2015/2016 – Issue II
ISSN 2051-6932 (Online)

Interstate

Journal of International Affairs

01010101000000001010101010101010101
01010101010101010101111110001010101
01010101010101010101010101010101010
10101010101010101010101010101010101
01010101011111111111100000010001001
0010101000001111**THE**00**CYBER**00**ISSUE**
01011010101001010010100011111111010
1001000110101010101010101010010101
01010101101010100010110101010000101
10101010010101010101110010101010101
01010010101010110010111100000000000
10101011101010101001111101010100100
10101010100000101010101010100101010
00110101101010101100101001010100101
0000000000111111000**SPECIAL**01**EDITION**

ALEX MIDDLETON
Stuxnet: The World's First Cyber… Boomerang?

JUSTINE CHAUVIN
Book Review: Cyber War Will Not Take Place

DR MADELINE CARR
Crossed Wires: International Cooperation on Cyber Security

MEMPHIS KRICKEBERG
The Internet as a Slippery Object of State Security

VAUGHAN AUSTIN HOLDING
Internet Freedom: Rhetoric VS Reality

Interstate Journal of International Affairs is hosted by the Department of International Politics, Aberystwyth University.

Interstate
Department of International Politics
Aberystwyth University
Penglais
Aberystwyth
Ceredigion
SY23 3FE
United Kingdom

Any opinions expressed in this issue are those of the individual contributors and do not necessarily represent those of the journal, the Department or the University.

INTERSTATE

2015/2016 – Issue II

Introduction **1**

Dr. Madeline Carr
Crossed Wires: International Cooperation on Cyber Security **2**

Justine Chauvin
Book Review: Cyber War Will Not Take Place **14**

Alex Middleton
Stuxnet: The World's First Cyber… Boomerang? **26**

Memphis Krickeberg
The Internet as a Slippery Object of State Security: The Problem of Physical Border Insensitiveness, Anonymity and Global Interconnectedness **33**

Vaughan Austin Holding
Internet Freedom: Rhetoric Versus Reality **43**

Managing Editor: Alex Middleton

Editors: Akos Erzse, Vaughan Austin Holding, Alex Hird.

Departmental Advisors: Dr. Madeline Carr, Elaine Lowe

Introduction

Cyber and Internet related discourses are typically lodged within technical disciplines such as Computer Science and Information Studies. Though Law and social scientists are increasingly contributing to this area, until recently, analyses of these issues applied through an International Political lens have been rare. Fortunately, the Department of International Politics at Aberystwyth University was among the early academic institutions to recognise that our discipline can offer tremendous input to the existing literature and debates. Over the past several years this has been achieved through the production of new research as well as offering supervision and teaching at all degree levels for students devoted to exploring International Politics in the cyber dimension.

Putting this special edition issue together has been a rich and rewarding experience for all involved. The articles contained within it are paying tribute to, and reflective of, the innovative nature of the work that has been carried out at the Cyber Connectivity Research Centre and at the Department more broadly. From all on the *Interstate* team, we hope you enjoy reading this special edition issue.

Alex Middleton
Managing Editor

Crossed Wires:
International Cooperation on Cyber Security

Dr. 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 cannot 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 led 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

[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).

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 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 is 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

[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 .

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 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. [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

[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 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 often 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.

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 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'.

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.

[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.

[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

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 '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.

[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).

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

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 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.

[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.

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

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

[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.

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 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

[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.

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.

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, curiosity 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.

Book Review: Cyber War Will Not Take Place

Justine Chauvin

Introduction

In *Cyber War Will Not Take Place*[1], Thomas Rid develops his argument on the concept of "cyberwar", previously formulated in an article of the same name[2] published in January 2012. His chief point is that "cyber war has never happened in the past, it does not occur in the present, and it is unlikely that it will disturb our future";[3] *ergo* the use of this concept to describe cyber-offenses is misleading.[4] He has also written several articles related to cyberwar[5], cyberweapons[6] and cyberpeace,[7] in which he argues against the militarization of the debate about cyberattacks,[8] and in particular the confusing use of analogies referring to the Cold War and nuclear deterrence.[9] In this piece, I will review the literature related to cyberwar and more specifically three widely disputed questions covered by Rid's book, namely the potential violence inflicted by cyberattacks, the definition of what is a cyberweapon, and – in relation to the attribution problem – the possibility of a cyberdeterrence strategy. As a conclusion, I will broaden the perspective by briefly highlighting other issues related to the current conceptualisation of cyberspace.

Will Cyberwar Take Place, Or Not?

John Arquilla and David Ronfeldt introduced the concept of cyberwar in 1993, [10] declaring that the information age will transform "the nature of war,"[11] and that the "military organization and doctrine, as well as strategy, tactics, and weapons design"[12] must necessarily be redefined. In the same line, James Adams stated in 2001 that "the information age is now revolutionizing warfare for the twenty-first [century]",[13] and that "Washington urgently needs to modernize its thinking and transcend its

[1] Rid, T. *Cyber War Will Not Take Place* (London: Hurst & Company, 2013).

[2] Rid, T. "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 35:1 (2012).

[3] Rid, *Cyber War*, p. xiv.

[4] Rid, *Cyber War*, p. xvi.

[5] Rid, T. "End this phony cyberwar", New Scientist, 219: 2933 (2013); Rid, T. "Think Again: Cyberwar", *Foreign Policy* (published 27 February 2012).

[6] Rid, T and McBurney, P. "Cyber-Weapons", *The RUSI Journal*, 157:1 (2012).

[7] Rid, T. "Cyberwar and Peace", *Foreign Affairs*, 91:6 (2012).

[8] Rid, "Cyberwar and Peace", p. 87.

[9] Rid, "Cyber War", p. 29.

[10] Arquilla, J & Ronfeldt, D. "Cyberwar Is Coming!", *Comparative Strategy*, 12:2 (1993).

[11] Arquilla, J & Ronfeldt, D. "Cyberwar Is Coming!", in *Athena's camp: Preparing for conflict in the information age*, (eds.) John Arquilla and David Ronfeldt (Santa Monica: RAND, 1997), p. 31.

[12] Arquilla, J & Ronfeldt, D. "Cyberwar Is Coming!".

[13] Adams, J. "Virtual Defense", *Foreign Affairs*, 80:3 (2001), p. 98.

strategies of deterrence and national security"[14] to be able to fight in the cyberspace which is the "new international battlefield."[15] Noticeably, Adams articulated all key elements which remain the dominant perception of cyber-conflicts amongst U.S. officials,[16] cybersecurity experts,[17] and a substantial number of scholars.[18] According to him, cyberwar is asymmetric and favours nations (above all, China[19] and Russia[20]) and non-state actors, less powerful from a conventional perspective but supposedly actively "exploring the possibilities raised by this new American vulnerability."[21]

Indeed, the U.S. is seen as especially vulnerable, because of its superiority in information technology, which in turn, increases its dependence on cyberspace, and the attractiveness of its national targets.[22] For instance, the former US Director of National Intelligence, Mike McConnell, declared that "as the most wired nation on Earth, [the U.S.] offer[s] the most targets of significance, yet our cyber-defenses are woefully lacking."[23]This idea is reinforced by the perception of cyberweapons as cheap and relatively easy to obtain,[24] but capable to engender "potential nightmares"[25]. Indeed, the idea that an "electronic Pearl Harbor"[26] will occur is widespread (Adams claimed that even if cyberattacks have not inflicted critical damage so far, they are nevertheless "just a taste of dangers to come"[27], while Clarke and Knake declared that "cyber war could devastate a modern nation"[28]). Accordingly, discourses about cybersecurity are abound of very evocative metaphors. Panetta declared notably that cyberattacks can "cause physical destruction and loss of life"[29] and "be as destructive as the terrorist attack 9/11."[30]

[14] Adams, "Virtual Defense", p. 99.
[15] Adams, "Virtual Defense", p. 98.
[16] Lynn, W. "Defending a New Domain", *Foreign Affairs*, 89:5 (2010).
[17] Clarke, R & Knake R. *Cyber War* (New York: Ecco 2010).
[18] See, e.g., Clark, W and Levin, P. "Securing the Information Highway", *Foreign Affairs*, 88:6 (2009); Knapp, K & Boulton, W. "Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments", *Information Systems Management*, 23:2 (2006); Valeri, L & Knights, M. "Affecting Trust: Terrorism, Internet and Offensive Information Warfare", *Terrorism and Political Science*, 12:1(2000).
[19] Adams, "Virtual Defense", p. 102.
[20] Adams, "Virtual Defense", p. 104.
[21] Adams, "Virtual Defense", p. 102.
[22] Adams, "Virtual Defense", pp. 98-99.
[23] McConnell, M. "How to win the cyber-war we're losing", *The Washington Post* [website] (28 February 2010). http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html
[24] Adams, "Virtual Defense", p. 104.
[25] Adams, "Virtual Defense", p. 102.
[26] *See, e.g.*, Bendrath, R. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection", *Information & Security: An International Journal* (2001)
[27] Adams, "Virtual Defense", p. 100.
[28] Clarke & Knake, *Cyber War*, pp. 30-31.
[29] Panetta, L. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security", *U.S. Department of Defense* [website] (New York City, 11 October 2012). http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[30] Panetta, ."Remarks".

Adams also develops the idea that in cyberspace, offense dominates defence (similarly, Arquilla and Ronfeldt stated that the information age has "offense-dominant attributes"[31]), and consequentially that the best defence is offensive, which means "deterring the attacks before they occur."[32] Therefore, the major problem in cyberspace is the attribution problem because it determines the possibility of retaliation, and deterrence.[33] Panetta stated that cyber attackers "will be far less likely to hit [the U.S] if we will be able to link the attack"[34] and that his department "has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of those attacks."[35] Moreover, McConnell also declared that to be able to deter cyberattacks, the U.S. must "reengineer the Internet to make attribution [...] more manageable."[36]

In this context, Rid was in total opposition with what seemed to be the mainstream assumptions about cyberwar, when he wrote in 2012:

"cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead."[37]

Drawing on Clausewitz's conception of war as an instrumental, political and potentially lethal "act of force to compel the enemy to do our will,"[38] Rid argued that cyberwar does not exist because "if the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria."[39] He concluded in highlighting that an act of "stand-alone cyber war, with code as the main weapon"[40] has never occurred yet, and that alarmist predictions as well as analogies between nuclear and cyber war are "misplaced and problematic."[41]

Reiterating his original statement in his book released in 2013, Rid's argument is significant and quite provocative, in the sense that it calls into question the very basis of the U.S. cyber security policy, which has named

[31] Arquilla J & Ronfeldt, D. *The Advent of Netwar* (Santa Monica: RAND, 1996), p. 94.
[32] Adams, "Virtual Defense", p. 108.
[33] Adams, "Virtual Defense", p. 109.
[34] Panetta, "Remarks".
[35] Panetta, "Remarks".
[36] McConnell, "How to win".
[37] Rid, "Cyber War", p. 6. [emphasis added]
[38] Clausewitz, C. *Vom Krieg* (Berlin: Ullstein 1832, 1980), 27, *cited in* Rid, "Cyber War", p. 7.
[39] Rid, "Cyber War", p. 10.
[40] Rid, "Cyber War", p. 29.
[41] Rid, "Cyber War", p. 29.

cyberspace the fifth domain of military intervention[42] (and defined it "as critical [...] as land, sea, air and space"[43]), as well as the relatively shared perception amongst scholars that "cyber war is real"[44] and even "already upon us."[45] In the next sections we will see how he challenges their visions and what the repercussions of these different conceptualisations are.

Cyberattacks & Political Violence

In his book, Rid resumes his initial findings and adds that "cyber attacks help to diminish rather than accentuate political violence."[46] Instead of a cyberwar, "the opposite is taking place: a computer-enabled assault on violence itself."[47] Indeed, he demonstrates how sabotage, espionage and subversion mediated though cyberspace are so far mostly non-violent and only indirect (in the sense that "computer code can only directly affect computer-controlled machines, not humans"[48]); something which makes them "less physical, less emotional, less symbolic, and less instrumental than more conventional uses of political violence."[49] Consequently, according to Rid, a cyberattack – in comparison with its kinetic alternatives – is often ethically preferable in the sense that it "may be less violent, less traumatizing and more limited."[50] In the same line, Tim Mauer argues that it might be a good thing if such a thing as cyberwar does exist, because cyberattacks cause limited damages and can save lives compared to other forms of attacks.[51]

However, this ethical superiority is contingent to the idea that the main goal of any form of political violence is to undermine social trust[52] and that cyber-offenders would logically use cyberattacks as a "non-violent shortcut",[53] as they have the capacity to achieve this goal in non-violent ways and, importantly, at lower costs. As Mauer rightly pointed out, this argument does not concern terrorist groups,[54] which could aim at making as much damage as they can to increase the traumatic effect of the attack. Nevertheless, Rid argues that "the use of cyber weapons that could inflict damage and pain comparable to pummelling of Dresden, London, Belgrade, or Beirut at the receiving end of devastating airpower is at present, too unrealistic even for

[42] In the U.S., the cyberspace is officially a new domain of warfare since 2011. U.S. Department of Defense, "The Cyber Domain : Security and Operations," *U.S. Department of Defense* [website]. http://www.defense.gov/home/features/2013/0713_cyberdomain/

[43] Lynn, "Defending", 101.

[44] Clarke & Knake, *Cyber War*, p. 30.

[45] John Arquilla, "Cyberwar Is Already Upon Us", *Foreign Policy* (published 27 February 2012). http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

[46] Rid, *Cyber War*, p. xiv.

[47] Rid, *Cyber War*, p. xiv.

[48] Rid, *Cyber War*, p. 13.

[49] Rid, *Cyber War*, p. 167.

[50] Rid, *Cyber War*, p. 171.

[51] Maurer, T. "The Case of Cyberwarfare", *Foreign Policy* (published 19 October 2011). http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar

[52] Maurer "The Case".

[53] Rid, *Cyber War*, p. 167.

[54] Maurer, "The Case".

bad science fiction plot."[55] Consequently, he dismisses the idea that cyberattacks can have similar effects as the kinetic ones in view of the cyberattacks on record. However, he cannot eliminate on this basis the idea that in the future cyberattacks may have comparable effects.

Furthermore, an interesting critique of Rid's vision of violence as intrinsically related to the human body (leading to his conclusion that cyberwar does not exist, because it cannot be violent enough to be defined as such[56]) has been formulated by John Stone[57]. He underlines notably that the link between violence and lethality (stipulated by Rid in accordance with his interpretation of Clausewitz's work[58]) is not inexorable: a military intervention, even in "minimizing loss of human life by employing advanced military technique"[59] is still an act of war (Stone uses the example of US raids on Schweinfurt in 1943, aiming not at killing civilians but at destroying the ball-bearing factories and thus undermining the German war capacities). Accordingly, Stone declares that acts of war "need not to be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war,"[60] and that consequently, "cyber war is possible [because] cyber attacks *could* constitute acts of war."[61] Erik Gartzke also criticises Rid, in saying that his argument stipulating that cyberwar does not exist "because it fails to conform to conventional definitions of conflict[62] is a perspective that risks becoming "a purely academic exercise",[63] neglecting the probable role of cyberattacks combined with actions "on the ground." He states that cyberwar is indeed not a distinct form of conflict; but is "basically tied to conventional forms of warfare."[64]

What is a Cyberweapon?

In his book, Rid underscores the need to define what a cyberweapon is.[65] His chief point is that if cyberwar has only remained a metaphor, cyberweapons do exist, in the sense that arms are not only used in war but for a wide range of purposes.[66] Therefore, it allows us to use the term cyberweapon (that is, "*computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, system, or living beings*"[67]) in a broader sense than cyberwar.[68] Moreover,

[55] Rid, *Cyber War,* p. 18.
[56] Rid, *Cyber War,* pp. 15-16.
[57] Stone, J. "Cyber War Will Take Place!", *Journal of Strategic Studies,* 36:1 (2013).
[58] Rid, *Cyber War,* p. 1-3.
[59] Stone, "Cyber War", p. 105.
[60] Stone, "Cyber War", p. 105.
[61] Stone, "Cyber War", p. 107.
[62] Gartzke, E. "The Myth of Cyberwar", *International Security,* 38:2 (2013), p. 49.
[63] Gartzke, E. "The Myth", p. 49.
[64] Gartzke, "The Myth", p. 59.
[65] *See also* Rid & McBurney, "Cyber-Weapons".
[66] Rid, *Cyber War,* p. 37.
[67] Rid, *Cyber War,* p. 37.
[68] Rid and McBurney, "Cyber-Weapons", p. *7.*

he draws a distinction between "*generic but low-potential tools*"[69] and "*specific but high-potential weaponry*"[70], and demonstrates than even an extremely sophisticated cyberweapon is not going to lead necessarily to a "cyber-catastrophe", precisely because of its degree of sophistication which allows to minimize or even remove the risk of collateral damage.[71] However, his argument is contingent to the idea that a cyber-attacker's goal is not to inflict as much collateral damage as they can, or alternatively that these attackers do not have yet the capacity to do so. Yet, Rid demonstrates quite persuasively that cyberattacks are not all the same and that making the distinction is fundamental in order to provide relevant solutions to cybersecurity issues. Moreover, he points out that exceptional cyber weapons require a large amount of human, technical and financial resources,[72] which undermines the common idea that cyberwar is asymmetric and, therefore, in favour of conventionally weak states and non-states actors.

Furthermore, he states that this distinction between weapons and non-weapons is fundamental because it has security (a tool with the potential to be used as a weapon is more dangerous), political ("an unarmed intrusion is politically less explosive than an armed one"[73]), and legal consequences[74]. Concerning the latter, Rid argues that this distinction is crucial because it is the first step to develop appropriate responses. If a very sophisticated piece of malware can gather a large amount of information and have noticeable consequences, but cannot be used for other purposes than spying, it should not be considered a weapon because "the law of conflict does not deem espionage an armed attack."[75] This example shows the pragmatic significance of Rid's argument: indeed, if cyberwar does not exist and only a few cyber instruments can indeed be rightly called "weapons", cyberattacks should not be examined from a "law of armed conflict" perspective. Yet, it has been done by scholars, such as Russell Buchan or Charles Dunlap[76] (even if the latter warns against the unproductive effects of applying a "martial rhetoric" to the cyberspace[77]), and nowadays, "few if any scholars publishing on international law and cyber security do so from a non-military perspective."[78]

[69] Rid, *Cyber War*, p. 36.
[70] Rid, *Cyber War*, p. 36.
[71] Rid, *Cyber War*, pp. 45-46.
[72] Rid, *Cyber War*, p. 45.
[73] Rid, *Cyber War*, p. 46.
[74] Rid, *Cyber War*, p. 46.
[75] Rid, *Cyber War*, pp. 46-47.
[76] *See, e.g.,* Buchan, R. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict & Security Law*, 17: 2 (2012); Dunlap Jr, C. "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly* (Spring 2011)
[77] Dunlap, "Perspectives", p. 83.
[78] O'Connell, M. "Cyber Security without Cyber War", *Journal of Conflict & Security Law*, 17:2 (2012), p. 199.

Cyberdeterrence & The Attribution Problem

In his book, Rid progresses beyond his initial triptych (online sabotage, espionage and subversion) to address for the first time one of the most prominent concerns about cyberattacks: the attribution problem. Leon Panetta declared – as has already been mentioned above – that the U.S. Defense Department, after "significant investments",[79] "has [now] the capacity to locate [potential aggressors] and hold them accountable for actions that harm America or its interests."[80] According to Rid, who assesses Panetta's rhetoric as including at least partly "a measure of bluff and bluster,"[81] the possibility of solving the attribution problem by improving only technological tools is misleading. In essence, he argues that far from being an inherent problem with cyberattacks (induced by their technical specificities), the attribution problem is more significantly a political one; consequently, no purely technical solution is likely to resolve it.[82] According to him, attribution is always a call of judgement (even if this point has been underexplored in IR – as opposed to Criminal law – where the "state-against-state" conventional conflicts "mostly left little doubt about the attacker's identity"[83]), and that achieving even an incomplete attribution cannot be done without non-technical insights.[84] He also stresses that the standards of proof depends on what is considered subjectively by governments as "sufficient basis for political action".[85] In doing so, Rid provides thought-provoking insight about the inherent part of subjectivity in the attribution problem, questioning the appropriateness of focusing only on technical capacities to resolve it.

This argument is of particular importance in view of the fact that some people impute the attribution problem and the difficulty of deterrence to the structure of the Internet itself, and therefore, propose to modify its design in order to solve this problem. This is noticeably the case in McConnell's analysis. He argues: "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment [...] more manageable."[86] This view and sentiment is also echoed in the work of David Clark and Susan Landau.[87] Their vision is embedded in the idea that a cyberdeterrence policy must be established in order to prevent cyberattacks, in the same way that deterrence has been used during the Cold War to protect the U.S. from nuclear attacks.[88] This use of analogies is widely criticised by

[79] Panetta, "Remarks."

[80] Panetta, "Remarks."

[81] Rid, *Cyber War*, p. 140.

[82] Rid, *Cyber War*, pp. 140-141.

[83] Rid, *Cyber War*, p. 141.

[84] Rid, *Cyber War*, p. 156.

[85] Rid, *Cyber War*, p. 162.

[86] McConnell, "How to Win".

[87] Clark, D & Landau, S. "Untangling Attribution", *Harvard National Security Journal*, Vol. 2, No. 2 (2011), p. 25.

[88] McConnell, "How to Win".

Rid, arguing that they fail to highlight the real cybersecurity issues.[89] Sean Lawson also has pointed out that it is the comparison between the effects of nuclear and cyberweapons that leads to the application of deterrence in the context of cybersecurity[90] . He states that "it is neither natural nor inevitable"[91] nor even desirable. Similarly, to Rid and James Lewis,[92] he considers that it results "in a tendency to focus on hypothetical worst cases while ignoring actual threats."[93] Howard Schmidt, former U.S. Cybersecurity Coordinator, reinforced this idea, stating – quite surprisingly for a U.S. official at that time – that "the government needs to focus its cybersecurity efforts to fight online crime and espionage",[94] and that cyberwar "is a terrible metaphor [...] and a terrible concept."[95]

Conclusion

The recurrent analogies with the Cold War and the attempts to implement a cyber-deterrence doctrine display interesting insights, denoting a common mentality and a shared experience of Cold War amongst the people in charge of cybersecurity. However, it is necessary to examine these rigorously in order to assess the impact of such mind-sets on the current development of cybersecurity and defence strategies.[96]

Undoubtedly, it is difficult to avoid the extremely sensitive issue of interests at stake, and how they can influence the discourses on cyber-threats. Mary O'Connell notably states that "plainly some of the pressure to militarize cyber security is being driven by business concerns in the military security sector."[97] Accordingly, Myriam Dunn Cavelty displays that cybersecurity is a highly politicised issue in a context where "different bureaucratic entities that compete against each other for resources [and that] this is usually done by stating an urgent need for action."[98] Moreover, she points out that "being a cyber-expert has become a lucrative market, but only if the problem is continuously portrayed as grave."[99]

[89] Rid, *Cyber War*, pp. 163-166.

[90] Lawson, S. "Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States", *First Monday* [website], 17:7 (2012). http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270

[91] Lawson "Putting"

[92] Lewis, J. "The fog of cyberwar", *International Relations and Security Network* [website] (2009). http://isnblog.ethz.ch/intelligence/isn-weekly-theme-the-fog-of-cyberwar

[93] Lawson, "Putting".

[94] *Cited in* Singel, R "White House Cyber Czar: 'There is no Cyberwar'", *Wired* [website] (4 March 2010). http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

[95] *Cited in* Sigel "White House"

[96] *On this topic, see, e.g.*, Shachtman N & Singer, P. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive", *Bookings* (published 15 August 2011). http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman

[97] O'Connell, "Cyber Security ", p. 197.

[98] Cavelty, M. "The Militarisation of Cyberspace: Why Less May Be Better", International Conference on Cyber Conflict Proceedings, *CCD CoE*, 2012.

[99] Cavelty "The Militarisation".

In regard to the acceptance of the concept of cyberwar by certain scholars, but most importantly by the U.S. administration, Rid – in challenging the validity of this conceptualisation and its related security, political and legal consequences – provides a thought-provoking analysis. As he has persuasively displayed, the debate about cyberattacks has been militarized and is now dominated by the "terminology of warfare",[100] which distorts the issues in emphasising on prospective catastrophic scenarios, and is counter-productive in addressing existing cybersecurity concerns.[101] However, his rigid conception of war might ignore some pragmatic uses of cyberspace that already are or will become crucial in the conduct of warfare, and his assessment of cyberwar on the basis of documented cyberattacks that have already occurred cannot totally exclude the possibility of "cyber act of wars" in the future.

[100] Rid, "Cyberwar and Peace", p. 87.
[101] Rid, *Cyber War*, pp. 163-165.

Bibliography

Adams, J. “Virtual Defense”, *Foreign Affairs*, 80:3 (2001).

Arquilla, J. “Cyberwar Is Already Upon Us.” *Foreign Policy* [website](published 27 February 2012). Available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

Arquilla, J & Ronfeldt, D. “Cyberwar Is Coming!”, *Comparative Strategy*, 12:2 (1993).

Arquilla, J & Ronfeldt, D. “Cyberwar Is Coming!” In *Athena's camp: Preparing for conflict in the information age*, edited by John Arquilla and David Ronfeldt. Santa Monica: RAND, 1997, pp. 23-60. Originally published in *Comparative Strategy,* 12:2 (1993): pp.141-165.

Arquilla, J & Rondfeldt, D. *The Advent of Netwar*. Santa Monica: RAND, 1996.

Bendrath, R. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." *Information & Security: An International Journal*. 7 (2001), pp.80-103.

Buchan, R. “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?” *Journal of Conflict & Security Law*, Vol. 17, No. 2 (2012), pp. 211-227.

Clark, D & Landau, S. “Untangling Attribution.” *Harvard National Security Journal*, 2:2 (2011), pp. 25-40.

Clarke, R & Knake R. *Cyber War* (New York: Ecco 2010).

Clark, W & Levin, P. “Securing the Information Highway”, *Foreign Affairs*, 88:6 (2009), pp. 2-10.

Dunlap, C. “Perspectives for Cyber Strategists on Law for Cyberwar.” *Strategic Studies Quarterly* (Spring 2011), pp. 81-99.

Dunn Cavelty, M. “The Militarisation of Cyberspace: Why Less May Be Better.” International Conference on Cyber Conflict Proceedings, *CCD CoE*, 2012.

Gartzke, E. “The Myth of Cyberwar.” *International Security*, 38:2 (2013), pp. 41-73.

Knapp, K & Boulton, W. “Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments”, *Information Systems Management*, 23:2 (2006), pp. 76-87.

Lawson, S. “Putting the “war” in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States.” *First Monday* [website], 17:7

(2012). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270

Lewis, J. "The fog of cyberwar." *International Relations and Security Network* [website] (2009). Available at: http://isnblog.ethz.ch/intelligence/isn-weekly-theme-the-fog-of-cyberwar

Lynn, W. "Defending a New Domain", *Foreign Affairs*, 89:5 (2010), pp. 97-108.

Maurer, T. "The Case of Cyberwarfare." *Foreign Policy* (published 19 October 2011). Available at: http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar

McConnell, M. "How to win the cyber-war we're losing." *The Washington Post* [website] (28 February 2010). Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

NSA. "Biography - General Keith B. Alexander" [website]. Available at: http://www.nsa.gov/about/leadership/bio_alexander.shtml

O'Connell, M. "Cyber Security without Cyber War." *Journal of Conflict & Security Law*, Vol. 17, No. 2 (2012), pp. 187-209.

Panetta, L. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security." *U.S. Department of Defense* [website] (New York City, 11 October 2012). Available at: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

Rid, T. "Cyberwar and Peace", *Foreign Affairs*, 91:6 (2012), pp.77-87.

Rid, T. "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 35:1 (2012), pp. 5-32.

Rid, T. *Cyber War Will Not Take Place* (London: Hurst & Company, 2013).

Rid, T. "End this phony cyberwar", New Scientist, 219: 2933 (2013), pp. 26-27.

Rid, T & McBurney, P. "Cyber-Weapons", *The RUSI Journal*, 157:1 (2012), pp.6-13.

Rid, T. "Think Again: Cyberwar." *Foreign Policy* (published 27 February 2012). Available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar

Shachtman, N & Singer, P. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive." *Bookings* (published 15 August 2011). Available at: http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman

Singel, R. “White House Cyber Czar: ‘There is no Cyberwar’.” *Wired* [website] (published 4 March 2010). Available at: http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

Stone, J. “Cyber War Will Take Place!” *Journal of Strategic Studies*, 36:1 (2013), pp. 101-108.

U.S. Department of Defense. “The Cyber Domain: Security and Operations.” *U.S. Department of Defense* [website]. Available at: http://www.defense.gov/home/features/2013/0713_cyberdomain/

Valeri, L & Knights, M. “Affecting Trust: Terrorism, Internet and Offensive Information Warfare”, *Terrorism and Political Science*, 12:1(2000), pp. 15-36.

Stuxnet: The World's First Cyber… Boomerang?

Alex Middleton

Introduction

IN June 2012, two years after the initial discovery of the Stuxnet worm,[1] an excerpt from David Sanger's then soon to be released book entitled *Confront and Conceal* was published in the *New York Times*.[2] This piece, purportedly based on the testimony of several current and former American, European and Israeli officials, declared that Stuxnet – "the world's first fully fledged cyber weapon"[3] - was engineered by the United States and Israel as part of a wider covert operation aimed at undermining the Iranian nuclear program.[4] Whilst the United States and Israel had long been suspected of developing this complex piece of malware, Sanger described the nature of their involvement more fully than any previous account.[5] Operation Olympic Games, the codename for this alleged joint venture, may well have succeeded in achieving its goal of disrupting Iran's nuclear enrichment program (although this debate is far from settled) but the deployment of a weaponized worm, which would cause physical damage to a nation-state's nuclear infrastructure, is likely to have spawned some rather sour implications for International Politics. It is these that this paper focuses on.

This article argues that the release of the worm is likely to have: 1) fueled an on-going cyber arms race by demonstrating to other nations the strategic utility of cyber weapons; 2) elevated the severity of the cyber threat by providing a broad range of actors with a template from which to construct their own cyber weapons; 3) set a precedent for the use of cyber weapons as instruments of state policy.

It should be noted that Sanger's account is far from definitive proof that the United States and Israel were the culprits behind the attacks on Iran's Natanz nuclear enrichment facility. However, regardless of who conducted the assault, the implications raised in this paper still apply given that Stuxnet unearthed itself in the summer of 2010.

[1] Stuxnet was discovered in June 2010 by a Belarusian security company. International Institute for Strategic Studies. 'Stuxnet: targeting Iran's nuclear programme', *Strategic Comments*, 17:2 (2011) p. 1.

[2] Sanger, D. 'Obama Order Sped Up Wave of Cyberattacks Against Iran'. *The New York Times* (online), 1 June 2012. Available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

[3] Langner, R. 'Stuxnet: Dissecting a cyberwarfare weapon', *IEEE Security & Privacy*, 9 (2011) p. 49.

[4] Sanger, D. 'Obama Order'.

[5] Coll, S. 'Stuxnet and the Rewards (and Risks) of Cyber War'. *The New Yorker* (online), 7 June 2012. Available at http://www.newyorker.com/online/blogs/comment/2012/06/the-rewards-and-risks-of-cyberwar.html.

Stuxnet's Influence on the Cyber Arms Race

Interest and development in offensive cyber weapons programs certainly predates the release of Stuxnet. Even prior to its discovery in June 2010, U.S. intelligence officials had estimated there to be around twenty to thirty militaries with respectable offensive cyber capabilities.[6] There is of course great difficulty in determining the precise period in which nations began to build-up their cyber arsenals as, in the words of Richard Clarke, former U.S. presidential advisor for cyber security, "the entire phenomenon of cyber war is shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency".[7] Events such as the distributed denial of service (DDOS) attacks on Estonia and Georgia in 2007/2008, which saw their business, financial and media online communications severely hampered,[8] demonstrated the strategic utility of cyberspace and thus would have intensified the emerging cyber arms race. Stuxnet, however, is widely regarded as a "game changer".[9] Unlike the malware used in previous cyber-attacks, it was highly targeted and designed to achieve a real world outcome.[10] As Industrial Control System (ICS) security analyst Ralph Langner notes, rather than being designed for denial of service attacks or industrial espionage, "Stuxnet's goal was to physically destroy a military target - not just metaphorically, but literally".[11] This highly sophisticated worm was able to breach the air gap at Natanz and instruct cascades of bulky IR-1 centrifuges to spin into overdrive and self-destruct.[12] This act, U.S. officials claim, would have set back Tehran's purported nuclear arms project by eighteen months to two years.[13]

The appeal of generating a Stuxnet-like cyber weapon for the implementation of state policy is then vast. The impact the release of this worm is likely to have had on the development and proliferation of cyber weapons worldwide should not be ignored. Not only are future variants of Stuxnet perfectly suited to covert operations because they afford their user a high degree of anonymity,[14] (meaning that states need not be fearful of retaliation or international condemnation) but they are also low cost when compared to conventional weaponry[15] and likely to possess tremendous asymmetric properties. But ownership of these future versions may not be

[6] Clarke, R & Knake, R. *Cyber War – The next threat to national security and what to do about it, 1st paperback edition* (New York, HarperCollins Publishers, 2012), p. 64.

[7] Clarke & Knake, *Cyber War*, p. xi.

[8] Collins, S & McCombie, S. 'Stuxnet: the emergence of a new cyber weapon and its implications', *Journal of Policing, Intelligence and Counter Terrorism*, 7:1 (2012), p. 83.

[9] Hypponen, M. 'Viewpoint: Stuxnet shifts the cyber arms race up a gear'. *BBC News* (online), 14 July 2012. Available at http://www.bbc.co.uk/news/technology-18825742.

[10] Collins & McCombie, 'Stuxnet', p. 80.

[11] Langner, R. 'Stuxnet: Dissecting', p. 49

[12] Blanche, E. 'Cyber wars'. *The Middle East* (London), December 2012, p. 14.

[13] Blanche. 'Cyber wars', p. 14.

[14] Collins & McCombie, 'Stuxnet', p. 87.

[15] Collins & McCombie, 'Stuxnet', p. 88.

limited to nation-states with ample resources. As the following section will demonstrate, Stuxnet is likely to have altered the nature of the cyber threat by inspiring and empowering a wide range of actors.

Stuxnet - A Blueprint for Future Cyber Weapons

Sean Collins and Stephen McCombie state that "Stuxnet and the future cyber weapons it will inspire have fundamentally changed the scope of cyber threats".[16] Indeed, whilst the potential of cyber-attacks to be a significant threat to critical infrastructure had long been discussed, it was the discovery of this malware in 2010 that finally provided the proof of concept.[17] Not only would this have been likely to inspire militaries to develop similar cyber weapons, but also a host of other actors including terrorist organizations, organized crime syndicates and hacktivist groups.[18] Whilst there lacks concrete evidence to prove that it was the United States and Israel who engineered the worm, there exists little doubt as to the type of actor involved. As Claire Yorke, a cyber-security researcher at the think tank Chatham House, commented: Stuxnet's "sophistication and complexity suggests it would have required significant time and resources beyond the capability of non-state actors".[19] The same, however, cannot be said today. Indeed, after Stuxnet "escaped into the wild" and infected thousands of machines on the public Internet, there are fears that the readily available malware will be reverse engineered not only by nation states for military purposes but also by other malicious actors who could then use the worm’s code and structure as a blue print for designing their own cyber weapon.[20] As Richard Clarke states in the appendix of the revised edition of *Cyber War*: "thanks apparently to U.S. intelligence, hackers around the world ha[ve] a sophisticated tool to attack the kind of networks that run electrical power grids, pipeline networks, railways, and manufacturing processes in refineries and chemical plants".[21] "The best cyber weapon the United States has ever developed", he insists "it then gave to the world for free".[22]

Parties interested in replicating this potentially lethal cyber weapon may also be aided by the freely available analysis on it by security firms and anti-virus vendors such as Symantec, Kaspersky Labs and Langer Communications. Each have carefully dissected the malware and provided commentary on it. Whilst this information is of course highly valuable from a defensive standpoint, it could also, as Paulo Sharkarian has argued, be turned on its

[16] Collins & McCombie, ‘Stuxnet’, p. 80.
[17] Collins & McCombie, ‘Stuxnet’, p. 80.
[18] Collins & McCombie, ‘Stuxnet’, p. 89.
[19] Hopkins, N. ‘Stuxnet attack forced Britain to rethink the cyber war’. *The Guardian* (online), 30 April 2011. Available at http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran.
[20] Collins & McCombie, ‘Stuxnet’, p. 89.
[21] Clarke & Knake, *Cyber War*, p. 296.
[22] Rosenbaum, R. ‘Richard Clarke on Who Was Behind the Stuxnet Attack’, *Smithsonian Magazine* (online), April 2012. Available at http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html.

head and be used to provide inspiration, information and guidance for future cyber weapons development.[23]

The release of Stuxnet will have implications for all states reliant upon ICT; the U.S. itself is thus far from immune. Indeed, what the U.S. unleashed (assuming it was the U.S.) could well come back to bite them. Such fears occupy passages in a recent report sent to Congress. The document clearly expresses concern that Stuxnet could be adapted into a weapon that could be used to cause widespread damage to critical infrastructure located on U.S. soil.[24] Clarke shares similar concerns; he even goes as far as to label Stuxnet a "cyber boomerang"- a weapon that may one day come back around to hurt its original creators.[25]

Cyber Weapons as Instruments of State Policy

Soon after the discovery of the malware in June 2010 speculation grew that this offensive cyber action would open the floodgates to newer, increasingly devastating digital attacks. *The New Yorker*'s Steve Coll stated that Stuxnet "has established new and disturbing norms for state aggression on the Internet and its side-channels".[26] Misha Glenny even went as far as to suggest that "all countries that possess an offensive cyber capability will be tempted to use it now that the first shot has been fired".

Had Stuxnet been understood to be the work of a state like North Korea it might be interpreted by the international community as rogue behaviour, however with the U.S. as one the key architects, the use of cyber weapons leads to different conclusions. The role of the U.S. as a global leader with considerable power to set the agenda on issues of what is acceptable in terms of global conflict sets a precedent for future consideration of cyber weapons as a legitimate and effective tool of statecraft. Indeed, the non-violent nature of the attack may make it appear preferable to conventional kinetic weapons in some ways.

In fact, there have been no follow up attacks on the scale of Stuxnet. However, given the long planning process for that project and the fact that it remained undetected for many years, this is not in itself indicative of anything conclusive. The important implications of U.S. involvement in Stuxnet remain in terms of the way the use of cyber weapons is perceived by the international community. Whether that is a positive development leading to less violent solutions to global tensions or a negative development leading to an increase in state-based attacks on critical infrastructure remains to be seen.

[23] Shakarian, P. ‘Stuxnet: Cyberwar Revolution in Military Affairs’, *Small Wars Journal,* 7:4 (2011), p.8-9.
[24] Farwell, J & Rohozinski, R. ‘Stuxnet and the Future of Cyber War’, *Survival: Global Politics and Strategy*, 53:1 (2011), p. 36.
[25] Clarke & Knake, *Cyber War,* p. 296.
[26] Coll. ‘Stuxnet and the Rewards (and Risks) of Cyber War’.

Conclusion

It is quite clear that the goal of Stuxnet was to disrupt Iran's nuclear enrichment program. Regardless of whether this was part of a grander covert operation codenamed Olympic Games, the implications remain much the same. This paper has argued that the deployment of Stuxnet is likely to have: 1.) fueled an on-going cyber arms race by demonstrating to other nations the strategic utility of cyber weapons; 2.) elevated the nature of the cyber threat by not only providing evidence that well-guarded critical infrastructure could fall victim to a cyber-attack, but also because the malware and the analysis on it is readily available for a broad range of actors to access; and 3.) set a precedent, which contributes to the legitimization of cyber weapons as instruments of state policy. This highly sophisticated weaponized worm may have achieved its objective, but this is likely to have come at a cost; a cost which may in fact someday come back to harm its original creators.

Bibliography

Blanche, E. 'Cyber wars'. *The Middle East* (London), December 2012.

Clarke, R & Knake, R. *Cyber War – The next threat to national security and what to do about it, 1st paperback edition* (New York, HarperCollins Publishers, 2012).

Coll, S. 'Stuxnet and the Rewards (and Risks) of Cyber War'. *The New Yorker* (online), 7 June 2012. Available at http://www.newyorker.com/online/blogs/comment/2012/06/the-rewards-and-risks-of-cyberwar.html.

Collins, S & McCombie, S. 'Stuxnet: the emergence of a new cyber weapon and its implications', *Journal of Policing, Intelligence and Counter Terrorism*, 7:1, (2012) pp. 80-91.

Farwell, J & Rohozinski, R. 'Stuxnet and the Future of Cyber War', *Survival: Global Politics and Strategy*, 53:1 (2011), pp. 23-40.

Glenny, M. 'A Weapon We Can't Control'. *The New York Times* (online), 24 June 2012. Available at http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

Hopkins, N. 'Stuxnet attack forced Britain to rethink the cyber war'. *The Guardian* (online), 30 April 2011. Available at http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran.

Hypponen, M. 'Viewpoint: Stuxnet shifts the cyber arms race up a gear'. *BBC News* (online), 14 July 2012. Available at http://www.bbc.co.uk/news/technology-18825742.

International Institute for Strategic Studies. 'Stuxnet: targeting Iran's nuclear programme', *Strategic Comments*, 17:2 (2011) pp. 1-3.

Langner, R. 'Stuxnet: Dissecting a cyberwarfare weapon', *IEEE Security & Privacy*, 9 (2011) pp.
49-51.

Rosenbaum, R. 'Richard Clarke on Who Was Behind the Stuxnet Attack', *Smithsonian Magazine* (online), April 2012. Available at http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html.

Sanger, D. ‘Obama Order Sped Up Wave of Cyberattacks Against Iran’. *The New York Times* (online), 1 June 2012. Available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

Shakarian, P. ‘Stuxnet: Cyberwar Revolution in Military Affairs’, *Small Wars Journal*, 7:4 (2011), pp.1-10.

The Internet as a Slippery Object of State Security: The Problem of Physical Border Insensitivity, Anonymity and Global Interconnectedness

Memphis Krickeberg

Introduction

CYBERSECURITY is presented in the growing literature on the subject as an essentially “slippery” object for state security.[1] The Internet puts a lot of stress on the conventional conception of state security as the insurance of the state's survival in the international realm. In addition, cybersecurity supposedly leads to a reconfiguration of state security which must be apprehended through new paradigms. In this article we establish a typology of the main arguments found in cybersecurity discourses that emphasize fundamental differences between cybersecurity and more conventional factors of state security in international relations. This will be complemented by discussing the effects of these discourses on the sovereignty-focused framework through which state security has been traditionally conceived. Moreover, we will point to some potential consequences of these paradigmatic mutations on the national/international security nexus.

We identify three important factors underlying the “slippery” character of the Internet as an object of state security: the problem of physical border insensitivity, anonymity and global interconnectedness. These three categories constitute the core issues which systematically come up in descriptions of particular cyber-threats. They form the central thread behind a seemingly fragmented enumeration of threat narratives, ranging from cyber-terrorism, cyber-hacktivism, cyber-criminality and so on.

I – The problem of physical border Insensitivity

The insensitivity of Internet flows to physical frontiers undermines a whole tradition of border-based state security, i.e. what Foucault calls the “state of territoriality”; the aim of which is to keep enemies at distance - out of the

[1] See: Denning, D. ‘Cyber Security as an Emergent Infrastructure’, in *Security Education and Critical Infrastructures*, edited by Armstrong, H. Irvine, Cynthia (New York, Kluwer Academic Publishers 2003) pp.1-2; Libicki, M. *Cyberdeterrence and cyberwar*, (Santa Monica, Rand Corporation, 2009); Department of Homeland Security, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, Office of the United States Department of Homeland Security, 2009); Achiary, A. Auverlot, D. Hamelin, J. ‘Cybersécurité, l'urgence d'agir’,*Centre d'Analyse Stratégique*, Analysis note 324 (2013).

ring-fenced sovereign territory.[2] The Internet erodes the relevance and protective value of physical borders and distance. It allows for an aggressor to carry out attacks which undermine state sovereignty without ever being present on the attacked nation's territory. The standard example is the 2010 Stuxnet attack on an Iranian nuclear power plant. The attacker was able to deliver a serious blow to Iran's sovereignty by weakening its ability to be energetically self-sufficient and, in case the uranium treated in the plant was indeed destined for military purposes, by impairing its military capacity for territorial defense from a distance. Moreover, a growing consensus seems to be emerging among cybersecurity experts and government agencies on the limited protective effect of reproducing the traditional border logic on cyberspace to protect key networks such as military or governmental information systems. A 2008 report on the state of cybersecurity R&D published by the French Central Direction for the Security of Information Systems points out that the delimitation of “protection perimeters” through the use of technical tools such as filters or firewalls seems to be less and less effective to prevent cyber-attacks.[3] This is due to the great diversity of “hidden channels” available for an attacker to reach his target and to the “semantic richness of authorized flux” which makes it difficult to filter out the bad from the good.[4]

Rather than reproducing a logic of security aimed at keeping threats at a distance, the report advocates the re-enforcement of network resilience as well as the development of cyber-profiling measures designed to compare the degree of difference between particular flux and a model of “normal” flux behavior.[5] Thus, cybersecurity tends to invert traditional state security mechanisms in the realm of international relations. Openness, i.e. acknowledging the irrelevance of territory emerges as the norm, while bordering, at least in its traditional sense of drawing out fixed lines between an outside and an inside, becomes the exception.

II- The problem of anonymity

The problem of anonymity on the Internet undermines another great foundation of state security: the division between friends and enemies in the international system. Enemies can be defined as such because malevolent acts or intentions can be, rightly or not, attributed to them. The Internet replaces attribution with speculation. Of all the cyber-attacks usually described in the literature, the 2007 cyber-attacks against Estonia, the 2010 Stuxnet attack or the 2013 attacks against various American newspapers, not one was linked with a 100 % certainty to any specific state or even any particular actor.

[2] Foucault, M. *Sécurité, Territoire, Population: Cours au Collège de France*, 1977-1978, (Paris, Seuil, 2004).

[3] Chabaud, F. *Recherche et développement en sécurité des systèmes d'information : orientations et enjeux*, (Paris, Direction centrale de la sécurité des systèmes d'informations, 2008) p.4.

[4] Chabaud, F. *Recherche et développement.* p.4

[5] Chabaud, F. *Recherche et développement.* p.7

The difficulties that this absence of attribution causes for security actors have been widely covered in the existing cybersecurity literature.[6] Therefore, we choose a different angle to look at the conflict between anonymity on the Internet and state security in the realm of international relations. While traditionalist and realist literature on security tends to see the sphere of international relations as autonomous and separated from domestic security, certain critical accounts of security practices have studied the use of international security issues to legitimize internal security dynamics and social control.[7] Thus, referring to the international order, to a sphere of potentially inimical forces, has been at the core of the provision of "ontological security" by the modern state.[8] Ontological security refers to how security practices generate a certain type of political and social order.[9] Hence, the modern state has progressively displaced traditional hierarchies such as the church by mediating between the daily life of its citizens and their anguish of violent death.[10] To put it simply, until the end of the Cold War, hostile states incarnated the main figure of the enemy and internal subversive movements or suspicious social groups were very often framed as agents of foreign powers. States can be easily denounced and/or constructed as inimical by the state and recognized as such by the population. The state can thereby assume the role of protector against its designated enemies and generate an impression of certainty among national citizens.[11]

The absence of certainty concerning the nature of malevolent actors on the Internet puts stress on the national state's function of generating "ontological security". We argue that the diverging assessments of the successful/ unsuccessful outcomes of cyber-threat securitizations show the uncertainty prevalent among academics and cybersecurity practitioners as to whether the alleged danger of cyber-threats is as easily understood by the general public as the "great danger" of the Soviet-Union during the Cold War, "rogue-states" in the 1990s and 2000s or even "terrorists" today.[12] The militarization of cybersecurity currently taking place in the US, i.e. the tendency to regard cyber-attacks as potential acts of war, combined with the use of historically

[6] See: Libicki, M. *Cyberdeterrence and cyberwar,* (Santa Monica, Rand Corporation, 2009); Deibert, R. 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 4 (2010) pp.15-32; Chapter 5 "Diffusion and Cyberpower" Nye, J. *The future of power*, (Philadelphia, Public Affairs, 2011).

[7] Campbell, D. *Writing Security: United Sates Foreign Policy and the Politics of Identity* (Minneapolis, University of Minnesota Press, 1998).

[8] Huysmans, J. 'Security! What Do You Mean? From Concept to Thick Signifier', *European Journal of International Relations*, 4:2 (1998) pp. 226–255.

[9] Huysmans, J. *Security!*

[10] Huysmans, J. *Security!*

[11] Huysmans, J. *Security!*

[12] See: Hansen, L & Nissenbaum H. 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly,* 53 (2009) pp. 1155–1175; Labrie, M. *La sécurisation du cyberterrorisme aux Etats-Unis Thèse de maîtrise* (Montreal, Université du Québec à Montréal, 2011).

pregnant war metaphors such as "cyber-Pearl Harbor", can be interpreted as an attempt to make cybersecurity more intelligible to public opinion by framing it through the familiar friend/enemy distinction which still constitutes a core paradigm of international relations and its mainstream interpretations. However, the plain fact that no cyber-attack until this day has caused as much damage as any act of physical warfare makes us cast doubt on the US' capacity to render credible its cyber-war/ "real war" comparison. The absence of violent death in cybersecurity matters appears to have left the general public indifferent to the "great menace" of cyber-threats.

III- The problem of interconnectedness and its impact on the state as a primary referent-object of security in international relations

Whereas anonymity poses the question of who the enemy is or what the threats are, another problem for state security posed by cybersecurity discourses is designating the actual referent-object of cybersecurity. Hence, it appears that due to the global interconnectedness of networks which transcends the distinction between national/international as well as public/private spheres, the state can hardly be isolated as a separate referent-object of security anymore. Although one has to be wary of technological-deterministic views which isolate "global interconnectedness" as a self-governing force which unilaterally changes (inter)national security configurations, the massive extension of the Internet does constitute a major condition of possibility of contemporary security mutations.[13] Not only do states heavily rely on private networks but "vital infrastructures" also depend on the latter. This state of interconnectedness is used to feed a rhetoric of "cascading effects" of cyber-threats and attacks; a rhetoric that now tends to replace the traditional state-centered notion of security.[14] Hansen and Nissenbaum conclude their analysis of cybersecurity discourses by pointing out that: "academic and policy discourse articulates in sum a wide array of threats to government, business, individuals, and society as a whole perpetuated by hackers, criminals, terrorists, commercial organizations, and nations that adopt cyber strategies for financial, ideological, political, or military gain".[15] This new trend in state-security discourses has four major consequences for international relations.

Firstly, the mutual dependency of states and societies on global computer networks legitimizes and accelerates a de-differentiation between security realms: between cyber-terrorism and cyber-crime, between cyber-war and cyber-(h)ac(k)tivism, between the police and the military field. This generates fundamental uncertainty among states as to the best way of dealing with cybersecurity. The projection of traditional and often aggressive

[13] Carr, M. *The Irony of the Information Age: US Power and the Internet in International Relations, Doctoral Thesis* (Canberra, Australian National University, 2011). p.64

[14] Hansen, L & Nissenbaum H. *Digital Disaster.* p.1161

[15] Hansen, L & Nissenbaum H. *Digital Disaster.* p.1162

national and military vocabularies on cybersecurity by the US can be interpreted as a potential solution to this problem. However, we argue that such a framing of cybersecurity does not necessarily indicate the dominant direction cybersecurity will take in the coming years but should rather be regarded as one type of discourse competing with others emanating from different actors.[16] For example, the International Telecommunications Union emphasizes the need for greater *transnational cooperation* in terms of cybersecurity generated by global interconnectedness.[17]

Secondly, rather than undermining the realist association between sovereignty and security, cybersecurity reconfigures it. Indeed, the language of sovereignty is still very strong in cybersecurity discourses and has actually been reinforced with the recrudescence of alleged state-based cyber-attacks in the last few years. The 2013 French White Paper on Defense (FWPD) clearly illustrates this: "The capacity to (...) protect ourselves against cyber attacks (...) has become an element of national sovereignty".[18] However, sovereignty cannot be understood anymore as a mere attribute of the state which is somehow spatially "contained" in an envelope of physical borders. Instead, a new post-territorial notion of sovereignty which "is more ambiguously located than in traditional national-military security" emerges from cybersecurity discourses.[19] This enhanced notion of sovereignty articulates national security together with the need to protect national economic interests allegedly menaced by cyber-threats as well as with the necessity to preserve the competitiveness of national companies which provide the infrastructure and tools of cybersecurity. Although sovereignty has always been used to legitimize the advancement of the economic interests of national ruling classes at the international level, the language of sovereignty and economics were formally two separate semantic spheres. Thus, the reference to global interconnectedness seems to be a powerful discursive move to bridge the two narrative fields.

Thirdly, cybersecurity generates new forms of international tensions which cannot be reduced to the traditional conflictual logics and security dilemmas which are usually associated with states' supposedly "eternal" quest for security.[20] The adoption by a state of a particular type of cybersecurity grammars and practices can potentially contradict other cybersecurity objectives of the same state or other states. A major distinction can be made between types of cybersecurity narratives based on Deibert's differentiation between risks *to* cyberspace i.e. "risks to the physical realm of computer and communication technologies" and risks *through* cyberspace i.e. "risks that arise from cyberspace and are facilitated or generated by its technologies,

[16] Hansen, L & Nissenbaum H. *Digital Disaster.* p.1162

[17] Wamala, F. *ITU National Cybersecurity Strategy Guide* (Geneva, International Telecommunications Union, 2011). pp.48-49

[18] Ministry of Defence. *French White Paper. Defense and National Security,* (Paris, Office of the Ministry of Defence of the French Republic, 2013). p.100

[19] Hansen, L & Nissenbaum H. *Digital Disaster.* p.1162

[20] Aron, R. *Paix et guerre entre les nations* (Paris, Calman-Lévy, 2004).

but do not directly target the infrastructures per se".[21] These two risks categories are related to a specific national/international dialectic. Thus, there seems to be a "robust international consensus, growing communities of practice, and an emerging normative regime around risks to cyberspace" taking the form, for instance, of the ITU's Global Cybersecurity Agenda framework which provides an inter-governmental platform to discuss cybersecurity issues.[22]

However, the monitoring, filtering of networks and censoring of content by certain states for various reasons, often pertaining to national security as in China's Golden Shield Program, can be potentially detrimental to the objective of a functioning and free-flowing global network put forward by cybersecurity, understood as security *of* the networks. [23] Although Deibert's dichotomy constitutes a good starting point to understand the complex relationship between cybersecurity, the national and the international level and how cybersecurity differentiates itself from more conventional state security factors, we argue that it needs to be refined. Indeed, Deibert's dichotomy tends to presume a natural association between, on the one hand, technical aspects with the international level and, on the other hand, political considerations with the national level. However, the seemingly "strictly" technical issue of defining threats to cyberspace can be just as political as threats from cyberspace and re-framed in the language of national sovereignty. This can happen for example when certain foreign-made technical devices essential for the proper functioning of networks such as routers are presented as national cybersecurity threats. In the French Senatorial Report on Cyber defense of July 18, 2012 the need for a European ban of Chinese fabricated routers was advocated because of the supposed presence of "back-doors" and spying tools. It called for their replacement by European-made equipment.[24] Two conclusions on the state security/cybersecurity/ international relations nexus can be drawn from this example: 1) Global interconnectedness does not erode national state security considerations. Technology itself does not automatically generate a new "global" form of security. 2) Cybersecurity relocates national security issues in new domains and therefore requires state security to be viewed through other lenses than the perspective of war or other types of violent confrontations.

[21] Deibert, R. 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 4 (2010) p.15.

[22] Deibert, R. *Risking Security*. p.15
Wamala, F. *ITU Cybersecurity*.

[23] Paganini, P. 'The business of censorship. Golden Shield Project, but not only ...' *Security Affairs*, [Blog] 19 November 2011, Available at: http://securityaffairs.co/wordpress/204/cyber-crime/business-of-censorship-golden-shield-project-but-not-only.html

[24] Bockel, J, M. 'Jean-Marie Bockel salue les dispositions du nouveau Livre Blanc en matière de cyberdéfense', *Jean-Marie Bockel* [Blog] 30 April 2013, Available at: http://jeanmariebockel.fr/jean-marie-bockel-salue-les-dispositions-du-nouveau-livre-blanc-en-matiere-de-cyberdefense

Finally, a fundamental paradigmatic change pertaining to the status of the state in international relations seems to be emerging from within cybersecurity discourses. Since the construction of the Westphalian order, state elites have always referred to the state as the primary referent-object of security in the realm of (western) international relations. The justification for the prioritization of state security has rested on the assumption that the state is the principal defender of the sovereign territory's integrity, the guarantor of "national unity" and the main protector of "societies" envisaged as "national communities". In this traditional paradigm, sub-fields of security such as the security of populations have tended to be considered as derivative of state security; as secondary issues.[25] Cybersecurity tends to erode this hierarchisation of security. Indeed, if state security is increasingly dependent on the proper functioning of predominantly private networks and if global interconnectedness fogs the distinction between state and private security, then the security of networks itself become the ultimate referent object of security from which state security derives.

This development seems paradoxical because the Internet was built upon research conducted by the RAND Corporation and the United States Department of Defense Advanced Research Projects Agency (DARPA) in the 1960s which sought to make military communication systems more resilient in the face of a nuclear attack (i.e. to reinforce the state's independence and status as the primary unit of survival).[26] As long as the Internet was restricted to exclusive military and academic circles, cybersecurity wasn't an issue in international relations. This changed with the massification of the Internet in the 1990s. Security shifts here from the defense of the state per se to the protection of flux circulation and networks. Although, as pointed out above, the Internet as such does not automatically engender transnational security dynamics, the objective of ensuring the circulation of information flow and sorting out between "good" and "bad" flux requires a full degree of transnational cooperation to be truly effective.[27] Hence, a tension arises between the necessity to secure the networks of global capitalist flux circulation and an international order still composed of sovereign and potentially rival states defending their national bourgeoisies and which are still greatly influenced by "traditional" and realist-type security paradigms.

[25] This sovereignist view of security traditionally formulated by state elites and realists has of course never adequately reflected the effectivity of modern security logics. Indeed, Foucault has shown that security cannot be reduced to territorial defense but is to be envisaged as the counterpart and condition of possibility of modern governmentality i.e. the particular logic of power that emerged in the 18th century and which "has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument". Foucault, M. *Security, Territory, Population: Lectures at the Collège de France,* (Hampshire, Palgrave MacMillan, 2009). p.144

[26] Ryan, J. *A history of the Internet and the digital future*, (London, Reaktion Books, 2010).

[27] Wamala, F. *ITU Cybersecurity.*

Conclusion

Cybersecurity narratives rest on a potentially deterritorialized and undetermined threat figure which equally menaces a wide array of referent-objects. It therefore appears to destabilize deep-rooted knowledge on what state security should be about in the realm of international relations. Moreover, it undermines the state's capacity of providing credible threat figures emanating from a "menacing outside" to its own populations. At the same time as cybersecurity discourses struggle to emphasize particular threat *figures*, incarnated by enemy states or terrorists, in a credible manner, the focus of security increasingly shifts to technical *vulnerabilities* which compromise flux circulation and associated risk calculations.

However, while cybersecurity discourses tend to present the re-conceptualizing of state security studied above as an outcome of increased computer-interconnectedness, we would like to point out that these discourses are inscribed in a semantic field which has rendered a traditional, realist-type notion of state-security heavily ignored over, at least, the past thirty years. Further critical research should demonstrate how cybersecurity practices and discourses do not generate but merely amplify the de-differentiation of security domains and the reference to a "continuum of threats" narrative which has characterized the development of international security since the 1980s.[28] Stressing the historical continuity between these securitarian evolutions and cybersecurity would be a welcome step towards countering national and transnational discourses which use the so-called "novelty" of cyber-threats to further (in) securitize the Internet and dismantle/restructure its open character.

[28] C.A.S.E. Collective, 'Critical Approaches to Security in Europe: A Networked Manifesto', *Security Dialogue*, 37:4 (2006) pp. 443-487.

Bibliography

Achiary, A. Auverlot, D. Hamelin, J. ‘Cybersécurité, l'urgence d'agir’,*Centre d'Analyse Stratégique*, Analysis note 324 (2013).

Aron, R. *Paix et guerre entre les nations* (Paris, Calman-Lévy, 2004).

Arquilla, J. ‘Cyberwar is already among us. But can it be controlled?’, *Foreign Affairs*, 91:2 (2012).

Bockel, J, M. ‘Jean-Marie Bockel salue les dispositions du nouveau Livre Blanc en matière de cyberdéfense’, *Jean-Marie Bockel* [Blog] 30 April 2013, Available at: http://jeanmariebockel.fr/jean-marie-bockel-salue-les-dispositions-du-nouveau-livre-blanc-en-matiere-de-cyberdefense

Campbell, D. *Writing Security: United Sates Foreign Policy and the Politics of Identity* (Minneapolis, University of Minnesota Press, 1998).

Carr, M. *The Irony of the Information Age: US Power and the Internet in International Relations, Doctoral Thesis* (Canberra, Australian National University, 2011).

C.A.S.E. Collective, ‘Critical Approaches to Security in Europe: A Networked Manifesto’, *Security Dialogue*, 37:4 (2006) pp. 443-487.

Chabaud, F. *Recherche et développement en sécurité des systèmes d'information : orientations et enjeux*, (Paris, Direction centrale de la sécurité des systèmes d'informations, 2008).

Deibert, R. ’Risking Security: Policies and Paradoxes of Cyberspace Security’, *International Political Sociology*, 4 (2010) pp.15-32.

Denning, D. ‘Cyber Security as an Emergent Infrastructure’, in *Security Education and Critical Infrastructures*, edited by Armstrong, H. Irvine, Cynthia (New York, Kluwer Academic Publishers 2003) pp.1-2

Department of Homeland Security, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, Office of the United States Department of Homeland Security, 2009).

Foucault, M. *Sécurité, Territoire, Population: Cours au Collège de France*, 1977-1978, (Paris, Seuil, 2004).

Foucault, M. *Security, Territory, Population: Lectures at the Collège de France*, (Hampshire, Palgrave MacMillan, 2009).

Hansen, L & Nissenbaum H. ‘Digital Disaster, Cyber Security, and the Copenhagen School’, *International Studies Quarterly,* 53 (2009) pp. 1155–1175.

Huysmans, J. ‘Security! What Do You Mean? From Concept to Thick Signifier’, *European Journal of International Relations*, 4:2 (1998) pp. 226–255.

Labrie, M. *La sécurisation du cyberterrorisme aux Etats-Unis Thèse de maîtrise* (Montreal, Université du Québec à Montréal, 2011).

Libicki, M. *Cyberdeterrence and cyberwar,* (Santa Monica, Rand Corporation, 2009).

Ministry of Defence. *French White Paper. Defense and National Security,* (Paris, Office of the Ministry of Defence of the French Republic, 2013).

Nye, J. *The future of power*, (Philadelphia, Public Affairs, 2011).

Paganini, P. ‘The business of censorship. Golden Shield Project, but not only ...’ *Security Affairs,* [Blog] 19 November 2011, Available at: http://securityaffairs.co/wordpress/204/cyber-crime/business-of-censorship-golden-shield-project-but-not-only.html

Ryan, J. *A history of the Internet and the digital future*, (London, Reaktion Books, 2010).

Wamala, F. *ITU National Cybersecurity Strategy Guide* (Geneva, International Telecommunications Union, 2011).

Internet Freedom: Rhetoric Versus Reality

Vaughan Austin Holding

Introduction

IN the last few years the Internet has borne witness to and facilitated a great deal of social and societal change. From Hilary Clinton's positive 2010 address; 'Remarks on Internet Freedom', to the Tunisian and Egyptian revolutions that showcased the power of social media, the internet, its use and power, has been at the forefront of recent news.[1] However, equal to, if not overtaking the positive and enabling factors of the Internet in recent years are the many controversies surrounding it. While undoubtedly carrying the potential to do great good, the Internet has been plagued with numerous impediments, setbacks and controls that greatly damage its offered freedoms. ACTA, SOPA, PIPA, Tempora, Prism, DMCA and adult content opt in, are all examples of recent controversies surrounding freedom on the Internet.[2] What is particularly surprising is that all of these restrictions to freedom stem from the very states that laud Internet freedom so highly. The US and UK being so publicly supportive of Internet Freedom in rhetoric, yet so thoroughly undermining it in action represents a key impediment to global Internet Freedom. If the leading global states are unwilling to forward Internet Freedom in any more than word, how can others be expected to in deed? The current system of Internet governance in general presents a relatively hostile environment within which to foster Internet Freedom. The power of large corporations and companies is immense and the influence they have is equal to their power. Both of these factors further impede the proliferation of Internet Freedom in a way that is currently being decided in the courts of the United States. It is not the undemocratic states that appear to pose the largest threat to Internet Freedom, but the very states that should be protecting it.

[1] Clinton, H. 'Remarks on Internet Freedom' *Washington.* 21 January 2010
Available at: http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

[2] Note: Stop Online Piracy Act (SOP) and; Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) were United States House and Senate Bills that would have forced Internet Service Providers (ISPs) to adhere to strict laws regarding copyrighted material and police content and Internet users. Both Bills died before they were enacted in the face of massive public opposition. Anti-Counterfeiting Trade Agreement (ACTA) is a similar proposal coving much of Europe, Canada, Australia and New Zealand. Although having many signatory states, ratification limits are yet to be reached meaning the agreement is not in force. Digital Millenium Copyright Act (DMCA) is part of US copyright law that was extended to cover Internet content that may violate existing laws. PRISM and TEMPORA are programs run by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ). Both programs are similar and act as meta data mining programs of online and phone communications. Details of the secret programs were leaked as part of the Edward Snowdon leaks. Adult content opt in is an initiative by the UK government requiring consumers to 'opt in' to have the ability to access online pornography when they sign up with a new ISP. Blocking of online pornography is an attempt to stop minors accidentally accessing it. The opt in came in to effect in early 2014.

This piece will begin by presenting a distinction of the different aspects of Internet Freedom and a brief outline of its current global standing. It will then explain the damage caused by the disparity between freedom rhetoric and reality, after this it will move to explain the current systems of governance and the hostile environment this creates for global Internet freedom. Finally, this work will offer a small and by no means conclusive list of possibilities that would ease the transition to wider freedoms before drawing together the conclusions into a brief summary.

Distinct Aspects

Internet Freedom is an amalgam of two distinct aspects. The initial aspect is the actual physicality of connection; being able to access infrastructure such as computers, phone lines or mobile devices. With the rapid pace of technological advancement, the dropping costs linked to Moore's Law and programs like the Mark Zuckerberg fronted internet.org, access rates to infrastructure are increasing rapidly.[3] There are numerous other programs that aim to reduce the digital divide and new Internet users are joining the web each day. Therefore, this piece will concentrate primarily on the second aspect of Internet Freedom; unfettered access to online content.

Recently declared a human right under the 2012 United Nations Human Rights Council resolution 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (HRC 2012, Resolution A/HRC/20/L.13), online interactions are now afforded protection equal to offline, real world interaction.[4] The HRC 2012 resolution links to The Universal Declaration of Human Rights Article 19, specifically the protection of free speech as an attempt to further Internet Freedom through uncensored discourse and content regardless of frontiers.[5] Although now considered a human right, the HRC 2012 resolution has appeared relatively impotent since its adoption and there are still extensive levels of censorship online. There are numerous reasons for online censorship but one of utmost pertinence is that it is almost impossible to form a global consensus on content and access that will attract global support.

As with any contentious subject there will be differing norms and views. The Internet is no exception. Different States have different societal norms and

[3] internet.org is a foundation aimed at bringing cheap and simple Internet infrastructures to the world's poorest areas in order to make them part of the 'knowledge economy' and bring the advantages of the Internet to them. internet.org, *Introductory Video.* Available at http://www.internet.org*;* Intel co-founder Gordon Moore's simple law; "The number of transistors incorporated in a chip will double approximately every 24 months" has been linked to a decrease in cost as technology increases. Intel, *Moore's Law explanation.* Available at http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html

[4] United Nations General Assembly, Human Rights Council. 'The promotion and enjoyment of human rights on the Internet'. 29 June 2012. Resolution A/HRC/20/L.13. Available at http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280

[5] Universal Declaration of Human rights. Available at http://www.un.org/en/documents/udhr/

these are reflected in Internet content and acceptable online subjects. Simply put, not everyone *wants* to have free and unfettered access to the Internet. The ideals of Internet Freedom are prevalent mainly in Western states. Many states view much Internet content as offensive and adversely influential, one just has to consider the 'Innocence of Muslims' riots of 2012.[6] Of course in any state there will be a continuum between those that wish to access all material and make their own decisions and those that wish to be shielded from certain content. The logical outcome of this would be to make the Internet completely free and have consumers set their own individual parameters of censorship, however as shall be expounded, this is not a realistic proposition and generally leads to a level of censorship that will vary from region to region, state to state.

Rhetoric Versus Action in Western States

The United States, a country that prides itself in its history of liberty and freedom, certainly has a strong public rhetoric regarding Internet Freedom. Indeed, Hillary Clinton has presented several public speeches that provide a litany of the ways that the Internet can enhance a state's economy, religious freedom and democracy. However just months after her 2010 address, 'Remarks on Internet Freedom' it was discovered that the US had launched a concerted and highly advanced cyber attack against Iran.[7] The hypocrisy of lauding the democratizing factors of a free Internet while simultaneously using it as an advanced attack mechanism was not a one off. In 2013 the Edward Snowden leaks highlighted the NSA PRISM program, a classified system forcing US ISPs and phone providers to supply a huge amount of metadata to US security agencies for analysis, and allowing the NSA direct access to company servers. [8] Given Hillary Clinton's position as Secretary of State (who also serves on the National Security Council) at the time both events were underway it seems likely that Clinton was aware of the actions. This kind of hypocrisy is incredibly damaging to any of the legitimate claims or attempts at supporting Internet Freedom. Even more recently in October 2015, the Cybersecurity Information Sharing Act (CISA) bill was passed.[9] CISA allows technology companies to share information on cyber threats with US authorities and other companies in order to enhance group security,

[6] Kirkpatrick, D. 'Anger Over a Film Fuels Anti-American Attacks in Libya and Egypt'. *The New York Times* (online) 11 September 2012. Available at http://www.nytimes.com/2012/09/12/world/middleeast/anger-over-film-fuels-anti-american-attacks-in-libya-and-egypt.html?_r=0

[7] See Stuxnet attack:
Farwell, J.& Rohozinski, R. 'Stuxnet and the Future of Cyber War', *Survival: Global Politics and Strategy*, 53:1 (2011); Langner, R. 'Stuxnet: Dissecting a Cyber Warfare Weapon', *Security and Privacy, IEEE*, 9:3 (2011).

[8] Greenwald, G. & MacAskill, E. 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian* (online) 7 June 2013.
Available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[9] Thielman, S. 'Senate passes controversial cybersecurity bill Cisa 74 to 21', *The Guardian* (online) 27 October 2015. Available at http://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote

however the bill is vague enough to allow for large scale personal data sharing without a warrant.[10] President Obama signed the bill into law, which was attached to the federal funding 'omnibus' bill, on the same day that the rest of America was preoccupied with the release of the newest Star Wars film. If leading states such as the US do not fully support Internet Freedom, or discuss it in an open and honest manner then there seems little hope for a global movement.

Internet Freedom is a continuum line of liberty and security, the more freedom, generally the less security and vice versa. As has been briefly shown the Internet is a powerful tool indeed at a state level for surveillance and other means. One expects a degree of control and surveillance in non-democratic states such as China and Cuba and these abuses of freedom are well documented.[11] The propensity to abuse Internet freedoms by democratic states however provides a much bigger impediment to Internet Freedom as a whole. If the states that support Internet Freedom are not willing to adhere to their own rhetoric the hypocrisy is an instantaneous barrier to spreading the freedoms they claim to support through foreign policy. Presumably it will also raise questions as to why the US and UK would support Internet Freedom and its proliferation when they are perfecting means of using it as a surveillance tool. The Internet offers such attractive surveillance opportunities to security services that unfettered, unrestricted and anonymous Internet access does not seem a realistic global goal. Just like Western democratic states, states that are not governed by a system of democracy are acutely aware of the power that the Internet has to facilitate subversion of state control.[12] The Arab spring uprising is a prime example of the dangers that the Internet can impose on a government. Between these two it seems unlikely that either type of state will gain dramatically from advancing Internet Freedom.[13]

[10] Reynolds, M. 'CISA security bill passes Senate with privacy flaws unfixed', *Wired* (online) 27 October 2015-12-23. Available at http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/

[11] Freedom House reports on China and Cuba
Freedom house, *China Internet Freedom Report*. (2013) Available at http://freedomhouse.org/report/freedom-net/2013/china#.UtbPvWRdVH0; Freedom House, *Cuba Internet Freedom Report*. (2013). Available at http://freedomhouse.org/report/freedom-net/2013/cuba#.UtbQA2RdVH0

[12] Stepanova, E. 'The Role of Information Communication Technologies in the "Arab Spring": Implications Beyond the Region'. *PONARS Eurasia Policy Memo No. 159* (2011) p. 2
Available at http://ponarseurasia.com/sites/default/files/policy-memos-pdf/pepm_159.pdf; Allagui, I & Kuebler, J. 'The Arab Spring and the Role of ICTs', *International Journal of Communication,* 5 (2011) p. 1436. Available at http://www.arifyildirim.com/ilt508/ilhem.allagui.pdf

[13] There are some proponents that propose the merits of advancing and projecting power through openness and reversing censorship, however the amount and scope of writing seems relatively narrow and does little to encompass the wider pictures and issues yet still raises and presents some cogent arguments. See: Carr, M. 'Internet Freedom, Human Rights and Power', *Australian Journal of International Affairs,* 67:5 (2013)

Corporate Power

The current system of laws and Internet governance that stems from the US monopoly on Internet control simply does not support widespread freedom promotion. The US government is particularly susceptible to large lobbying bodies and some of the largest of these bodies are the well-funded music and movie industry trade bodies. These bodies have the congressional influence and money to quickly move bills through congress that favour control over freedom. While the SOPA and PIPA bills were killed in house it was only through the opposition and awareness brought by some of the Internet giants such as Google, Twitter and Wikipedia.[14] Large bodies have a great deal of influence in congress and therefore pose a real risk to Internet Freedom when that runs counter to their wishes. As has been shown they *can* be overruled by popular public opinion but only with the backing of equally large organisations. The CISA bill however, was not so easily curtailed. Even the HRC 2012 resolution, that protects human rights on the Internet, appears to offer little real protection. The Electronic Frontier Foundation keeps a track of US court cases stemming from online actions and interactions that threaten to set precedents for future online freedom of speech issues.[15] Many of these court cases seem to have been offered little protection under Article 19 of the Universal Declaration of Human Rights that was reaffirmed under HRC 2012. A recent case whereby an Estonian online news aggregator, Delfi, was held liable by the European Court of Human Rights for third-party posted comments, has the potential to set an incredibly damaging precedent. Even in the face of the HRC 2012 resolution, it was decided in the Strasbourg court that this particular human right is not applicable.[16] The slow increase of intermediary liability and accountability may well represent the first steps of a slippery slope that will see ISPs become increasingly and eventually overly cautious in content moderation for reasons of liability protection.[17] While clearly this is a hypothetical scenario, the beginnings of a slippery slope are becoming apparent. If Internet governance does indeed place further filtering and responsibilities on ISPs and other intermediaries, then Internet Freedom as a global prospect becomes severely impinged. In another recent and pivotal turn, the US court of appeals for the District of Columbia has made a ruling against net neutrality.[18] Net neutrality is the

[14] Internet's dark day: Anti-piracy bills take a beating. *The Seattle Times* (online) 18 January 2012. Available at http://seattletimes.com/html/nationworld/2017274222_sopa19.html

[15] Free speech information, *Electronic Frontier Foundation.* Available at https://www.eff.org/issues/free-speech

[16] Guillemin, G. *Case Law, Strasbourg: Delfi AS v Estonia: Court Strikes Serious Blow to Free Speech Online.* Inforrm Blog (online) 15 October 2013. Available at http://inforrm.wordpress.com/2013/10/15/case-law-strasbourg-delfi-as-v-estonia-court-strikes-serious-blow-to-free-speech-online-gabrielle-guillemin

[17] Schellekens, M. 'Liability of Internet Intermediaries: A slippery Slope?', *SCRIPTed,* 8:2 (2011) p. 168. Available at http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/schellekens.asp

[18] Roberts, D. 'Appeals Court Rules Against FCC's Right to Protect Net Neutrality. *The Guardian* (online) 14 January 2014. Available at http://www.theguardian.com/technology/2014/jan/14/net-neutrality-internet-fcc-verizon-court; Fung, B. 'Federal Appeals Court Strikes Down Net Neutrality Rules'. *Washington Post* (online) 14 January 2014. Available at

equal and non-preferential treatment of all websites and services and is integral to the spread of global Internet Freedom through equal and unfettered access.[19] The DoC court ruling while not final if upheld would enable ISPs to boost or curtail speeds to specific sites. It would also mean that ISPs could charge connection fees to popular sites such as Facebook, YouTube and Twitter or bandwidth hungry sites such as Netflix or Hulu.[20]

Should this ruling be upheld it would become a major impediment to global Internet Freedom. With ISPs providing services based on a discriminatory and profit based model the potential for ISPs to block or throttle access to competitors' sites would be great. Clearly this limitation of content would run completely contrary to the basic tenets of Internet Freedom and as such represent the potential for a severe impediment to the spread of global Internet Freedom.

Multi-Stakeholderism - A Case of Too Many Cooks

As previously mentioned, the current power of lobbying bodies and the move toward intermediary liability runs counter to the proliferation of Internet Freedom. It becomes increasingly apparent that the current multi-stakeholder system can only facilitate a restricted level of Internet. Multi-stakeholderism is such a complex method of governance that is does little to promote and facilitate the free potential of the Internet. This governance system is an incredible complex one that finely balances many different systems, governments, companies and states. However, this balance is potentially very precarious given that "different logics, languages and political cultures enter the scene, when different stakeholders share the same political arena".[21] There are so many bodies involved in the multi-stakeholder approach, and as previously discussed, the different societal, political, economic and security views, culminate to create incredible difficulty for minor issues to be resolved let alone an issue such as global Internet Freedom.

Potential Alternative Systems

The Internet has become very adept at governing itself on a small scale. Many popular websites such as Reddit and Imgur run based on a user generated ranking system and simple algorithms.[22] There is very little

http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/14/d-c-circuit-court-strikes-down-net-neutrality-rules/

[19] Ciarlo, M. A Guide to the Open Internet. *the*openinter.net. Available at http://www.theopeninter.net/

[20]Roberts, D. 'Appeals Court Rules Against FCC

[21] Padovani, C. 'WSIS and Multi-Stakeholderism', in *The World Summit on the Information Society: Moving from the Past into the Future,* edited by Kleinwächter, W & Stauffacher, D (New York, The United Nations Information and Communication Technologies Task Force, 2005) p. 147

[22] Wilhelm, A. Interview with Imgur creator. *The Alan Schaaf Interview - What is Image Host Imgur, And How Didi it Get Started?* (online) 10 February 2010.
Available at http://thenextweb.com/us/2010/02/10/alan-schaaf-interview-image-host-imgur-started/#!sitd3

outside governance for these sites. Many other sites use similar systems to rank content. Wikipedia and other Wikis use a system of user generated content and collaboration.[23] Likewise relevant to self-governance is the manner in which the Internet community has rallied around contentious freedom of speech subjects and house bills like SOPA and PIPA, or used social networking to bring around governmental change. In these scenarios large bodies of citizens can bring around revisions under the assistance, but not control, of larger organisations. It would appear that a similar, ground up rather than top down governance would facilitate global Internet Freedom far more effectively. Clearly this would require a complete change to the governance of the Internet, or deference to consumers by large companies. Neither of these systems seem particularly realistic options and as such perhaps do not represent satisfactory substitutes to the current system, however they are representative of the possibilities of an alternative. Clay Shirky offers a very cogent argument in a 2012 TED talk, whereby he postulates that open source programming could revolutionize the notion of government through widespread public collaboration.[24] Perhaps a similar system could be applied to Internet Governance which would have the corollary of advancing a global form of Internet Freedom, if indeed that is what the collaborators chose to accept. The Internet is still a relatively young technology and has undergone numerous changes and revisions in governance, technological aspects, content and use to warrant optimism over positive changes however unlikely they seem.

Conclusions

As has been argued, the multi-stakeholder approach to Internet governance does little to actively promote unfettered and free access to the Internet. The sheer number of interested regulatory parties and the divergence of views, laws, governments and norms do little to facilitate, and much to impede the global spread of Internet Freedom. The recent slew of highly contentious rulings and discoveries emanating from some of the biggest proponents of Internet Freedom is likewise exceptionally damaging to the promotion and furtherance of freedom as supposedly protected under HRC 2012. The sheer financial, and influential power held by some of the leviathan companies and parties currently involved in trying to bring around change in the governance and supply of the Internet shall prove to be a real issue of freedom in the coming months and years. While some of the recent initiatives such as SOPA and PIPA were quashed, it remains to be seen if the current onslaught on net neutrality will attract enough defensive support to reverse the rulings. If not this could pose to be a critical blow for Internet Freedom. This writing has

[23] Viégas, B et al. 'Talk before youType: Coordination in Wikipedia', *Proceedings of the 40th Hawaii International Conference on System Sciences* 2007. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4076527; Wikipedia information entry. *Wikipedia.* Available at http://en.wikipedia.org/wiki/Wikipedia

[24]Shirky, C. 'How the Internet Will (One Day) Transform Government', *TED* September 2012. Available at: http://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government.html

merely touched the surface of the issues at hand. The implications of Internet Freedom and its assistance or impediment has a knock on effect for International Relations as a whole. The battles currently being fought in the US, the centre of Internet governance, will undoubtedly impact and set precedents around the rest of the world for Internet Freedom. This will open international discourses as the Internet is now an inescapable part of life that effects International commerce, discourse and relations and any US ruling will be carefully watched by the rest of the International Community.

Bibliography

Allagui, I & Kuebler, J. 'The Arab Spring and the Role of ICTs', *International Journal of Communication*, 5 (2011) pp. 1435-1442
Available at: http://www.arifyildirim.com/ilt508/ilhem.allagui.pdf

Ball, J. 'Revealed: How US and UK spy Agencies Defeat Internet Privacy and Security', *The Guardian* (online) 6 September 2013
Available at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Carr, M. 'Internet Freedom, Human Rights and Power', *Australian Journal of International Affairs*, 67:5 (2013) pp. 621-637

Ciarlo, M. A Guide to the Open Internet. *theopeninter.net.*
Available at: http://www.theopeninter.net/

Clinton, H. 'Remarks on Internet Freedom' *Washington.* 21 January 2010
Available at:
http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

Clinton, H. 'Internet Rights and Wrongs: Choices and Challenges in a Networked World'
Available at: http://blogs.state.gov/stories/2011/02/15/internet-rights-and-wrongs-choices-and-challenges-networked-world

Electronic Frontier Foundation, *Free speech information.*
Available at: https://www.eff.org/issues/free-speech

Farwell, J.& Rohozinski, R. 'Stuxnet and the Future of Cyber War', *Survival: Global Politics and Strategy,* 53:1 (2011)

Freedom House, *China Internet Freedom Report*. (2013)
Available at: http://freedomhouse.org/report/freedom-net/2013/china#.UtbPvWRdVH0

Freedom House, *Cuba Internet Freedom Report*. (2013)
Available at: http://freedomhouse.org/report/freedom-net/2013/cuba#.UtbQA2RdVH0

Fung, B. 'Federal Appeals Court Strikes Down Net Neutrality Rules'. *Washington Post* (online) 14 January 2014.
Available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/14/d-c-circuit-court-strikes-down-net-neutrality-rules/

Greenwald, G. & MacAskill, E. 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian* (online) 7 June 2013.

Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Guillemin, G. *Case Law, Strasbourg: Delfi AS v Estonia: Court Strikes Serious Blow to Free Speech Online.* Inforrm Blog (online) 15 October 2013.
Available at: http://inforrm.wordpress.com/2013/10/15/case-law-strasbourg-delfi-as-v-estonia-court-strikes-serious-blow-to-free-speech-online-gabrielle-guillemin/

Intel, *Moore's Law explanation.*
Available at: http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html

Internet's dark day: Anti-piracy bills take a beating. *The Seattle Times* (online) 18 January 2012.
Available at:
http://seattletimes.com/html/nationworld/2017274222_sopa19.html

internet.org, *Introductory Video.*
Available at: http://www.internet.org

Kirkpatrick, D. 'Anger Over a Film Fuels Anti-American Attacks in Libya and Egypt'. *The New York Times* (online) 11 September 2012.
Available at: http://www.nytimes.com/2012/09/12/world/middleeast/anger-over-film-fuels-anti-american-attacks-in-libya-and-egypt.html?_r=0

Langner, R. 'Stuxnet: Dissecting a Cyber Warfare Weapon', *Security and Privacy, IEEE,* 9:3 (2011) pp. 49-51

MacAskill, E et al. 'Mastering the Internet: How GCHQ Set Out to Spy on the World Wide Web', *The Guardian* (online) 21 June 2013
Available at: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

Padovani, C. 'WSIS and Multi-Stakeholderism', in *The World Summit on the Information Society: Moving from the Past into the Future,* edited by Kleinwächter, W & Stauffacher, D_(New York, The United Nations Information and Communication Technologies Task Force, 2005)

Reynolds, M. 'CISA security bill passes Senate with privacy flaws unfixed', *Wired* (online) 27 October 2015-12-23
Available at: http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/

Roberts, D. 'Appeals Court Rules Against FCC's Right to Protect Net Neutrality. *The Guardian* (online) 14 January 2014.

Available at: http://www.theguardian.com/technology/2014/jan/14/net-neutrality-internet-fcc-verizon-court

Schellekens, M. ‘Liability of Internet Intermediaries: A slippery Slope?’, *SCRIPTed,* 8:2 (2011) pp. 154-174
Available at:http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/schellekens.asp

Shirky, C. ‘How the Internet Will (One Day) Transform Government’, *TED.* (2012). Available at:
http://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government.html

Stepanova, E. ‘The Role of Information Communication Technologies in the “ArabSpring”: Implications Beyond the Region’. *PONARS Eurasia Policy Memo No. 159* (2011) pp. 1-6.

Thielman, S. ‘Senate passes controversial cybersecurity bill Cisa 74 to 21’, *The Guardian* (online) 27 October 2015
Available at: http://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote

United Nations General Assembly, Human Rights Council. ‘The promotion and enjoyment of human rights on the Internet’. 29th June 2012. Resolution A/HRC/20/L.13.
Available at : http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280

Universal Declaration of Human rights.
Available at :http://www.un.org/en/documents/udhr/

Viégas, B et al. ‘Talk before you type: Coordination in Wikipedia’, *Proceedings of the 40th Hawaii International Conference on System Sciences* (2007).
Available at:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4076527

Webber, M. ‘PRISM - What You Need to Know About the People Who Know Everything About You’, *Tech Help Made Easy* (online) 5 July 2013
Available at:
http://www.techhelpmadeeasy.com/what-is-prism/

Wikipedia, *Wikipedia information entry,*
Available at: http://en.wikipedia.org/wiki/Wikipedia

Wilhelm, A. Interview with Imgur creator. *The Alan Schaaf Interview - What is Image Host Imgur, And How Didi it Get Started?* (online) 10 February 2010.
Available at: http://thenextweb.com/us/2010/02/10/alan-schaaf-interview-image-host-imgur-started/#!sitd3

10001011010101000010110101010010101
01010111001010101010101010010101010
11001011110000000000010101011101010
10100111110101010010010101010100000
10101010101010010101011100101010101
00110101101010101100101001010100101
0000000000111111000**SPECIAL**01**EDITION**