

# A New Paradigm for Law, Policy and Technology: National Security and “Cyber” Hit the News

Pauline C. Reich

Professor, Waseda University School of Law, Tokyo,  
Japan

RAISE, Singapore, March 9, 2010

[pcreich@aol.com](mailto:pcreich@aol.com)

# New Issues, New Books

- Pauline C. Reich, J.D., M.A. and Eduardo Gelbstein, Ph.D., LAW, POLICY AND TECHNOLOGY: INFORMATION WARFARE, CYBERTERRORISM AND DIGITAL IMMOBILIZATION (IGI Global, USA, Summer 2010)

# Where are we, anyway?

- Preliminary stage of defining what the terms bandied about by the media mean in terms of law, policy, national security and technology communities
- To write laws and apply them, we need definitions
- To describe/defend national security, we need definitions
- To engage in diplomacy, we need definitions

# Uncharted waters - When to reinvent?

- Example: Silicon Valley 1990s
- New paradigm
- Many young entrepreneurs, easy venture capital, new ways of doing things
- Many failures
- Return to mixture of new and existing structures for businesses

# Cyberterrorism – not even a consensus on what is terrorism...

Maura Conway:

“When it comes to the intersection of terrorism and the Internet, three phenomena are distinguishable:

- Attacks upon or via the Internet
- Dissemination of terrorist content
- Other uses (e.g. the use of Internet telephony and virtual financial transfers in attack preparation, etc.)”

# Defining “cyber”

- Recent research – 28 definitions of *cyberspace*
- “Definitions should be used as an aid to policy and analysis and not a limitation on them”- Franklin D. Kramer, “Cyberpower and National Security: Policy Recommendations for a Strategic Framework,” in CYBERPOWER AND NATIONAL SECURITY, Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz

# Daniel Kuehl definition of cyberspace

- “An operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected and Internettetted information systems and their associated infrastructures.”

# Generic term – “cyberattack” may be more useful until we define terms

- Attacks on Estonia in 2007 and terminology applied:
- Cyberwar
- Cyber riot
- Cyber mob
- Etc.

Functional definition might be better – what happened to the critical information infrastructure? How much damage? What kind of damage?

Real problems for the law  
community:

Attribution

Anonymity

Botnets

Traceability

Presenting evidence in  
court

**Points to be worked out  
through diplomacy and policy**

Country to country

Regionally

Internationally

- Conveying what is acceptable and what is not
- Non-state actors
- State actors
- Sanctions

# OK, now we have somewhat described it functionally – what do we do?

- Investigation – possible
- \* Deterrence-a viable strategy? Perhaps the best option we have for now and one in which RAISE members can play a role in finding means
- Retaliation – in what form?
- What does a cyberwar look like, anyway?
- No paradigm for it – certainly not a nuclear one
- Legislation - What is the benefit of shutting down an individual country's network as a defensive measure? The global network?

# Deterrence

## **PROS**

“Cyberpower and National Security: Policy Recommendations for a Strategic Framework,” Franklin D. Kramer in CYBERPOWER AND NATIONAL SECURITY, pages 15-17

A viable strategy

Need to consider in overall concept of deterrence, not as separate cyber arena

Combination of potential retaliation, defense, dissuasion

Retaliation not limited to cyber means – could be diplomatic, economic, kinetic or cyber

Retaliation would be at a time, place and manner of target’s choosing

## • **Con**

- Difficulty of attribution of sources of cyber attacks

# Kramer (continued)

- Important differentiations could be of consequence:
- State actors have geopolitical aims and are susceptible to classic geopolitical strategies
- Retaliation might be more available against state actors
- Dissuasion might be more effective against state actors
- Non-state actors less susceptible to classic geopolitical strategies
- Indirect strategies, such as affecting the country in which they live , might have impact, e.g. on “patriotic hackers”

# Analysis of Kramer (continued)

- “Cyber defense, law enforcement and, for terrorists, classic counter terrorist techniques may be most effective”
- PR question- when does law enforcement get involved and how ? Look at Korea and Estonia cyberattacks in 2009 and 2007 respectively
- Which types of agencies get involved and how?
- What capability does an individual country have or should it have?
- Another important question:
- At what threshold is a more significant/robust response appropriate?
- Estonia does 98% of its banking online and its system was down for a number of days
- How to distinguish *high end* and *low end* attacks
- Or what about military immobilization? Critical information infrastructure?

# Kramer

- A major part of deterrence policy will be to create greater capabilities to assist in attribution, including:
- Developing more effective technical means, such as monitoring and intrusion devices, traceback and forensic capacities
- Other technical efforts, e.g. new architectures, protocols, types of servers and routers
- Recommends making appropriate private networks “hard targets” – why not making all networks “hard targets”?
- Recommends creating an international framework that will help end such cyber conflict –
- Where is NATO going? Estonia Cyber Defense Center conferences may yield some strategies
- United Nations?
- Regional organizations first?
- The former are roles that RAISE members might get involved with (government and academe), but what about private sector?
- In addition to the technical responses, Kramer suggests the expansion of intelligence capabilities and law enforcement capabilities for low end attacks – again, how do we trace when there is anonymity? Can tech community develop more capability to do so?
- PR – The Estonia and Korea attack scenarios did not rely extensively on these capabilities and creating such a climate may be repugnant to privacy and human rights communities

# Michael N. Schmitt's Six Criteria Applied to Viewing Cyberattacks

- Severity – scope and intensity of attack – number of people killed, size of area attacked, amount of property damage. The greater the damage, the stronger the argument for treating a cyber attack as an armed attack
- Immediacy – duration of cyber attack, how long its effects were felt. Longer duration = stronger rationale for treated as an armed attack
- Directness – harmed caused, proximate cause of harm?
- Invasiveness – electronically crosses borders and causes harm within a victim state.
- Measurability – quantifiable damage, not speculative harm.
- Presumptive legitimacy – state practice and accepted norms of behavior in the international community.
- See “Analyzing Cyber Attacks Under Jus ad Bellum,” in Jeffrey Carr, *INSIDE CYBER WARFARE*, pages 60-61 (O’Reilly, 2010), citing Schmitt
- And T. Wingfield

# Initiatives

- Estonia – adoption of new Penal Code provisions and national cyber security strategy after 2007 attacks – might be a useful model for other countries, though it discusses gaps and deficiencies in national law and international efforts
- Council of Europe
- Still talking about cyber terrorism?
- United Nations
- General Assembly proposed resolutions
- Asia-Pacific/Oceania region – What role can RAISE take? Can we lobby/educate within APEC? ASEAN? Other organizations? Conduct region-specific research? Teach the rest of the world how we are doing things?

# Some of the roadblocks to improving the state of the art

- Closed communities
  - Law enforcement at national and international levels – when should they dialogue with the tech experts? Learn from them?
  - National security agencies must of necessity keep a distance from the rest of us
- Policy and legal issues surrounding the question of when should an average citizen's privacy be invaded in the name of national security?

# For the latter issue, see work by Marc Rotenberg, for example

- In the modern era, the right of privacy represents a vast array of rights that include clear legal standards, government accountability, judicial oversight, the design of techniques that are minimally intrusive and the respect for the dignity and autonomy of individuals. The choice that we are being asked to make is not simply whether to reduce our expectation of privacy, but whether to reduce the rule of law, whether to diminish the role of the judiciary, whether to cast a shroud of secrecy over the decisions made by government.
- In other words, we are being asked to become something other than the strong America that could promote innovation and safeguard privacy that could protect the country and its Constitutional traditions. We are being asked to become a weak nation that accepts surveillance without accountability that cannot defend both security and freedom.
- That is a position we must reject. If we agree to reduce our expectation of privacy, we will erode our Constitutional democracy.
- Marc Rotenberg, Electronic Privacy Information Center, Privacy vs. Security? Privacy (2007)
- Of course, each economy present in RAISE will have to decide its own policy on such issues in the context of its own laws

# On the other hand, see

- National Security Council
- The Comprehensive National Cybersecurity Initiative
- Howard Schmidt announcement on March 2, 2010 about declassification of parts of CNCI in effort to improve transparency
- A change to “transparency and partnership” in US cybersecurity policy
- Of course each economy in RAISE will have to make its own decisions about these and other issues in the context of its own laws and policies adopted

# Various Cybersecurity acts pending in US Congress

- Controversial proposals include authorizing the President of the United States to shut down private sector networks in case of national emergency, certification of Information Security professionals
- No word from White House officials speaking at RSA about status of those bills

# Where do we go from here?

- Real need for interdisciplinary teams and dialogues
- Real need for brainstorming at the national level
- Real need for a commitment to maintain peace in the cyber realm, to use the networks for world development, not for the same old same old

# Some steps that could be useful

- Setting up national, regional and global think tanks that are coordinated among disciplines and engaged in knowledge sharing, e.g. law, policy, diplomacy, Information Technology
- Providing good knowledge bases in each country with open access
- Funding for research and collaboration – **we really, really need to generate Asia-Pacific/Oceania/South Asia publications because our scenarios are sometimes quite different from those in the West**
- **Translation of scholarship and information into major UN languages – particularly from Asia-Pacific region, since it is one of the largest users of Internet, with fastest growth rate**
- Development of a global treaty about cyber attacks affecting national security with sanctions other than war

## For further reading – many publications in recent years

- Susan W. Brenner, CYBERTHREATS, Oxford University Press (2009)
- Scott W. Beidleman, DEFINING AND DETERRRING CYBER WAR, Army War College, Pa. (2009) (Available via [worldcat.org](http://worldcat.org))
- Bradley L. Boyd, CYBERWARFARE: ARMAGEDDON IN A TEACUP? Master's Thesis, Fort Leavenworth (2009) (via [worldcat.org](http://worldcat.org))

# And...

- Jeffrey Carr, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD, O'Reilly (paperback) (2009)
- Eric Chabrow, "Howard Schmidt Dismisses Cyberwar Fears," 3/5/10, [http://www.govinfosecurity.com/articles.php?art\\_id=2267&rf=030810eg](http://www.govinfosecurity.com/articles.php?art_id=2267&rf=030810eg)
- Eric Chabrow, "Howard Schmidt Achieves Rock-Star Status," 3/1/10, <http://blogs.govinfosecurity.com/posts.php?postID=464>
- Martin C. Libicki, CYBERDETERRENCE AND CYBERWAR, RAND (2009) Available in PDF format from website, <http://www.rand.org>
- Martin C. Libicki, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE, Cambridge University Press (2007)
- Ministry of Defense, Estonia, Cyber Security Strategy (2008) (PDF)

# And

- National Security Council – The Comprehensive National Cybersecurity Initiative,  
<http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>
- National Security Council – Transparent Cybersecurity- Howard Schmidt, 3/1/10,  
<http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity>
- RSA Conference 2010 Webcasts, Remarks from Howard Schmidt, 3/2/10, <http://media.omegiaweb.com/rsa2010/webcast.htm?id=1-6>
- RSA Conference 2010, Panel Discussion: Big Brother,  
<http://media.omegiaweb.com/rsa2010/video-only.htm?id=2-1>

# And

- Marc Rotenberg on Security vs. Privacy (in *Scheier on Security*), [http://www.schneier.com/blog/archives/2009/05/marc\\_rotenberg.html](http://www.schneier.com/blog/archives/2009/05/marc_rotenberg.html)
- Marc Rotenberg, Privacy vs. Security? Privacy, 11/9/07, [http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-privacy\\_b\\_71806.html](http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-privacy_b_71806.html)
- Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law* 37:885, 913-915 (1999)
- T. Wingfield, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE, pages 124-127, Aegis Research Corp. 2000

# Let's continue the open discussions and brainstorming in RAISE....

- Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute
- Waseda University School of Law
- 1-6-1 Nishi-Waseda
- Shinjuku-ku, Tokyo 169-8051
- Japan
- pcreich@aol.com
- (81) (3)-5286-1854
- (81) 90-6545-4353