Cybersecurity and spam:

WCIT and the future

Richard Hill
Hill & Associates
Geneva, Switzerland
rhill@hill-a.ch

Shawn Powers
Georgia State University
Atlanta, USA
smp@gsu.edu

***Abstract*—Various proposals for treaty provisions to increase international cooperation to improve cybersecurity and to combat spam were opposed by various countries (in particular the United States) during the ITU's 2012 World Conference on International Telecommunications (WCIT-12) in Dubai. For this and other reasons, a large block of developed countries did not sign the treaty approved in Dubai. This situation creates uncertainty regarding cooperation with respect to security issues and can lead to a continuation of unilateral, and extraterritorial, assertions of national powers, including surveillance and cyberwarfare. Yet there are continued calls for cooperation, in particular at the bilateral level. This paper provides background information and analysis, suggesting possible ways forward.**

Keywords—cybersecurity, spam, ITU, WCIT, cyberwarfare

I. Introduction

The World Conference on International Telecommunications (WCIT-12) was convened in December 2012 at the request of the members of the International Telecommunication Union (ITU) in order to revise the International Telecommunication Regulations (ITRs), a treaty which had been agreed in 1988 and which opened the way for the privatisation and liberalization that has since characterized the telecommunications sector [1].

The purpose of the ITRs is to establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services. The ITR's provide the groundwork from which the ITU promotes the development of telecommunication services and their most efficient operation while harmonizing the development of facilities for worldwide telecommunications.

The ITU Members States felt that it was necessary to revise the ITRs in light of the significant structural and technological changes that have taken place since 1988, in particular privatisation, liberalization, and the growth of mobile and IP-based networks.[1]

For various reasons[2], those structural and technological changes have resulted in a degradation of network security, increasing cybercrime, proliferation of viruses, worms and other malware, and proliferation of spam. The Internet was initially deployed to connect a handful of large, expensive computers operated by a small group of trusted collaborators. Security was not a major design goal. As Robert Khan, co-creator of TCP/IP, puts the matter: “At present, the Internet environment is tilted in favor of those with adverse motives, while the rest of the community must be on constant vigil to defend against harmful interference.”[3]

In addition, various states have been accused of practicing cyberwarfare. Not surprisingly, the USA accuses China [4] and Russia [5] of actively engaging in cyber-warfare or at least in commercial cyber-espionage. However, it is generally accepted that the USA and Israel conducted an apparently successful secret cyber-attack on Iranian nuclear facilities, through the Stuxnet virus [6]. Separately, Chinese government researchers have published in the open literature accounts of some of their work [7].

Given the ambiguous legal and normative doctrines governing the use of cyberwarfare, states are increasing their investments in offensive and defensive cyber weapons. For example, documents leaked by former NSA-contractor Edward Snowden reveal that the U.S. government ordered 231 offensive cyber-exploitation operations in 2011 [8]. Such operations are supported by over $1.65 billion in annual funding and aim to infiltrate millions of networked devices by 2015 [9]. According to a Presidential Policy Directive, a “cyber effect” is “the manipulation, disruption, denial, degradation, or destruction of computers, information or communications sytems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereron.”[10] The cited Directive contains provisions regulating the use by the United States of offensive cyber effect operations. But, unless limits are internationally agreed, state-led cyberwarfare threatens the trust required among stakeholders for any effective internationally agreed cybersecurity goals, and thus presents a unique challenge moving forward, and an opportunity for increased international cooperation. Indeed, the 2013 Seoul Conference on Cyberspace stressed the benefits of such international cooperation.[3]

[1] See ITU Plenipotentiary Resolution 146 (Antalya, 2006)

[2] Some of which are outlined in [2].

[3] See the Results of the Seoul Conference on Cyberspace 2013, available at:

As a result, concern regarding the lack of security of the Internet is widespread [11]. Vint Cerf, Khan's TCP/IP co-creator, agrees that a change is needed, noting, "We can't let it sit the way it is now, it is simply not adequate. We're depending too heavily on the internet, for too many different things to allow it not to be evolved to a more secure state."[12] Google's Eric Schmidt predicts, "In a world of asynchronous threats it is too dangerous for there not to be some way to identify you. We need a [verified] name service for people. Governments will demand it."[13] One solution, proposed by Robert Khan, would add a digital-object architecture to the Internet, possibly allowing for greater real-time monitoring and prevention of cyber threats [14].

Consequently, there have been calls for international cooperation to address these issues and alleviate the problems.[4] Richard Haass, President of the Council on Foreign Relations, suggests "Cyber is exactly at the point today where nuclear was maybe 50 years ago, where people are beginning to think, what sort of rules do we set up? What sort of arrangements do we put into place?"[16] The East West Institute's 2012 Cybersecurity Summit called for greater collaboration on cybersecutity between both the private and public sectors and international actors, noting "securing cyberspace is a global challenge—one that cannot be solved by a single company or country on its own."[17]

And indeed similar concerns and calls for cooperation are found in international agreements such as ITU Resolution 130, which recites various threats and trends and notes "the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memorandums of understanding, etc)".

II. Discussions at WCIT

A. Preparations for WCIT

Given this background, it is not surprising that the issues of cybersecurity and spam were raised during the preparatory process for WCIT. Indeed, the issue of Internet security had already surfaced in 1988 at the ITU's World Administrative Telegraph and Telephone Conference (WATTC), which was the predecessor of WCIT and which approved the 1998 version of the ITRs. When the WATTC was convened on 28 November, the Morris Internet worm[18] was still a topic of concern. Although the worm itself was not explicitly mentioned in the ITRs, the "avoidance of technical harm" provision of Article 9 is generally considered to have been inspired by a desire to take steps that would prevent a reoccurrence of problems of this type. This is possibly the first treaty provision dealing with the security of telecommunication networks, a form of cybersecurity.[5] A similar provision was subsequently added to what is now Article 42 of the ITU Convention.[6]

Various proposals were presented to WCIT regarding security and spam. All called for increased international cooperation, but differed in other respects.

One analyst [21] took the view that the true nature of some of the proposals was to limit state-sponsored cyberattacks and/or cyberwar. While an analysis of such proposals is beyond the scope of the present papers, one author (Hill) has made such an analysis and he does agree with this view[7].

The USA made it clear that it was opposed to any text on security or spam in the ITRs,[8] refusing even to consider a proposal that was essentially copy-pasted from one of US President Obama's Presidential Declarations[9]. The USA was successful in modifying the position of the European and some other with the result that there were strong differences of views going into the conference. The main reason given by the US for opposing cooperation to improve security and combat spam was a concern that a treaty provision to that effect could be used by authoritarian countries to justify censorship or other restrictions on freedom of speech or human rights [22] [23] [24].[10].

http://www.seoulcyber2013.kr/en/media/View.do?media_id=2242 accessed 30 October 2013

[4] See ITU WTSA Resolutions 40 and 52; and http://www.internetsociety.org/spam accessed 28 July 2013; and [15].

[5] Actually the original predecessor of the ITRs, the 1865 treaty that created the ITU, included a provision regarding the use of encryption, and such provisions are also found in later versions. But those provisions were as much about costs (they prevented the use of private short-codes which reduced the number of words in a telegram) as about national security, so they cannot be considered to be security provisions in the modern sense of the term. See [19].

[6] A detailed discussion of the evolution over time of provisions related to security in the various instruments of the ITU (including the "technical harm" provision of Article 9 of the ITRs) is given in [20].

[7] In a forthcoming book on the ITRs and WCIT [41].

[8] See WCIT document 9 "United States of America Proposals for the Work of the Conference", August 3, 2012,which notes that cyber security should be treated by member states primarily as a sovereign issue, and opposes "any effort to interfere with those rights."

[9] See ITU documents CWG-WCIT12/C-60 for the proposal, and CWG-WCIT12/TD-62 for the US opposition, expressed as "cybersecurity should not be included in the ITRs in any way, shape or form." The proposal is CWG/4/225 in the publicly-available "Draft of the future ITRs" found at http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf accessed 2 September 2013.

[10] When he testified before the US Congress on February 5, 2013, FCC Commissioner Robert McDowell stated "In fact, last year, China teamed up with Russia, Tajikistan and Uzbekistan to propose to the UN General Assembly that it create an 'International Code of Conduct for Information Security' to mandate 'international norms and rules standardizing the behavior of countries concerning

However, such reasoning is considered incongruous in light of the recent revelations regarding the PRISM and MUSCULAR surveillance programs, given that the US apparently conducts pervasive domestic and foreign surveillance, and that at least some of the foreign surveillance appears to be done without meaningful judicial oversight [25] [26] [27].[11] Be that as it may, the discussions at WCIT were difficult. However, compromise text was agreed.

B. *Outcome of WCIT*

The articles approved at WCIT include two new articles on security and spam. These articles state:

> "6: Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public."
>
> And
>
> "7: Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.
>
> Member States are encouraged to cooperate in that sense."

These articles have been heavily criticized in the US, however that criticism is not valid from a legal point of view [1]. More importantly, the position taken by the US at WCIT may create some backlash in light of the revelations outlining the scope of the National Security Agency's (NSA) surveillance operations[28] [29] [30].

III. The Future

A persistent refusal by many countries to be bound by the 2012 ITRs might have undesirable consequences. One way to avoid this situation would be that more countries agree to be bound, while recognizing that the treaty must be implemented in a non-controversial manner, that is, so as to avoid the negative consequences that some fear may be engendered [1].

If this does not happen, then signatory states may choose to enter into additional arrangements that might be detrimental to the global interconnectivity of today's telecommunications systems, which include the Internet. As a Canadian think-tank put the matter [31]:

> "the larger problem [of the split between signatories and non-signatories] in the long term is the overall degree of complexity introduced into the governance of international telecommunications, the potential for increased transaction costs and the eventual possibility of significant divergence between the two treaty regimes over time. Given the similarity between the two treaties [1988 versus 2012], as well as the long history of routine cooperation on international telecommunications and the resulting business relationships and accumulated social practice, there are reasons to believe that this complexity may be manageable, if suboptimal. This assessment may not apply, however, in the event that the parties to the new ITRs engage in subsequent negotiations, building on the accompanying resolutions to erect a parallel institution for Internet governance. In the event such a parallel institution duplicates the function of the Internet Assigned Numbers Authority or the IETF, the potential exists for serious harm to global interoperability. Further, since routing is currently done without regard for international borders, the existence of parallel Internet governance regimes that may evolve with very different privacy protections poses challenging questions about the sustainability and desirability of legacy routing practices."

It would thus appear important to continue current efforts to restore dialog, while recognizing that there are real differences in views about balancing human rights versus state security concerns, with a sharp split between countries. The split is most apparent between Western democracies and authoritarian countries, but there are differences even amongst the Western democracies (for example, restrictions on political speech are common in continental Europe, but unconstitutional in the USA). Restrictions in non-democratic countries can be widespread: apparently Chinese authorities monitor and remove posts on social networks [32], and Iran is developing software to control and restrict access to social networks [33]. In general, one can say that Western democracies privilege the rights of individual, while other countries seek to balance those rights with collective rights[12], that is, with the rights of a group or of the state as an entity (the concept of group rights in international law is controversial [34]).

information and cyberspace.' Does anyone here today believe that these countries' proposals would encourage the continued proliferation of an open and freedom-enhancing Internet? Or would such constructs make it easier for authoritarian regimes to identify and silence political dissidents?" see http://www.fcc.gov/document/commissioner-mcdowell-congressional-testimony accessed 28 July 2013.

[11] And, according to one of the authors (Hill) a legal analysis of the ITRs does not support the allegation that it could threaten freedom of speech [1].

[12] For example, at WCIT China stated that said that human rights concerned the rights of individuals, but also collective rights; and that they pertain to individuals and Member States alike. See 1.32 and 1.64 of WCIT document 77.

Despite this conceptual split, increasingly, both democratic and non-democratic governments are recognizing the need for greater restrictions and regulation of online behavior.

For example, the Russian Federation stated[13]: "However, freedom to express opinion together with anonymity should not become a synonym of impunity. Member States shall take necessary measures to ensure balance between freedom of expression to one citizens and non-infringement of rights and freedom to other citizens." And Iran stated[14]: "Internet has been used as a tool/means to disseminate false, untrue, misleading, inciting, provocative information, propaganda, cultural attack which have had adverse impact on culture, dignity, customs, tradition, conviction belief, friendship, family life, honor of peoples in certain circumstances, and for certain countries as well as social instability, security, integrity, unity, solidarity, integrity, political stability and peace in certain other countries."

Of course, the concept of protecting citizens from certain types of information exists also in Western democracies. Apart from the well-known case of European restrictions on hate speech, negation of genocide, and certain political parties, the UK Prime Minister recently called for restrictions on search-engine results in order to reduce access to child abuse images, and default filtering by ISPs to reduce child access to pornography [35]. And India has taken actions in some cases to block access to web sites that were felt to contain hate speech that was promoting violence [36].

Moreover, despite rhetoric to the contrary, the U.S. government supports greater government involvement in the establishment of baseline cyber security. According to Assistant Secretary of State Lawrence E. Strickling, "Given all the human actors involved in the Internet with all their competing interests, we have to ask, do governments have to be involved to sort out these interests so that the Internet will continue to thrive? I say yes."[37]

Similarly, CYBERCOM and NSA Director Keith B. Alexander (2012) has argued that securing private networks cannot not be achieved through voluntary mechanisms alone: "Recent events have shown that a purely voluntary and market driven system is not sufficient. Some minimum security requirements will be necessary to ensure that the core, infrastructure is taking appropriate measures to harden its networks."[38]

Despite this emerging consensus, publicly, governments articulate clear differences in approaches to balancing the right of the state to protect itself and its citizens with the right of free speech and other human rights. The tension arising from those differences affected the discussions at WCIT, and also the decision regarding whether or not to sign the ITRs, because of the symbolic and political implications of signing, and this quite independently of the legal implications.

Some may take the view that there is no need for a treaty regarding international telecommunication matters: any matters requiring inter-governmental coordination can be handled by soft-law, or bilateral or regional agreements. But the divergence of views expressed at WCIT indicates that there is a need to agree some basic principles at a high level, and to enshrine them formally in a treaty. Lack of treaty-level agreement regarding cooperation with respect to network security issues in effect favors the current practices of unilateral surveillance such as the US Prism program, and in effect makes it more difficult to combat spam, and to eliminate, or at least minimize, cyberwarfare. As noted explained below, this can have negative effects not just for human rights, but also for the commercial interests of global companies.

IV. Conclusion

Global trade and economic interdependence create incentives for nation-states to come together and agree to additional rules, or treaties, that collectively bind behavior and ensure the protection of shared resources. If one considers the Internet as a microcosm of society, then its natural progression from an infant, specialized technology to the global network of networks would likely follow the path of any highly complex and interdependent community. This is to say, it is both natural and predictable that, as the Internet becomes more and more integral to the collective welfare of citizens around the world, governments will act to protect this shared resource from the abuse of malicious actors.

Currently, governments approach this challenge from drastically different vantage points. In the authors's view, cybersecurity and Internet freedom are two opposite sides of the same coin. The principles that have allowed for the Internet's development and transnational growth, such as openness, interoperability, anonymity, flattened hierarchy, are precisely its weaknesses when it comes to securing the network of networks. Oftentimes, the exact same tools that enable greater cybersecurity can also enable human rights infractions, surveillance and restrictions of freedom of expression. This tension is, again, both natural and predictable given the lack of international consensus regarding the exact scope of protections for freedom of expression, privacy, intellectual property and individual rights in general.

Thus, a coordinated, satisfactory intergovernmental approach to cybersecurity seems highly unlikely at the moment. Moreover, without the proper incentive structure for states to agree limit offensive cyber operations, and share or coordinate cyber defense efforts, the trust required for any meaningful international effort will be limited.

Moving forward, governments should agree to cooperate and to continue discussions, rather than dismissing the issue on the grounds that any agreements or discussions infringe on national sovereignty. And, in addition to working on new technologies and programs to help secure parts of the web, the private sector needs to help shift the context within which states view cybersecurity. In Western countries focusing on how properly to balance security with individual freedoms is a

[13] In a contribution to the ITU's World Telecommunication Policy Forum (WTPF), see 2.3.1(n) of document WTPF-IEG/3/6 <http://www.itu.int/md/S13-WTPF13IEG3-C-0020/en> accessed 3 August 2013.

[14] In a contribution to the WTPF, see 2.3.1(d) of WTPF-IEG/3/3 <http://www.itu.int/md/S13-WTPF13IEG3-C-0005/en> accessed 3 August 2013.

natural approach, but this approach needs to be nuanced when applied at the international level by recognizing that, at present, there are very different views regarding the actual scope of human rights[15] and free speech. As Vint Cerf notes, "Because this is a gigantic collaboration and there is no central control, you can't force people to adopt security mechanisms in this kind of a global system. You have to create incentives for them to want to do that."[12]

The most powerful incentive that could push states to agree on a truly international and coordinated approach is economic. Not only must governments be reminded of the possible catastrophic economic consequences of cyber security failure, but they also need to be cognizant of the negative consequences of unilateral cyberwarfare. For example, it has been said that the U.S. private sector will likely lose billions in revenue as a result of the disclosure of the PRISM program. And American internet and technology companies, such as Google, Twitter and Microsoft, are increasingly viewed skeptically as potentially complicit with U.S. offensive cyber attacks [40].

In the authors' view, scaled internationally, current government-driven approaches to cybersecurity not only risk the integrity of the Internet, but they also threaten the economic model that Internet and technology sectors depend on. This needs to be made more clear, and properly documented, in order to create more powerful incentives for states to restrain cyberwarfare tactics and agree to an international, shared approach to cyber defense.

In this light, policy makers, including in the US, may wish to consider whether accession to the 2012 ITRs might send a positive signal in favor of future international cooperation.[16]

References

[1] Richard Hill, "WCIT: Failure or success, impasse or way forward?" *International Journal of Law and Information Technology*, Vol. 21 No. 3, p. 313, DOI:10.1093/ijlit/eat008.

[2] Richard Hill, "The Internet, its governance, and the multi-stakeholder model", *Info*, Vol. 16 No 1 (forthcoming)

[3] Robert Khan, "The Role of Architecture in Internet Defense," in Kristin M. Lord and Travis Sharp (editors), *America's Cyber Future: Security and Prosperity in the Information Age*", Center for a New American Security, Washington, DC., June 2011

[4] David Sanger, "U.S. Blames China's Military Directly for Cyberattacks", *New York Times*, 6 May 2013, available at: http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0 accessed 30 October 2013

[5] AP, "U.S. report blasts China, Russia for cyberattacks", *USA Today*, 3 November 2011, available at: http://usatoday30.usatoday.com/news/washington/story/2011-11-03/china-russia-cybersecurity/51065010/1 accessed 30 October 2013

[6] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012, p. A1.

[7] Richard Stone, "A Call to Cyber Arms", *Science*, vol. 339, 1 March 2013, p. 1026

[8] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show", *Washington Post*(31 August 2013, available at: http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html accessed 3 September 2013

[9] United States of America, "FY 2013 Congressional Budget Justification", Volume I: National Intelligence Program Summary, February 2012

[10] United States of America, , "U.S. Cyber Operations Policy," Presidential Policy Directive/PPD 20, October 2012

[11] David Talbot, "The Internet is broken", *MIT Technology Review*, December 2005/January 2006, p. 62 available at http://www.technologyreview.com/news/405318/the-internet-is-broken/ accessed 15 June 2013

[12] Vint Cerf, "Can We Make the Internet Safer?" Lecture delivered at the University of Maryland's A. James Clark School of Engineering, April 7, 2011, available at http://lecture.umd.edu/detsmediasite/Play/4feab66caa824cafae6d01798b4849e51d accessed 1 September 2013

[13] Marshal Kirkpatrick, "Google, Privacy, and the New Explosion of Data", Techonomy, 4 August 2010, available at: http://techonomy.typepad.com/blog/2010/08/google-privacy-and-the-new-explosion-of-data.html accessed 30 October 2013

[14] Robert Khan, "The Role of Architecture in Internet Defense", CNRI, June 2012, available at http://www.cnri.reston.va.us/papers/CNAS_CyberSecurity_Kahn.pdf accessed 3 September 2013.

[15] William New, "European Commission VP Kroes Urges Open Internet, Prods Copyright Owners", *Intellectual Property Watch*, 21 March 2013 available at http://www.ip-watch.org/2013/03/21/european-commission-vp-kroes-urges-open-internet-prods-copyright-owners/ accessed 22 March 2013.

[16] Richard Haass, interview with Eric Schmidt and Jared Cohen at the council on Foreign Relations, 29 November 2010 available at https://www.youtube.com/watch?v=eJAMD5p5tQo accessed 3 April 2013

[17] East West Institute,. "Building Trust in Cyberspace." 3rd Worldwide Cybersecurity Summit in New Delhi, 2012

[18] Ted Eisenberg et. al, "The Cornell Commission: On Morris and the Worm", *Communications of the, ACM*, June 1989, Volume 32, Number 6, p. 706

[19] Daniel R. Headrick, *The Invisible Weapon: Telecommunications and international Politics 1851-1945*, Oxford University Press, 1991, p. 45

[20] Anthony Rutkowski, "Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850", *Info*, Vol. 13 No. 1, pp.13 – 31

[21] Milton Mueller, "Threat Analysis of the WCIT: Part IV: the ITU and Cybersecurity", Internet Governance Project, 21 June 2012, available at http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/ accessed 3 September 2013

[22] Majority Committee Staff, "Hearing on International Proposals to Regulate the Internet", *Memorandum to the Committee on Energy and Commerce*, May 29, 2012 available at http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CT/20120531/HMTG-112-HHRG-IF16-20120531-SD001.pdf accessed 28 July 2013

[23] Chris Rizo, "Int'l proposals for U.N. Internet regulations draws bipartisan rebuke", *FierceOnlineVideo*, June 20 2012, available at http://www.fierceonlinevideo.com/story/plans-un-internet-regulations-draws-bipartisan-rebuke/2012-06-20 accessed 28 July 2013

[15] For example, the United States requires judicial oversight for monitoring of communications by its citizens, but no such oversight is required for monitoring of communications by non US-persons, see [39]

[16] However, it must be noted that objections to the ITRs were not limited to the security and spam provisions mentioned in this paper. A legal analysis of the objections is given in [1]. A more complete discussion, covering non-legal issues, is given in [41].

[24] US Congress, *Congressional Record*, vol. 158, no.116, Wednesday, August 1, 2012, House, pp. H5599-H5602 available at http://www.gpo.gov/fdsys/pkg/CREC-2012-08-01/html/CREC-2012-08-01-pt1-PgH5599-3.htm accessed 3 September 2013

[25] Richard Hill, “Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?”, in Weber, R. H., Radu, R., and Chenou, J.-M. (editors) *The evolution of global Internet policy: new principles and forms of governance in the making?*, Schulthess, Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (forthcoming)

[26] National Security Agency, “The National Security Agency: Missions, Authorities, Oversight and Partnerships”, 9 August 2013, available at: http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf accessed 13 August 2013

[27] Casper Bowden, “The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights”, Note for the European Parliament (2013) avaialbel at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf accessed 23 September 2013

[28] David Bosco, “Brazil Wants UN to Help Safeguard Internet”, *Foreign Policy*, 8 July 2013 available at http://bosco.foreignpolicy.com/posts/2013/07/08/brazil_wants_un_to_help_safeguard_internet accessed 28 July 2013; the article quotes Brazilian Foreign Minister Antonio Patriota.

[29] John Naughton, “Edward Snowden’s not the story. The fate of the Internet is”, *The Guardian* 28 July 2013, avaialable at http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet accessed 31 July 2013

[30] Evgeny Morozov, “The Price of Hypocrisy”, *Frankfuter Allgemeine*, 24 July 2013 available at http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html accessed 31 July 2013.

[31] M. Raymond and G. Smith, “Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance,” Centre for International Governance Innovation, Internet Governance Papers, Paper No. 1, July 2013, available at http://www.cigionline.org/sites/default/files/no1_4.pdf accessed 10 August 2013

[32] Tom Simonite, “Reading the Tea Leaves of Censorship”, *MIT Technology Review*, vol. 116, no. 4 , July/August 2013, p. 20

[33] Steven Musil, "Iran develops software to control social networks". *CNET*, 6 January 2013, available at http://news.cnet.com/8301-1023_3-57562295-93/iran-develops-software-to-control-access-to-social-networks/ accessed 15 June 2013

[34] Corsin Bisaz, *The Concept of Group Rights in International Law: Groups as Contested Right-Holders, Subjects and Legal Persons*, Martinus Nijhoff, 2012

[35] David Cameron, “The internet and pornography: Prime Minister calls for action”, *speech*, 22 July 2012 available at https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action accessed 28 July 2013

[36] Editors, “India Defends Internet Censorship”, *Jakarta Globe*, 24 August 2012, avaiable at http://www.thejakartaglobe.com/archive/india-defends-internet-censorship/ accessed 28 July 2013

[37] Lawrence Strickling, “Remarks”, conference at The Media Institute, 24 February 2010 available at http://www.ntia.doc.gov/speechtestimony/2010/remarks-assistant-secretary-strickling-media-institute accessed 4 September 2013

[38] Keith Anderson, “U.S. Cyber Command Cybersecurity Legislation Position Letter”, United States Cyber Command, 3 May 2012, available at http://publicintelligence.net/u-s-cyber-command-cybersecurity-legislation-position-letter/ accessed 3 September 2013

[39] National Security Agency, “The National Security Agency: Missions, Authorities, Oversight and Partnerships”, 9 August 2013, available at http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf accessed 13 August 2013

[40] James Staten, “The Cost of PRISM will be larger than ITIF Projects,” Forrester Research, 14 August 2013, available at http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects accessed 3 September 2013

[41] Richard Hill, *The new International Telecommunication Regulations: A Commentary and Legislative History*, (forthcoming) Schulthess