculation over recent attacks on South Korea – allegedly by North Korea. Hern, A. 'North Korean 'cyberwarfare' said to have cost South Korea £500m', *The Guardian,* 16 October 2013 http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea.

[24] Vatis, M. 'The Council of Europe Convention on Cybercrime', *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC, The National Academies Press, 2010), p. 218. http://www.nap.edu/catalog/12997.html.

This brief account of some of the political impediments to greater international cooperation on cyber security points to a broad range of issues that demand much more in depth and sustained attention from International Relations as a discipline. It is both surprising and puzzling that a discipline so well equipped to address issues of global security, cooperation, war, peace, power and competition has yet to contribute more significantly to understanding the implications of the information age. This special issue reflects the willingness, curiousity and capability of the next generation of IR scholars to address these questions and I am proud to be published in their company.

Bibliography

Applebaum, A. 'For Estonia and NATO, A New Kind of War', *The Washington Post*, 22 May 2007, p. A15 http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html.

Berinato, S. 'The Future of Security', *Computerworld*, 30 December 2003 http://www.computerworld.com/s/article/print/88646/The_future_of_security .

Biddle, E.R. 'Brazil: Cybercrime Law Could Restrict Fundamental Rights, Internet Openness', *Global Voices Advocacy Blog,* 8 November 2011 http://advocacy.globalvoicesonline.org/2011/11/08/brazil-cybercrime-law-could-restrict-fundamental-rights-internet-openness/ .

Booth, K. & Wheeler, N.J. *The Security Dilemma: Fear, Cooperation, and Trust in World Politics*, New York, Palgrave Macmillan, 2008.

Carr, M. *US Power and the Internet in International Relations: The Irony of the Information Age,* London, Palgrave Macmillan, 2016.

Clarke, R.A. & Knake, R.K. *Cyber War: The next threat to national security and what to do about it*, New York, HarperCollins, 2010.

de la Chapelle, B. 'Towards Multi-Stakeholder Governance – The Internet Governance Forum as Laboratory', in *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment,* Kleinwachter, W. (ed.), Marketing for Deutschland GmbH, 2007.

Convention on Cybercrime, Council of Europe, *http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.*

'Cyber Warfare – Beyond Estonia-Russia, The Rise of China's 5th Dimension Cyber Army', *Asymmetric Threats Contingency Alliance (ACTA) Briefing,* 30 May 2007, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/300507.php.

Death, C. (ed.), *Critical Environmental Politics,* London, Routledge, 2014.

'Estonia hit by "Moscow cyber war"', *BBC News*, 17 May 2007 http://news.bbc.co.uk/2/hi/europe/6665145.stm .

'Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks', *The Sydney Morning Herald*, 16 May 2007 http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html

Greenemeier, L. 'Estonian 'Cyber-Riot' Was Planned, But MasterMind Still a Mystery', *Information Week*, 3 August 2007 http://www.informationweek.com/news/showArticle.jhtml?articleID=201202784

Harley, B. 'A Global Convention on Cybercrime?', *The Columbia Science and Technology Law Review* blog, 23 March 2010 http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.

Hern, A. ‘North Korean ‘cyberwarfare’ said to have cost South Korea £500m’, *The Guardian,* 16 October 2013 http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea.

James, S. ‘Hacktivist’s Advocate: Meet the lawyer who defends Anonymous’, *The Atlantic,* 2012 http://www.theatlantic.com/international/archive/2012/10/hacktivists-advocate-meet-the-lawyer-who-defends-anonymous/263202/ .

Keating, V. & Ruzicka, J. ‘No Need to Hedge: Identifying trusting relationships in international politics’, *Review of International Studies*, 40:4 (2014), pp. 753-770.

Kydd, H., *Trust and Mistrust in International Relations*, Princeton, Princeton University Press, 2005.

Maude, F. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, London, Cabinet Office, 2011.

‘NATO Probes Cyber Attacks on Estonia’, *Deutsche Welle*, 18 May 2007, http://www.dw-world.de/dw/article/0,,2542756,00.html?maca=en-rss-en-all-1573-rdf .

Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Obama, President Barack, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* Washington DC, The Whitehouse, 2011.

Rid, T. *Cyber War Will Not Take Place*, London, Hurst and Company, 2013.

Ruzicka, J. & Wheeler, N.J. ‘The Puzzle of Trusting Relationships in the Nuclear Non-Proliferation Treaty’, *International Affairs*, 86:1 (2010), pp. 69-85.

Spafford, E.H. Testimony at *Cybersecurity: Assessing our Vulnerabilities and Developing an Effective Response*, hearing before the Committee on Commerce, Science, and Transportation, United States Senate, 19 March 2009.

Stoltenberg, J. ‘Zero-Sum? Russia, Power Politics, and the post-Cold War Era: Session at the Brussels Forum with participation of NATO Secretary General Jens Stoltenberg’, NATO, 20 March 2015 http://www.nato.int/cps/en/natohq/opinions_118347.htm?selectedLocale=en.

Traynor, I. ‘Russia accused of unleashing cyberwar to disable Estonia’, *Guardian Unlimited*, 17 May 2007 http://www.guardian.co.uk/russia/article/0,,2081438,00.html

Vatis, M. ‘The Council of Europe Convention on Cybercrime’, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC, The National Academies Press, 2010 http://www.nap.edu/catalog/12997.html.

Watney, M. ‘Cybercrime regulation at a cross-road: State and transnational laws versus global laws’, *International Conference on Information Society,* 2012.

Wilson, C. ‘Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress’, Washington DC, Congressional Research Service, 17 October 2003.