CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

MARCH 18 - 19, 2012 | TORONTO, CANADA

"Do you see over yonder, friend Sancho, thirty or forty hulking giants?
I intend to do battle with them and slay them."

Miguel de Cervantes Saavedra, Don Quixote

CYBER DIALOGUE 2012 BRIEFS: THINKING STRATEGICALLY ABOUT CYBER SECURITY

The increasing technological sophistication of black hat hackers and organized criminal groups has rendered the use of cyberspace a business risk for many corporations and banks. More recently however, cyberspace has become a tool for projecting national power, procuring profit and promoting instability and disruption, hence catapulting the risk far beyond business and into the political and strategic realms. Indeed, the fact that states are now potentially both protagonists and principal targets of cyber attacks heightens the political risks involved, to the point that securing the domain through both offensive and defensive measures has become a strategic priority for most major powers.

Since the 1970s, Information Communications Technologies (ICTs) have gradually become a central part of military doctrine and operations.[1] The Internet, in particular, has served as a strategic communications platform for opposing parties in conflict, a tool for organization, mobilization and recruitment, even conflict resolution.[2] It enables transnational cybercrime, which has far out-paced the financial losses engendered by more traditional forms of crime, and is a growing vector for economic and

1 Revolution in Military Affairs (RMA) – attention to the doctrine waned significantly following developments in Iraq after the initial invasion and following the Israeli Defense Force (IDF) debacle against Hezbollah in southern Lebanon in 2006.

2 Karatzogianni (2009).

industrial espionage. The perceived ease with which state or non-state actors can, via an individual, a group or the mass conscription of computers, disable data centres, clear bank accounts, or damage electricity grids or other critical infrastructure is a major global concern. The easy access to tools for perpetrating electronic attacks and electronic warfare tactics, and the sophisticated webs of anonymity and deceit underpinning them does little to assuage these concerns. Meanwhile, concerned that "the very technologies that empower us to lead and create also empower those who would disrupt and destroy," civilian powers are establishing boundaries to define what belongs to whom and who is allowed to wander where in cyberspace.[3] And having identified the Internet as a strategic communications tool, military and intelligence agencies are also staking their claim in cyberspace.[4]

Cyber tactics have been a central part of intra- and inter-state conflicts since the early nineties, including Sri Lanka, Israel-Palestine, India-Pakistan, Estonia and Russia-Georgia.[5] Economic, environmental and system damage created by the generic ILOVEYOU bug and the targeted SCADA system attack in 2000, and the 'Aurora' vulnerability probe in 2006 were constant reminders of the potential threats and vulnerabilities that an open and free cyberspace can pose.[6] On the basis of these incidents, strong claims have been made that cyberwar is "real" and capable of "devastating modern nations."[7] Estonian Defence Minister Jaak Aaviksoo argued that the [cyber] attacks "(…) [could] effectively be compared to when your ports are shut to the sea" (i.e. a naval blockade, an act of war). The Estonian Speaker of Parliament Ene Ergma likened cyber warfare to nuclear radiation:

> "When I look at a nuclear explosion and the explosion that happened in our country in May,

3 "Securing Our Nation's Cyber Infrastructure", speech by U.S. President Barack Obama, May 29, 2009.

4 Glenny (2010).

5 Carr provides an overview of cyber attacks over the decade spanning 2000-2010. Carr (2011)

6 The ILOVEYOU bug spread to some 45 million Windows PCs including classified systems in the U.K. and the U.S. Estimated worldwide damages exceeded $10 million. In Australia the remote takeover of a SCADA system by a disgruntled job applicant allowed him to take charge of 150 sewage pumps and spill more than a million litres of raw sewage into local parks, rivers and hotel grounds over a three-month period. The Idaho 'Aurora' vulnerability probe in 2006 exposed some North American power stations to electronic attack. The test target was a $1 million, 27-ton industrial diesel generator and the goal was to disable the machine in a controlled environment through an Internet-based attack. The lab allegedly developed "twenty-one lines of code that caused the generator to blow up." Rid and McBurnett (2012), p.5.

7 Betz and Stevens (2011)

> I see the same thing. Like nuclear radiation, cyber warfare doesn't make you bleed, but it can destroy everything."[8]

On closer examination however, evidence to support these claims is weak. Governments are correspondingly cautious when responding to allegations of state responsibility, even when there are strong indications of state involvement in the attacks.[9] For example, NATO chose to send experts to learn from the Estonia experience, rather than directly addressing the allegations made by the Estonian government regarding Russia's involvement or challenging Russia's denials.[10] Some observers have also noted that the current 'hype' around security in cyberspace presents 'a classic opportunity for threat inflation' such as that which emerged during the Cold War.[11] In March 2010, former cybersecurity czar Howard Schmidt noted that 'there is no cyber war", that it is a 'terrible metaphor" and a "terrible concept."[12] At the same time however, while information elements of contemporary warfare might not have been very evident in some of the recent conflicts mentioned above, some argue that "cyberspace did play a significant, if not decisive role in the [Georgia-Russia] conflict: as an object of contestation and as a vector for generating strategic effects and outcomes."[13] The same authors also raise important questions regarding the actions of civilians in cyberspace during conflict, noting that unlike voluntary civilian participation in the wars of the past, the "unpredictable nature of such outside participation [today] – global in scope, random in nature, can lead to chaotic outcomes, much like the trajectory and phase of a cyclone."[14]

The daunting prospect of the unknown coupled with an assumed effectiveness of cyber-espionage has led states to place cyberspace at the forefront of their national security agendas, both to secure the Internet (in terms of resources and institutional

8 Betz and Stevens (2011)

9 *Ibid*

10 Karatzogianni, (2009).

11 Morozov (2010),

12 http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

13 Deibert, Rohozinski and Crete-Nishihata (2012). According to the authors, "operations *in* and *through* cyberspace were present throughout the conflict and were leveraged by civilian and military actors on both sides. Russian and Georgian forces made use of information operations alongside their conventional military capabilities. Civilian leadership on both sides clearly appreciated the importance of strategic communication, and targeted domestic and international media in order to narrate the intent and desired outcome of the conflict."

14 *Ibid*

architecture), and legitimize the use of Internet capacities as a weapon in cyber 'warfare.'[15] Strategically, some countries have elevated cyberspace to a war-fighting domain along with land, air, sea and space, while terms such as cyber warfare and cyber weapons are increasingly heard in policy circles and the media, particularly since the Stuxnet worm was unleashed on Iranian nuclear centrifuges in 2011.[16] In June 2009, following designation of cyberspace as the "fifth domain," U.S. President Obama created the position of a cybersecurity czar, responsible for all federal issues pertaining to cyberspace. While various organizations, divisions and agencies already addressed the U.S. DoD's cyber security needs at the policy and operational levels. The U.S. Secretary of Defense formally recommended to the President that the United States establish the USCYBERCOM under US Strategic Command.[17] At the same time, a Joint Information Operations Warfare Center was created "to plan, integrate, and synchronize information operations in direct support of Joint Force Commanders and to serve as the USSTRATCOM lead for enhancing IO across the DoD."[18]

In March 2010, the U.S. Quadrennial Defence Review placed cyber security as one of the Pentagon's pivotal focus areas. More recently, the State Department released the U.S. International Strategy for Cyberspace, followed closely by the Pentagon's launch of the U.S. Cyber Defense Strategy, which emphasizes cyber weapon capabilities and active cyber defense. Assessments of the reach and effects of cyber-espionage, particularly by countries such as China, have been central components of these strategies. By the end of 2011, Australia, Brazil, Canada, the Czech Republic, the Democratic People's Republic of Korea, France, Germany, India, Iran, Israel, Italy, Kenya, Myanmar, Pakistan, the People's Republic of China, Poland, the Republic of Korea, the Russian Federation, Singapore, South Africa, Sweden, Taiwan, Turkey and the United Kingdom had or were planning to establish some form of formal cyber operations capability.[19] The EU and NATO have also developed cyber warfare capabilities.[20] Many

15 Meyer (2012)

16 The Stuxnet worm was unique in the high amount of intelligence it was programmed with, allowing it to infect tens of thousands of computers to increase the chances of reaching the targeted system (the Iranian nuclear centrifuges in Natanz), without creating collateral damage.

17 Carr (2011), *Inside Cyber Warfare: Mapping the Cyber Underworld*

18 For a more detailed idea of how complex the U.S. cyber security architecture is see: http://iac.dtic.mil/iatac/download/ia_policychart.pdf

19 Carr (2011)

20 *Ibid*

of these states have followed the lead of the U.S; others, especially China and Russia, have been developing information warfare doctrine and capabilities for decades, and view information security and governance as crucial to protecting and advancing their national interests.

In spite of the adverse economic climate, states are making enormous investments in advanced cyber capabilities to protect when possible, and use as an instrument of power when necessary. In 2010, a consulting firm issued a report estimating that the U.S. government's total spending on cyber security between 2013 and 2018 will reach $65 billion. This figure did not include either the funds that certain agencies are already spending on R&D on cyber capabilities and deterrence measures, or the amount private companies are investing.[21] Some have estimated that Western governments currently spend an annual $100 billion on telecommunications and cyber security, a figure set to double in the next six years.[22]

Nonetheless, despite a marked increase in the attention and resources allocated to cyber security and warfare, there is still no international agreement on what constitutes an "armed cyber attack" (in the wartime sense). Analysts are still struggling with how the concepts of offence, defense, deterrence, escalation, and arms control apply to the cyber domain.[23] Major powers such as the U.S., China and Russia continue to disagree about whether a new treaty for cyberwarfare is required. Those who insist that the core principles underpinning the UN Charter and the laws of armed conflict, including *jus ad bellum* and *jus in bello*, can be applied to conflict in the cyber domain have yet to clarify how these principles should apply to cyber 'weapons', particularly how they relate to territorially defined state actors.[24] In addition, it is unclear whether the concepts "use of force," "armed attack," "act of aggression," and "retaliation" can be applied to an alleged cyber attack, how attribution can be established, and whether cyber attacks should be judged by both the direct and indirect effects generated by both military *and* non-military actors, or just the means of an attack.[25] In short,

21 Market Research Media (2010)

22 Glenny (2012), quoting the findings of research by the London-based consultants Visiongain. http://www.nytimes.com/2012/03/09/opinion/tap-into-the-gifted-young-hackers.html?_r=2&src=tp

23 Nye (2011)

24 Bajaj (2010).

25 Hughes, (2010, 2009); Bajaj (2010); Deibert, Rohozinski and Crete-Nishihata (2012).

cyber-warfare remains highly problematic, not least because a classical act of war should be instrumental, political and potentially lethal. Since no cyber-related incident has yet met these criteria, current posturing can be easily critiqued as tilting at cyber windmills.[26]

Much of the underlying confusion grows out of different cultural norms and contradicting definitions of cyberspace that may, eventually be reconciled. Indeed, as noted by Betz and Stevens, defining cyberspace has important implications for the operations of power, "as it determines the purview of cyberspace strategies and the operations of cyber-power."[27] It "relates to what and whom we consider to be actors in cyberspace" and how different actors use cyberspace to pursue their own ends.[28] Similarly, traditional war strategies may not be applicable if the basic premise about the nature of that war is mistaken. In this regard, elevating activities such as espionage, crime, hacking and breaches of intellectual property to a state "which society has traditionally regarded as legally, morally and strategically exceptional," corresponds more to a strategic context of inter-state war and peace, rather than the current reality of more generalized confrontation and conflicts.[29] It may well be that the need for cooperation against threats posed by non-state actors prods states to move beyond the current zero-sum games surrounding security in cyberspace.[30] Finally, as noted by Deibert *et al*, consideration of some of the international legal and policy implications of actual cases that are being referred to as acts of war could help fill some of the major knowledge gaps that currently exist in the study of international relations and strategic affairs.[31]

In the meantime, continuing conceptual confusion coupled with on-going competition to project power and secure positions in cyberspace will likely exacerbate existing tensions between states.[32] Current dynamics are aligning in a manner that suggests

26 Rid and McBurney (2012)

27 Betz and Stevens (2011)

28 Betz, Stevens (Ch.1) See references to inclusive and exclusive models of cyberspace

29 *Ibid*

30 Nye (2010)

31 Deibert, Rohozinski and Crete-Nishihata (2012)

32 For more detail on these tensions see the corresponding Cyber Dialogue 2012 brief on "Wither the Rules of the Road for Cyberspace."

the emergence of a cyber arms race: offense is dominant, deterrence is difficult to signal due to the challenges of attribution, barriers to entry are low and the pressures to react quickly are mounting.[33] China and Russia will continue to call for 'cyber arms control' and international treaties to curb what they perceive an aggressive U.S.-led militarization of cyber space on the part of the U.S. and its allies.[34] Failure to make progress on a global set of norms for governance and behaviour in cyberspace will not help alleviate these tensions.

Much emphasis is being placed on military strategy, the refinement, enhancement and development of military cyber capabilities, and the central role of the military in securing cyberspace. Would it be more productive to discuss cyber weapons before moving to define cyber warfare or the applicability of the current laws of war? For example, Rid and McBurney note that there is no international consensus regarding the definition of a 'cyber-weapon' (nor is there consensus within the U.S. DoD). They propose that a cyber weapon is a subset of weapons; more generally, as computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings. They also note that a psychological dimension is a crucial element in the use of any weapon, but especially so in the case of a cyber-weapon. A first psychological dimension is the offender's intention to threaten harm or cause harm to a target (including questions of dual use); a second psychological dimension comes into play "if a weapon is used as a threat, or if its use is announced or anticipated: the target's perception of the potential of the weapon to actually cause harm."[35] They also suggest that cyber-weapons can be grouped along a spectrum: from the generic, low-end of the spectrum of malware (DoS and DDoS attacks as in the Estonia 2007 case) to the high-potential end of malware (as in Israel's 2007 attack on Syria's air defense system or the 2010 Stuxnet worm attack on Iranian centrifuges in Natanz). The former is "able to influence a system from the outside but technically incapable of penetrating that system and creating harm", while the latter "is capable of penetrating even protected and physically isolated systems and *autonomously* influencing output processes in order to inflict direct harm."[36]

33 Deibert and Rohozinski (2011)

34 See the Code of Conduct proposed by the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan in Oct. 2011 (A/66/359) http://rusemb.org.uk/policycontact/52

35 Rid and McBurney (2012)

36 *Ibid*

How might we use clarification on cyber weapons to move towards an acceptable definition of cyber warfare in the current strategic context? Where does the role of civilians (especially regarding their capacity to generate informational effects in and through cyberspace) figure in these definitions?

Is the current emphasis on military strategy, capabilities and weapons misplaced? How might it undermine other important aspects of grand strategy - political, diplomatic, informational, economic as well as military - in relation to cyberspace and those who act in and through cyberspace? What are the targets of cyberpower?[37] Can common understandings on vulnerabilities serve as the basis for confidence- building measures for reaching agreement on acceptable cyberspace norms? How can states cooperate to protect (soft and hard) targets of mutual interest from the forms of power exercised by non-state actors? Where might points of agreement on stewardship and governance of cyberspace emerge? Does the military have a stake in promoting good cyber stewardship? And finally, what tensions emerge between the drive to protect and project national interests on the one hand, and domestic policymaking around cyber security on the other?

Prepared by Camino Kavanagh with the support of Matthew Carrieri

---

Camino Kavanagh is currently pursuing a PhD at Kings College London's Dept. of War Studies and is a non-resident fellow at University of Toronto's Canada Centre for Global Security Studies and the Citizen Lab. Her principal research focus is on power dynamics in (and in relation to) cyberspace. Camino is also a Fellow at NYU's Center on International Cooperation (CIC) where she focuses principally on transnational threats such as organized crime and trafficking. She has an MA in Contemporary Warfare and an MA in International Human Rights Law

Matthew Carrieri is currently finishing his MA in Near Eastern Studies with business focus at NYU; and has a BA in Middle East Studies from McGill

37 See Nye (2010) for an overview of soft and hard targets in cyberspace.

BIBLIOGRAPHY

Bajaj, Kamlesh. *The Cybersecurity Agenda: Mobilizing for International Action*. East-West Institute, 17 June 2010. Web. http://www.ewi.info/cybersecurity-agenda.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*.

Abingdon, UK: Routledge, for the International Institute for Strategic Studies, 2011.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media (2011).

Deibert, Ronald J, Rafal Rohozinski, and Masashi Crete-Nishishita. "Cyclones in cyberspace: Information sharing and denial in the 2008 Russia-Georgia war." *Security Dialogue*, 43:1 (2012).

Deibert, Ronald J, Rafal Rohozinski. "The new cyber military industrial-complex." *Globe and Mail*, 28 March. Available at: http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/

Glenny, Misha. "Tap Into the Gifted Young Hackers." *The New York Times*. 8 March 2012. Web. http://www.nytimes.com/2012/03/09/opinion/tap-into-the-gifted-young-hackers.html?_r=2&src=tp.

---. "Who Controls the Internet?" *The Financial Times*. 8 October 2010. Web. http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html.

Karatzogianni, Athina. *Cyber-Conflict and Global Politics*. New York, NY: Routledge, 2009.

Market Research Media. *U.S. Federal Cybersecurity Market Forecast* 2013-2018. Feb. 2012.

Market Research Media. http://www.marketresearchmedia.com/2009/05/25/us-federal-cybersecurity-market-forecast-2010-201

Meyer, Paul. "Cyber-Security Through Arms Control: An Approach to International Cooperation." *The RUSI Journal*, 156:2 (April/May 2011).

---. "Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda." *The RUSI Journal*, 157:1 (February/March 2012).

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: PublicAffairs, 2011.

Nye, Joseph S. *Cyber Power*. Rep. Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Web. http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html.

---. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5:4 (Winter 2011.

Rid, Thomas and Peter McBurney. "Cyber-Weapons." *The RUSI Journal*, 157.1 (February/March 2012).

Russia. Ministry of Foreign Affairs. *Concept of a Convention on International Information Security*. The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 28 October 2011. Web. http://rusemb.org.uk/policycontact/52.

Singel, Ryan. "White House Cyber Czar: 'There is No Cyberwar'." *Wired*. 4 March 2010. Web. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/.

U.N. General Assembly, 66th Session. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. (A/66/359). 14 September 2011. Web. http://daccess-ddsny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

United States. Department of Defense. Information Assurance Technology Analysis Center. *The DoD IA Policy Chart*. 20 June 2011. Web. http://iac.dtic.mil/iatac/ia_policychart.html.