IDC HERZLIYA | Lauder School of Government, Diplomacy & Strategy | IPS Institute for Policy and Strategy
כנס הרצליה השנתי האחד-עשר
HERZLIYA 2011 הרצליה
The Eleventh Annual Herzliya Conference
כנס הרצליה HERZLIYA CONFERENCE
February 6-9, 2011
WORKING PAPER

Security in Cyberspace

D. Housen-Couriel, Adv, Yuval Ne'eman Tel Aviv Workshop for Science, Technology and Security

The Institute for Policy and Strategy

The Institute for Policy and Strategy (IPS) conducts projects and research on a broad analytical scope, concentrating on identifying emerging issues and trends crucial to Israel's national policy and decision-making process, including national security and strategy; foreign policy; the Jewish people; social policy and education.

Drawing on its range of networks and convening power, IPS fosters informed dialogue and debate, which impact national policy by producing and following the implementation of pragmatic responses, strategic directions and policy solutions.

The Herzliya Conference

Israel's premier global policy gathering, the Annual Herzliya Conference on the Balance of Israel's National Security is the flagship of IPS activities. The conference exclusively draws together international and Israeli participants from the highest levels of government, business and academia to address the most pressing national, regional and global issues.

The Conference proceedings, reports and recommendations provide leaders with timely and authoritative assessments and policy recommendations needed to guide their organizations through the challenging geopolitical, economic and social developments. As strategic, political processes and events emanating from an ever-turbulent Middle East increasingly impact the global arena, the deliberations at Herzliya cover a broad span of issues, ranging from nuclear proliferation and the Middle East peace process to finance, energy security and global warming.

Introduction

A lawyer's toolbox contains, to a large degree, definitions that allow him or her to make sense of human actions and the situations they create; and in the event, to argue for the application of a specific legal norm to human activity. The end result of this activity will for the most part be either a yes or no answer: the act in question is legal, or it's illegal. This constantly evolving process of refining definitions and concepts is a key aspect of the process of legal interpretation.[1] The new realm of cyberspace challenges international lawyers at this very fundamental level of definition. Where we thought that we had worked out, for the most part, a thorough understanding of the concept of state sovereignty, the limits on the use of force by states on the international plane, and the consequences of breaching those limits – a paradigm shift is now demanded of us. In the words of a leading scholar in the field, "Computer network attack represents a new tool of coercion in the international arena, one that is fundamentally different from those previously available.[2] And a second scholar extrapolates that "new tools require new rules".[3]

The professional troubles of international lawyers notwithstanding, the confusion around definitions and applicable legal norms of for terms such as cyberspace, cybersecurity, cyberattack, cyberterror and cybercrime has immediate, real-world and significant outcomes. In the various cyber events with which many of us are familiar, and which are occurring now with regularity, nation-states and international organizations do not have an available, credible response. The international system simply does not know what the rules of the game are, nor (yet) what they ought to be, even when pressing issues of national and international security arise. So that the massive disruption and distortion of Estonian government and financial websites in April and May 2007 resulted in the conviction and fining of a single hacker for about $1,400 – and a promise from NATO to start thinking hard about the cybersecurity problem;[4] China's Operation Aurora in the second half of 2009, which was aimed at appropriating source code and other data from dozens of leading high tech, security and defense companies resulted in notification by Google that it intended to review its business relationship with China[5] and the declaration by US Secretary of State Clinton[6] that allegations of Chinese cyberactivity raised "very serious concerns and questions". Reactions at the international level to the Stuxnet operation have been at the most, muted, although tens of thousands of computers and systems have been affected globally.[7] On the other end of the cybersecurity spectrum, when

1 H.L.A. Hart, The Concept of Law, Clarendon, 1961; G. Paton and D. Derham, A Textbook of Jurisprudence, 4th ed., Oxford, 1972.

2 M. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 Columbia Journal of Transnational Law 885 (1999).

3 D. Hollis," New Tools, New Rules: International Law and Information Operations", in G. David and T. McKeldin, ed.'s, The Message of War: Information, Influence and Perception in Armed Conflict, Temple University Legal Studies Research Paper No. 2007-15 , 2008.

4 R. McMillan, "NATO to set up cyber warfare center", Network World, May 15, 2008.

5 Google, "A New Approach to China", January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html,

6 "We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. I will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear." Secretary of State Clinton, "Statement on Google Operations in China", US Department of State, January 12, 2010.

7 W. Broad, J. Markoff, D. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", New York Times, January 15, 2011.

a state's political leadership imposes an internet and communications blackout, as did President Mubarak last week, official response is also subdued.[8] Beyond declarative protest, the global community does not have a ready response; at least, not a response that is being shared publicly. And this is currently the main challenge of cybersecurity for lawyers – working out these prospective rules of engagement.

The dilemma of definitions

The initial difficulty with defining cyberattack within the international legal regime, is, of course, that we're not sure that we can actually call it an "attack". In his seminal article on computer network attack (CNA) in 1999, William Schmitt writes that "...[t]o constitute an armed attack [that is, in the meaning of Article 2(4) of the UN Charter], the CNA must be intended to directly cause physical damage to tangible objects or injury to human beings."[9] Cyberattack that remains within the virtual realm, as those mentioned above do, for the most part, does not in fact cross this threshold.[10]

Interestingly, the focus of the international legal community has thus, in the meantime, been to promote what the International Telecommunications Union (ITU), the UN, the European Community, the OECD and several leading countries in cyberspace have called "a culture of cybersecurity".

The first international body to attempt a definition of cybersecurity's parameters was, not unexpectedly, the ITU itself. The doyen of international organizations, founded in 1865, has consistently distinguished itself in forward-looking and consensus-based regulation of communications infrastructures, beginning with the innovative telegraph lines crossing Western Europe in the second half of the 19th century.[11] Thus, in a 2008 resolution of the ITU standardization sector, ITU-T, cybersecurity was defined as:

> ...the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[12]

The ITU terminology and broad approach to "organization and user's assets" has been adopted and adapted by others, notably the OECD and the UN, in more recent years, and the ITU itself has recently resolved to adapt its definition to changing cybersecurity realities.[13] As it stands, this initial ITU does provide a frame of reference for discussing cybersecurity – but in only the most general of terms. For instance, it gives the practitioner no clear sense of what the "cyber environment", or "cyberspace" might be, for instance. Although one observer has defined this new realm as "the place where your phone call happens",[14] this important term has yet to be carefully defined. Perhaps the best effort so far has been that of the US Department of Defense, which defines cyberspace as:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[15]

Yet in this definition, the exclusion of human beings - operations personnel, web data producers and consumers, and perhaps especially those who are responsible for the maintenance and repair of the elements of cyberspace – would seem a significant oversight.[16]

Substantive norms- a *jus specialis*

Leaving aside for a moment the issue of defining our terms, it's central to the concluding thesis offered below that international lawyers have yet to meet the substantive challenge of elucidating the norms applicable to state and non-state entities when they act in cyberspace. This has not been for lack of initiative: there are presently several separate multilateral endeavors underway to forge a new treaty regime for cyber activity, mostly hostile cyberactivity.[17] These efforts are in addition to tens of working papers,[18] academic proposals,[19] conferences[20] and single state initiatives.[21]

Particular attention should be paid to the behavior of cyber-active states, as well (nearly all of the 193 in existence today), as indications of emerging customary law.[22] Interestingly, state responses to hostile cyber activities at the inter-state level have so far been characterized by restraint, as noted above. One example of a specific response is found in several countries having put the international community "on notice" that hostile acts or threats to their network assets or critical

8 D. McCollough, "Egypt's Internet disconnect reaches 24 hours", CNET News, January 28, 2011.

9 Supra note 2, at 935.

10 See, however the US Joint Forces military doctrine's operational definition of computer network attack, which does not contain this threshold. There, CNA's are defined as "..operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves." See Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, as amended through 31 December 2010.

11 A. Noll, The ITU in the 21st Century, 5 Singapore Journal of International and Comparative Law, 2001.

12 ITU-T Resolution 1205.X, 2008, 3.2.5.

13 Resolution WGPL 9, "Definitions and Terminology relating to building confidence and security in the use of ICT technologies", Final Acts of the Guadalajara Plenipotentiary Conference, 2010.

14 See also an exploration of continued existence in cyberspace after death, R. Walker, "Cyberspace When You're Dead" New York Times, January 5, 2011.

15 See "Cyberspace", in Joint Publication 1-02, [US] Department of Defense Dictionary of Military and Associated Terms, as amended through 31 December 2010. See also an earlier definition, the 2000 American National Standard T1.523-2001 for Telecommunications, - Telecom Glossary, cited in S. Rosenne, The Perplexities of Modern International Law, Hague Academy of International Law, 2002, p.348.

16 The White House's 2009 Cyberpolicy Review did include this human element, for instance; as did the ITU in its cybercrime legislation white paper. See, respectively, White House Cyber Policy Review, 2009 +and National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23); and the ITU Toolkit on Cybercrime Legislation.

17 See the interesting Note by the Secretary General containing the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 of 30 July 2010. The Group, composed of

18 For a recent example, see *K. Rauscher and A. Korotkov, Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, The East West Institute, January 2011.

19 For example, see D. Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", 47 Harvard International Law Journal 179 (2006); and **A Proposal for an International Convention on Cyber Crime and Terrorism** (2000, "the Stanford Proposal") at http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

20 The Munich Security Conference, held February 4-6 is a recent example. There, British Foreign Secretary William Hague called for an international cyber code of conduct, in revealing a hacker attack on the UK's Foreign Office, "William Hague reveals hacker attack on Foreign Office in call for cyber rules", The Observer, 6.2.2011.

21 [add note, EWI paper]

22 Customary law is a source of international law, according to Article 38 of the Statute of the International Court of Justice. Custom is defined as evidence of a general practice of states accepted as law, once certain criteria of consistency and awareness of a legal obligation are met.

infrastructures would be generate a military response. This mechanism goes to the important issue of cyberdeterrence, discussed in depth in Dr. Libicki's 2009 paper on Cyberdeterrence and Cyberwar.[23]

The single successful treaty effort so far has been that of the Council of Europe, whose Convention on Cybercrime from 2001 has been ratified by 30 countries, including non-Europeans such as Japan, the US and Canada.[24] The Convention is the only binding international instrument on cybersecurity, and has a double aim of providing guidelines for national legislation and a framework for cooperation among State Parties. It addresses, in particular, the costs of global cybercrime, the cost of which has been estimated by President Obama as approximately a trillion dollars annually.[25]

Four concluding thoughts

Cybersecurity and its attendant legal issues have raised difficult but fascinating challenges within the international legal community. We are no longer certain that state sovereignty is tied inexorably and nearly exclusively to the physical attributes of territory and population; we have no effective "international organization" model for governing the internet and the world wide web – if, in fact, they ought to be governed in the way that term is presently understood; we're not sure at what point hostile cyberactivity crosses the Charter threshold of prohibited use of force; and we certainly have no reliable way, at present, to attribute responsibility for activities in cyberspace to a given state, organization, group or individual.

Given these uncertainties, four concluding thoughts:

- We need a carefully-crafted set of cyberspace norms that flow from the deep understanding that the international community has today of permitted and prohibited uses of kinetic force, a ***jus specialis*** rather than a *jus de novo.*
- The technical means for **user attribution** of cyber activity – including, possibly, user, supplier and system accreditations prior to the initiation of activity, should be developed in conjunction with the legal norms of attribution.
- A better understanding of the interfacing **of dual- and multi- use critical infrastructures**, ICT and otherwise, with the internet and the world wide web must be developed, including mapping of domino effects when a given infrastructure is impacted.
- Finally, agreed **rules of engagement** that allow military systems to act with a high degree of certainty regarding the authorization of the use of military force, either virtual or kinetic; and the elaboration of appropriate rules of war.

*****

23 Rand, 2009. Libicki concisely writes (at p. 8) that "Deterrence has to work in the mind of the attacker." Open declarations on the part of states regarding their self-identified thresholds of threat and the response that can be expected promote this aim, although such declarations also serve to expose vulnerabilities.

24 Convention on Cybercrime, Council of Europe, 2001; and Additional protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, 2006. Israel is not a party to either document. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG

25 "War in the fifth domain" The Economist July 1, 2010: "Mr Obama has quoted a figure of $1 trillion lost last year to cybercrime—a bigger underworld than the drugs trade, though such figures are disputed." At the Munich Security Conference, a figure of 1.6 billion dollars was quoted. See C. Habig, "Cyberspace Presents Complex Global Challenges", Munich Security Conference, 6.2.11 (http://www.securityconference.de/Program.425+M578c0183589.0.html?&L=1).

Yuval Ne'eman Workshop for Science, Technology and Security

Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program with the intention of exploring the link among security policy, technology and science. For this reason the workshop holds an annual series of conferences and conducts research. The workshop covers various topics such as international relations and strategy, missiles and guided weapons, robotics, space policy and security, cyberspace and cyber warfare, nuclear energy, homeland security, the interplay between society and security, force build up policy and government decision-making processes.

Institute for Policy and Strategy
Lauder School of Government, Diplomacy and Strategy
Interdisciplinary Center (IDC) Herzliya
P.O.Box 167, Herzliya 46150, Israel
Tel: 09-9527389, Fax: 09-9527310
E-mail: ips@idc.ac.il
Website: www.ips.idc.ac.il

DESIGN: NIRIT GIL