CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

MARCH 18 - 19, 2012 | TORONTO, CANADA

CYBER DIALOGUE 2012 BRIEFS: THE WHO'S WHO OF POLICING IN CYBERSPACE

The past decade has witnessed a gradual shift in the way individuals and groups operate in cyberspace. Only in select, mainly autocratic countries, did the government or government proxies intervene to "police" the behavior of Internet users. In the West, the policing of cyberspace was initially the domain of engineers, forum moderators, and Internet "founding father" stewards such as Vint Cerf, Jon Postel and Steve Crocker. Their interests were mainly technical in nature: identifying software bugs, testing technological innovations, and promoting standards or goods. Informal mechanisms to develop standards and practices through the mechanisms of Request for Comments (RFCs) were first introduced in 1969 as part of the ARPANET project, evolving into the official publication channel for the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), and more generally, the global community of network researchers.[1]

However, as information communications technologies (ICTs) came to represent more consequential vectors for determining political and social outcomes, so too did the interest afforded as to how these should be policed and by whom. In the early days, this interest was generally relegated to law enforcement officials trying to track down 'teenage hackers' who sharpened their skills by hacking into government servers; or more seasoned politically motivated "hacktivists" who inhabited the cyber underground. The overall political, economic, and social costs of these activities were relatively low, as reflected in the corresponding levels of investment in policy and operational responses.

Today, however, policing of cyberspace has taken on a whole new meaning, not least because cyber incidents are now considered by many governments as national security threats. Those who have taken up or broadened cyber-related policing functions

1 http://en.wikipedia.org/wiki/Request_for_Comments

either formally or informally include law enforcement officers, special agents, the military, private enterprise (particularly Internet service providers (ISPs), social networking services and risk management companies), "hacktivists," organized criminal groups and even private individuals. But who is mandated to police cyberspace, and how are they approaching it?

LAW ENFORCEMENT

Increasing levels of cyber crime, economic and industrial espionage, organized crime, and terrorist activity are pushing more countries to develop cyber-policing capabilities. Law enforcement bodies such as the Federal Bureau of Investigation (FBI), the Serious and Organized Crime Agency (SOCA) and the Police Central e-crime Unit in the UK, Chile's Brigada Investigadora del Cibercrimen (BRICIB), and Mexico's Policia Cibernetica have fully embraced technology for investigative purposes, investing heavily in developing capacity and capabilities to police cyberspace.[2]

In the U.S., the FBI has established cyber-squads in all of its field stations. It has 1,000 specially trained agents, cyber analysts and forensics experts within its ranks. It has also deployed 63 legal attachés across the globe and embedded special agents in police departments in Romania, Estonia, Ukraine and the Netherlands to deal with cyber incidents, share information and help coordinate investigations into cyber incidents.[3] At home, it works closely with the Department of Homeland Security (DHS), the Central Intelligence Agency (CIA), and the National Security Agency (NSA) on existing and emerging cyber threats. The FBI is a core member of the National Cyber Investigative Joint Task Force, which brings together eighteen U.S. law enforcement, military and intelligence agencies to prevent current and predict future cyber attacks. It views partnerships with the private sector as key to the success of its operations.

Botnets are a particular target of cyberspace focused policing efforts as they pose a significant threat to end users, businesses and, increasingly, governments.[4] The FBI has made many tactical gains responding to the complex use of botnets by cyber

2 RSA 2012 presentation

3 *Ibid*

4 Eneken Tikk-Ringas, (forthcoming 2012), *Botnet Control & Command Takedown: Legal Considerations and the Role of ISPs*

criminals. For example, last April, the FBI managed to dismantle the Coreflood botnet which had affected an estimated two million users, one quarter in the United States. Coreflood had enabled hackers to seize control of zombie computers and steal personal and financial information. Acting on a request by the FBI, the Justice Department sought and won permission from a federal judge to work via a non-governmental organization - Internet Systems Consortium - to seize control of the botnet and deliver a command to the zombie computers to disable the malicious software.[5] This takedown was allegedly the first case in the United States in which authorities swapped out criminal servers for government servers to intercept communications between infected systems and the servers controlling them.[6]

The case established legal precedent but raised many questions, with some observers suggesting that the U.S. government's proactive move holds risk, not least because of data retention issues and uncertainty surrounding the impact of sending commands to infected machines.[7] Dutch law enforcement used a similar approach to successfully disable the Bredolab botnet, which had apparently infected some 30 million computers worldwide.[8] Other law enforcement agencies, principally in Europe and North America, have worked with private companies and ISPs to take down botnets; while IT companies such as Microsoft, ISPs and researchers working together or in isolation, have produced successful takedowns.[9] Collaboration in some of these areas is also emerging at the international level, for example, through the INTERPOL-ICANN partnership for international security. Yet the initiative is limited since neither of these organizations has an operational mandate.[10]

Law enforcement agencies have invested considerable time and money to bring down criminal networks on the web and are achieving some success at the tactical level. Nonetheless, cybercrime losses continue to climb due to a variety of economic and technological factors that advantage cyber criminals. First, many cybercriminals are

5 U.S. District Court of Connecticut, Case 3:11-cv-00561-VLB Document 32, Filed 04/13/11; Wired, Zetter (2011)

6 *Wired*, Zetter (2011)

7 *Wired*, quoting Chris Palmer, technology Director at the Electronic Frontier Foundation, in With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal, Zetter (2011)

8 U.S. District Court of Connecticut, Case 3:11-cv-00561-VLB Document 32. Filed 04/13/11

9 Tikk-Ringas (forthcoming 2012). See also Hathaway (2011) for detailed analysis of US-led multi-sector takedowns of botnets including MS-ISAC vs. QAKBOT,; Microsoft vs. Rustock Botnet and NCFTA vs. Pump and Dump Scam

10 Hathaway (2011)

motivated by the increasing economic value of Internet transactions.[11] Second, cybercriminals have generally proven more adept at leveraging technological innovation.[12] In most instances, "cybercops" are simply outgunned both technologically and organizationally in matching today's cyber criminals. The growing cybercriminal law enforcement gap raises alarm bells when considering the degree of institutional adaptation required to effectively respond to the growth in cybercrime. The challenge is even greater for less wealthy nations or fragile states, where law enforcement capacity is weak, and other pressing priorities take precedence over meeting the high costs of addressing system vulnerabilities. In addition, the number of cyber-related activities deemed criminal seems to be increasing, placing additional pressures on law enforcement agencies while simultaneously suggesting a major push to "securitize" the Internet.

Legitimate law enforcement bodies are required to operate within the law to conduct investigative and operational work in cyberspace. Lack of international agreement on the normative basis to do so is problematic, not least because of the disparities that exist between different cultural and legal interpretations of what is considered "illegal" in different jurisdictions. One group of countries is using the Council of Europe Cybercrime Convention as a guiding tool for the adoption of national legislation and sees transnational international law enforcement cooperation as the key to countering cybercrime. The Convention emphasizes respect for core human rights principles. Other states, opposed to broadening the Convention into an international treaty, are less likely to place rights and freedoms and transnational international law enforcement cooperation at the center of efforts to counter cybercrime and related offenses. At the same time, as the "cyber threat" continues to grow, the gap between countries which have traditionally respected privacy rights and Internet freedoms and those that do not continues to narrow, representing a significant contradiction in current state narratives.

In order to maneuver around current restrictions, states on both sides of the fence are increasingly referring to the principles of necessity and proportionality to legitimize breaches of privacy, including *ex-ante* operations such as filtering web content and

11 Rush, Smith, Kraemer-Mbula, and Tang (2009)

12 Hathaway (2011); http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf; Entrust, http://www.entrust.com/bill-conner-congressman-burgess/index.htm

monitoring social media or the broader use of surveillance and censorship tools.[13] States are also relying on privatized enforcement to evade restraints on the exercise of legal power over the Internet.[14] Other recent trends include the creeping criminalization of a range of online activities such as file sharing, peer-to-peer communications, and the use of copyrighted works.[15] The result of these combined actions is a narrowing of privacy rights and an increase in the range of official policing in cyberspace.

THE PRIVATE SECTOR

The private sector is playing an important role in defining, policing, and responding to cyber threats and vulnerabilities.[16] At the strategic level, private risk analysis companies are advocating for an increased role in the policing of cyberspace, particularly through the currently fashionable notions of dynamic or active defense. The concept is aimed at helping companies and organizations create a system of layered defence and rapid response capabilities aimed at minimizing overall risk vis-à-vis cyber attacks. Response mechanisms include "uncovering and rooting out attackers through forensics analysis," and would be carried out by the company or organization.[17] At the tactical level, certain IT companies, such as Microsoft continue to work with law enforcement, researchers and ISPs to track and take down botnets. Others, including ISPs and social networking services have worked with law enforcement agencies to understand and respond to criminal syndicates' or terrorist use of ICTs in advancing their goals. While many of these public-private partnerships are viewed as positive, they are coming under increasing scrutiny as cyber-related incidents move up the threat scale and onto the strategic agenda, while privacy and other freedoms are moved, if not shoved, down the rights scale and off the strategic agenda.

The West has traditionally criticized autocratic governments for Internet filtering,

13 A/HRC/17/27,

14 Tulloch (2010)

15 Bills such as the Stop Piracy Online Act (SOPA) in the U.S. was severely critiqued for potentially opening up government loopholes for policing the Internet and restricting citizens' rights and freedoms.

16 In 2011, it was estimated that the growing market for cyber security services generates $40-$60 billion annually in the U.S. alone. Deibert and Rohozinski (2011)

17 The underlying tenets of dynamic/ active defense figure as a central axis of the U.S. DoD's 2011 Cyber Defense Strategy.

monitoring and controlling cyber cafes, deploying cyber police or cyber armies to monitor civilians, removing Internet sites or posting "favorable content". Recently a spotlight has been placed on the degree to which private companies in the West have provided autocratic governments with many of the capabilities and skills to operationalize such efforts. These companies also openly promote products for surveillance to governments and police agencies in democratic countries. For example, Italian-based Innova offers "solutions for the interception of any kind of protocols and IP-based communication, such as web browsing, email and web-mails, social networks, peer–to-peer communication, chat and video-chat" while Endace Accellerated, a New Zealand-based company, promotes the "power to see all for government" and the U.K.-based Gamma Group offer "turnkey lawful interception projects," including SMS interception, speech identifying tools, and data retention.[18]

In 2011, the UN Special Rapporteur on Freedom of Expression, Frank La Rue noted his deep concern about these techniques, principally because the lack of transparency surrounding the measures makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by states.[19] He also noted that the private sector must respect human rights and therefore should be required to act with due diligence to avoid infringing on the rights of individuals, whether in cyberspace or physical space.[20] Whether Western governments should ban the export of these technologies to repressive governments is a subject of much debate. Evident contradictions emerge around such measures, especially if the same Western governments are funding and promoting the dissemination of circumvention technologies to "hacktivists" and protesters in autocratic states.[21]

Notwithstanding, the onus to respect the rights of individuals does not lie solely with ISPs. Governments are increasingly seeking to exert control over ISPs and hold them legally liable for failing to prevent access to content deemed illegal.[22] Indeed, a number of legislative proposals would require ISPs to blacklist sites holding certain content, thus placing unwarranted policing responsibility on the shoulders of private actors.

18 See Privacy International's Big Brother Inc. project https://www.privacyinternational.org/big-brother-incorporated

19 A/HRC/17/27, Sect. A (1)

20 *Ibid*

21 Diamond (2011)

22 *Ibid*

For example, in 2011 a controversial cybercrime bill was tabled in Brazil.[23] If passed, ISPs and sites like YouTube and Flickr could become liable for unlawful content posted by their users. ISPs, email service providers, and other Internet intermediaries would be obligated to collect and retain users' personal data for extended periods of time.[24] Potentially more invasive is Bill C-30, tabled in Canada in 2011, which would require ISPs to acquire the ability to engage in multiple simultaneous interceptions and gives law enforcement the power to audit their surveillance capabilities. It would also give the government the power to install its own equipment directly onto private Internet provider networks.[25] In other countries, this is already occurring. The UK has introduced similar mechanisms, for example through the "voluntary" Cleanfeed system.[26]

Given the perceived scale of cyber-related threats in national security circles, it is difficult to discern how such initiatives might be made less intrusive on privacy rights. Conversely, in November 2011, in a historical ruling that clashed with the prevailing [EC] Executive view, the European Court of Justice decided "[EU] member states cannot impose the filtering of the Internet for the purpose of preventing illegal downloads of copyrighted files."[27] The ruling will have an impact on existing or proposed filtering technology measures in France, Italy, Ireland and the UK, and may serve as the basis to challenge judicial decisions across the region. Initiatives launched by companies such as Google to reveal the worldwide status of online impediments to freedom of expression may help shed light on the scope of the privacy problem.[28]

23 See PL 84/1999 - htwww.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028

24 http://advocacy.globalvoicesonline.org/2011/11/08/brazil-cybercrime-law-could-restrict-fundamental-rights-internet-openness/

25 See Bill C-30 opens Canada to Big Brother Inc. business: Geist. http://www.thestar.com/business/article/1136406--bill-c-30-opens-canada-to-big-brother-inc-business-geist

26 Cleanfeed is a trademark of the THUS company group and refers to privately administered ISP-level content filtering service operating in the U.K. and Canada. It is also the name of a proposed mandatory Australian ISP-level content filtering system currently undergoing testing (CHECK). The original intent of Cleanfeed was to block access to child abuse/pornography content located outside the country operating the filtering system. In the U.K. however, its use has now been extended to block websites that link to copy-righted material. It is critiqued for its censorship potential - some ISPs have apparently been threatened with legal compulsion if they don't implement the system - and lack of transparency regarding its use. Some have even likened the powers of censorship available through use of Cleanfeed to those currently employed by China. See: Peter Bright (2011), UK Cyber Strategy: Stuxnet, censorship and cyber-specials, Ars-Technica and Lillian Edwards (2006), From Child Porn to China, in one Cleanfeed, SCRIPT-ed, Vol.3 Issue 3, Sep. 2006. See also, See also: http://www.bbc.co.uk/news/technology-17270817

27 See Judgment in Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) at http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf

28 Edwards (2006)

THE MILITARY

In countries like China and Iran, militaries have established and deployed 'cyber armies' to police the on-line behaviour of citizens within and beyond their borders. Western militaries are also stretching policing boundaries in cyberspace. For example, in 2008 the U.S. military decided to dismantle a website that hosted an online forum established by the CIA and Saudi intelligence as a "honey pot" to glean intelligence and identify potential terrorist attacks. When the Pentagon determined that the site put American lives at risk, it took down the site, inadvertently causing significant disruption to more than 300 servers in Saudi Arabia, Germany and Texas. The decision to dismantle the forum strained relations between the CIA, Pentagon, and its Saudi counterparts. This bureaucratic bungle also shed light on important issues regarding cyber command and control, and confusion between what is considered policing and intelligence activity on the one hand, and wartime [Defence Department] authority and activity on the other.[29] It also raised complex questions about the use of cyberspace to gather intelligence or to disrupt 'the enemy' that remain unresolved.

More recently, the 2011 U.S. Department of Defense Cyber Defense Strategy emphasizes 'active cyber defense,' suggesting that the US will carry out offensive operations in cyberspace when vital national interests are threatened.[30] This expansion raises concerns about transparency and privacy; how classified military information might be shared with traditional law enforcement; and the degree to which such strategies are resulting in the 'militarization of cyberspace'.[31]

ILLICIT POLICING

Organized criminal groups also engage in forms of policing in cyberspace, using the Internet and mobile technology to conduct surveillance of and gather intelligence on those who may be intent on exposing their activities, and terrorize those who pose a threat to them. Organized criminal groups may also be used a proxy agents for state sponsored cyber mischief.

29 Nakashima (2010); Morozov (2010)

30 DoD Cyber Defense Strategy

31 RSA 2012

For example, in 1994, a Colombian counter-narcotics cell accidentally discovered a computer centre manned in shifts around the clock by 4-6 technicians. A front man for Cali cocaine cartel leader Santacruz Londoño owned the building. The facility boasted a $1.5 million IBM AS400 mainframe, the kind once used by banks. It was networked with half a dozen terminals and monitors. The Colombian Attorney-General allowed U.S. agents to fly the mainframe to the U.S. where it was analyzed by DEA experts and other intelligence agencies. The 'Santacruz computer' was never returned and the DEA's report was deemed highly classified. However, the computer allegedly held a database of residential and office phone numbers of U.S. diplomats and agents (both known and suspected U.S. law enforcement, intelligence, and military operatives) based in Colombia. In addition, the phone company was supplying the cartel with complete records of all telephone calls in the form of the originating and destination phone numbers. The cartel's intelligence arm then used custom-designed software to cross-reference the phone company records against their own list of suspected law enforcement, military, and intelligence officials or agents to produce a list of potential informants. Law enforcement officials never revealed the fate of the informants in the Santacruz computer. It is believed that suspected informants were either tortured to reveal information or killed outright.[32] More recent cases point to organized criminal groups using equally sophisticated measures to monitor authorities or negative on-line coverage of their activities.

CITIZEN POLICING

Private individuals are increasingly policing the Internet through the broad range of readily accessible tools on offer: whether uncovering technological flaws in emerging ICTs and software, recovering lost or stolen mobile phones and laptops, tracking unfaithful spouses, reporting on-line bullying or responding to government requests to support local or national cyber security efforts, citizens are engaged.

In many countries, governments are increasingly engaging private citizens to carry out quasi-policing functions. The "patriot army" of China and the "Electronic Army" of Iran are some of the more familiar examples whereby hired hacks also engage in activities ranging from basic surveillance and censorship to propaganda, cyber-attacks, cyber espionage and counter-espionage. In the West, governments are inviting

32 Paul Kaihla, The Technology Secrets of Cocaine Inc., *Business 2.0*, July 2002

citizens to join cyber militia such as the U.S. Infragard or UK Internet Safewatch (e.g., U.K. citizen-specialists, often cheekily referred to as i-Plods).[33]

In other settings where threats are much more tangible, citizens take up police functions themselves, using blogging sites or Twitter to fill the void left by weak and corrupt police forces or silenced or co-opted traditional media. The results can be very dangerous. In 2011 for example, several bloggers working out of Nuevo Laredo, Mexico, were violently killed by members of drug cartels who berated them *post-facto* for participating in online discussions about the drug situation in Mexico and for tipping off authorities about their activities. Mexican bloggers fear that the recent attacks will prevent people from using the Internet to circulate information on what is happening in different parts of the country.[34]

States are developing innovative measures to respond to cyber threats and have made reasonable progress in some areas, particularly cybercrime. At the same time, many worry that ICT innovations may actually refine instruments of violence and public surveillance rather than enhance freedoms and foster economic prosperity.[35] The number of public and private actors taking on policing or quasi-policing functions is growing, while challenges related to cross-jurisdictional legal definitions and effective checks and balances remain unresolved. In both developed and weak or fragile states, ICTs enable illicit groups to perform policing functions to advance their own interests or foster fear. In autocratic states, fear of the impact of ICTs is pushing leaders to develop more sophisticated policing methods to silence dissent, many provided by private companies based in the West. And in Western states, endless contradictions between the rights and security agendas are undermining strategic narratives both at home and abroad. Underpinning these challenges are a range of serious social, economic and political issues that will not be resolved solely through the criminalization of behaviour and the securitization of responses.

33 Klimburg (2011)

34 Interviews with Mexican investigative journalists, November-December, 2011

35 Karatzogianni (2009)

HOW SHOULD THESE MANIFOLD CONTRADICTIONS BE RESOLVED?

The longstanding international normative regime protecting individual and group rights, including privacy, continues to be seriously tested by the manner in which states are conceptualizing and operationalizing cyber security strategies. The rapid expansion of cyberspace offers the world unprecedented access to new democratic means of communications. However, as this paper has chronicled, a growing cyberspace presents equally unprecedented opportunities for the state to monitor its citizens in equally undemocratic ways. Unfortunately, a number of Western security agencies have started to deploy technologies that run contrary to their democratic ideals. The situation is even worse in more restrictive non-democratic states. Is the security and rights dichotomy reconcilable? What lessons can be garnered from tensions that have existed on the security vs. rights agenda outside of cyberspace? Would broader agreement or buy-in on an international normative base for responding to cybercrime help diffuse some of the major tensions emerging between the two poles? Who would oversee such a process? Are other measures possible?

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 Center 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

BIBLIOGRAPHY

Big Brother Incorporated. Privacy International, 2011. Web.

https://www.privacyinternational.org/big-brother-incorporated.

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

Brazil. Chamber of Deputies. PL 84/1999. http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028.

Bright, Peter. "UK "cyber strategy": Stuxnet, censorship, and cyber-specials." *Ars-Technica*. 28 November 2011. Web. http://arstechnica.com/tech-policy/news/2011/11/uk-cyber-strategy-stuxnet-censorship-and-cyber-specials.ars.

Deibert, Ron and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy*, 21:4 (October 2010).

Edwards, Lilian. "From child porn to China, in one Cleanfeed." *SCRIPT-ed*, 3:3 (September, 2006).

European Union. Court of Justice. *Judgment in Case C-70/10: Scarlet Extended v. Societe Belge Des Auteurs Compositeurs Et Editeurs SCRL (SABAM)*. 24 Nov. 2011. Web. http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf.

Geist, Michael. "Bill C-30 Opens Canada to Big Brother Inc. business: Geist." *The Toronto Star*. 26 February 2012. Web. http://www.thestar.com/business/article/1136406--bill-c-30-opens-canada-to-big-brother-inc-business-geist.

Hathaway, Melissa. "Taking a Byte Out of Cybercrime." *Hathaway Global Strategies LLC* (2011).

Kaihla, Paul. "The Technology Secrets of Cocaine." *Business 2.0*. July 2002.

Karatzogianni, Athina. *Cyber-Conflict and Global Politics*. New York, NY: Routledge, 2008.

Klimburg, Alexander (2011): Mobilising Cyber Power, *Survival: Global Politics and Strategy*, 53:1, 41-60

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

Nakashima, Ellen. "Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies." The Washington Post. 19 March 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

RSA Conference 2012, Moscone Center, San Fransico, CA. February 27 – March 2. http://365.rsaconference.com/community/archive/usa/blog/2012/03/01/video-rsac-us-2012-keynote--combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies--robert-s-mueller-iii

Rush, Howard, Chris Smith, Erika Kraemer-Mbula, and Puay Tang. *Crime online: Cybercrime and illegal innovation*. Project Report. NESTA, London, UK. July 2009. Web. http://eprints.brighton.ac.uk/5800/1/Crime_Online.pdf.

Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011).

Tikk-Ringas, Eneken. *Botnet Control & Command Takedown: Legal Considerations and the Role of ISPs*. Forthcoming 2012.

Tulloch, James. "End of the Internet As We Know It?" *Allianz*. 26 July 2010. http://knowledge.allianz.com/demographics/current_affairs/?1564/cyber-war-cybersecurity-cybercrime-internet.

United Nations. General Assembly, 17th Session. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue." (A/HRC/17/27). 16 May 2011.

United States. Department of Defense. Department of Defense Strategy for Operating in Cyberspace. July 2011. Web. http://www.defense.gov/home/features/2011/0411%5Fcyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

United States District Court, District of Connecticut. *Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief*. Case 3:11-cv-00561-VLB Document 32. Filed 13 April 2011.

Zetter, Kim. "With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal." *Wired*. 13 April 2011. Web. http://www.wired.com/threatlevel/2011/04/coreflood/.