International Cyber Security Conference Final Report

Chuck Barry, Lauren Lee, and Marek Rewers

Center for Technology and National Security Policy

National Defense University

June 2009

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

CTNSP International Cyber Security Conference
29-30 April 2009
Wrap up Report by Chuck Barry, Lauren Lee, and Marek Rewers

I. Introduction

The Center for Technology and National Security Policy (CTNSP) hosted the "Challenges in International Cyber Security" conference at the National Defense University (NDU) on April 29-30, 2009. In addition to 40 speakers and organizers, an average of approximately 135 persons attended each session, including more than two dozen non-U.S. attendees.

The Conference Agenda is enclosed at the end of this report. This unclassified event was held under NDU's non-attribution rules; hence the report that follows summarizes main points from each panel without reference to persons or affiliation.

II. Twelve key observations during the conference:

- There is, in essence, but one network in cyberspace and all stakeholders have to cooperate in securing that network for every user. At present, each nation or corporation operates on its own and secures its own networks; there are no rules of the road or commonly accepted defense measures. Cyber threats are addressed reactively on a case by case basis. All this is very inefficient and ineffective for countering a widening range of global threats. Every cyberspace user should recognize it is time to move toward international agreement on better governance and provide for responsive, distributive and integrated defenses.

- Developing effective defenses requires improved mechanisms of indication and warning, increased situational awareness, and the employment of advanced technology. It also requires the technology to develop methods of attack attribution so we can respond to threats.

- There is broad consensus that international dialogue on cyber governance, crime and security is imperative and overdue. Allies look for the U.S. to take the initiative, perhaps initially with a small group. However, the U.S. should also initiate dialogue with other major cyberpower states, including Russia, China, India and Brazil. Multilateral discussions and eventual agreements on unlawful activities, securing transnational critical infrastructure, and attribution metrics will provide open and real-time understanding of network safety and security. However, it is imperative that while we develop advanced measures to prevent crime and avoid conflict we also protect civil liberties.

- The potential for warfare in the cyber domain will be determined by three factors – the development of laws, a deterrence construct, and operations. Law is the first thing. It addresses the essential questions of legal entities and the international laws they must abide. Issues that must be addressed include the proper role of sovereignty, right of passage, defining internal versus external defense, and the preservation of personal rights.

- Cyber threats are by their very nature asymmetrical and credible deterrence requires at least the capability to respond in kind to cyber attacks. However, we have not yet made the distinction as to what constitutes a legitimate response to cyber attacks.

- There are three general levels of 'bad' cyber activity – individual hackers, organized criminal activity, and nation state on nation state attacks. States counter the first two levels by building law enforcement institutions while the last level falls under the laws of armed conflict and is dealt with by defense ministries and departments. This traditional bureaucratic division of effort will build two separate defense capabilities – one for internal and one for external threats – and spread our intellectual capital across two separate cyber security organizations. It is not clear that would be preferable. We need to think more about the information age implications for organizing our defenses.

- The first requirement when seeking to coalesce cyberspace governance is the recognition that spoken and written words form the foundation of our understanding of cyberspace and its governance. As such we need to come up with clear definitions if effective governance is to exist. We also need a common lexicon and broader understanding of criminal threats, governance tools and what constitutes cyber security.

- The U.S. and others have not fully established national governance over cyberspace matters. For example, it is unclear where responsibility lies for protecting computer networks. In order to develop a coherent approach to international cyber governance, the U.S. needs to overcome such ambiguity by building a system of national governance for cyberspace.

- We have entered an age of global interdependency in terms of national security and financial stability. This requires a new degree of international coalescence. Connected with this are serious questions about the ability to build trust with certain nations. We must determine the areas of mutual interests, threats and vulnerabilities so as to develop proper/acceptable self defense tactics. We should approach the table with global financial stability as a least common denominator, then transition into mutual national security interests.

- When assessing international prospects for future cyber security efforts, considerations of statute and law are essential first order tasks. In addressing this issue, it is critical to go beyond the customary focus on infrastructure security; content security is equally important.

- The international community needs to federate monitoring efforts not just among governments but also across the public-private divide. By sharing operational information and working in close coordination, such federations will more effectively leverage the tools they have for countering emerging cyber threats. Close cooperation can also have a “rub off effect’ improving habits generally; a good example being the NATO Cooperative Cyber Defense Centre of Excellence in Estonia, which has already had a positive effect on the Alliance as a whole.

- Meshing commercial goals with national security goals will further incentivize close cooperation and security advances. Collaboration among international industries can work from the outside in to get foreign governments to embrace cyber security standards. This includes embracing cloud computing as a solution to many security problems. Another important step is the development of a culture of ethics and responsibility regarding cyber security, and the education of future generations of managers, leaders and policy makers into that culture.

III. Two points echoed throughout:

- There is as yet no international approach to cyber security and as a matter of urgency the international community needs agreements that define cyber “rules of the road” and provide security similar to other domains of human endeavor – the sea, air, space and land. The cyberspace challenge is made more daunting by two striking differences. Firstly, cyberspace is not bounded by the familiar geographic frame of reference that defines all other domains. Secondly, those to be governed in cyberspace are not a manageable number of ships, planes, etc. on fixed routes, but billions of global users acting continuously and almost anonymously. And the cost of entry is negligible.

- The process of reaching international agreements on cyber security will be long and arduous, given the number of national and transnational stakeholders and the challenges just noted. Though many called for cooperation, no global or regional forum was recommended as the place to start the process. Most of the world looks to the U.S. to take the lead. Yet calls for U.S. leadership were coupled with emphasis that others expect and intend to have considerable voice in shaping cyber security agreements.

IV. Conclusions and Recommendations

- There is a big gap in our understanding of the perspectives of other nations and organizations such as the EU on cyber security. This first conference focused on other nations and international organizations, as well as the views of major U.S. agencies and the private sector, was a start at closing that gap. This is a useful model for the future.

- The concerted effort made to hear perspectives from Brazil, Russia, India and China (the so-called BRIC countries) and international organizations such as NATO, EU, ICANN and ITU paid off and was welcome by U.S. as well as international participants. We should build on this experience to start a dialogue that can inform U.S. policy makers.

- Among the 3-4 annual conferences held on cyber issues, CTNSP will endeavor to conduct one a year with strong international participation. We will look to increase international participation among speakers as well as attendees with the aim of furthering discussion on international norms for cyber security.

- Those who did not participate but who should do so at future events, including major industry players and high-density international users such as Germany.

- A major power that was not present (but represented in an outstanding way by a U.S. expert) was China. In future conferences at the unclassified level we should strive to hear directly from China on their approach to cyber governance, crime and security.

- The U.S. should consider a major new initiative in the area of international cyber security, one to commence the process of cooperation among nations, beginning with allies but also, perhaps separately, with each major cyber power. Initial goals might be to agree on terms of reference and definitions, then proceed to confidence and security building measures, and perhaps an annual conference at some level of official representation. Rudiments of collaboration already exist at NATO, the Council of Europe and (we have heard) the Shanghai Cooperation Organization. The U.S. goal should be to assert leadership and demonstrate initiative around which other powers can coalesce.

- Several participants, including from MIT, Chatham House and Lomonosov University (Moscow) expressed interest in continued engagement with CTNSP on the subject of cyber security, in particular, setting up venues to discuss definitions and norms related to cyber governance. We will evaluate the possibilities and may have recommendations along these lines in the near future.

V. Panel Highlights

Topic 1 - The International Challenges of Crime, Security, and Governance

The nature of our response to cyber-crime has remained basically unchanged over the past 25 years though it has grown exponentially as a threat due to the value of information systems. One reason for little progress is the lack of a universal language to describe the problems we face. Lexicon is needed to define precisely the dimensions of cyber crime given the differences that exist among nations. Once a common understanding of the threat, a vast array of actors need to devote a great deal more resources to counter cyber crime.

One of the most important groups of actors we have to engage is the cyber technology industry. From an international perspective there is a proliferation of differing privacy and data protection laws and regulations making it difficult for international corporations to meet global security challenges. Streamlining and standardizing regulations would help private industry develop effective solutions to cyber threats. Additionally we must understand the relationship between privacy and security as they are inexorably linked. Strategically, we need to adopt a risk-based approach to deal with compliance issues.

In addition to common definitions and engaging industry, there is a need to develop an understanding of cyber governance issues. The U.S. is the natural leader in advancing cyber security; therefore U.S. participants should be well informed on our positions when participating in international forums. Key to this preparation will be to understand the current and developing cyber environment.

Currently the Internet is largely governed by ambiguous semi-public, semi-private, part-U.S. based, part-internationalized organizations (e.g., ICANN & ITU). The U.S. should develop sound positions on what role such organizations will play in the future and how they can be folded into a developing cyber security structure. We need national positions on what role international conventions such as the Cyber Crime Convention of the Council of Europe should play in addressing cyber security.

Topic 2 - Policy Challenges in Defending Against Cyber Attack

Cloud computing is just emerging as the third phase of Internet evolution. We have to make careful yet wise policy choices that will strengthen security while not impeding progress. We should be embracing the cloud.

Law enforcement works only with identification and attribution. We have to be able to do this in cyberspace. In addition, we need to move to one common understanding of a threshold for unacceptable behavior. We need to clarify and build on existing norms rather than seeking to start from scratch.

Doing the basics right has not been a priority for DOD. It is a significant challenge dominated by embedded culture, methodical processes and the regular turnover in political leadership. The dictates of these factors automatically influence priorities. Lack of a clear concept of territorial jurisdiction, sovereignty, territorial integrity result in inconsistent approaches to cyber events/attacks even within a given agency, including and perhaps especially DOD.

Another challenge is to ensure security not only of data but of usage of data. Security of usage would allow use of fully open networks and in effect, bring more effective cyber security.

We must understand and accept that there are multiple views regarding policy aimed at countering cyber attack. By accepting and encouraging a competitive market of ideas the best solutions will emerge more rapidly than with a rigid tightly controlled mechanism.

Addressing concerns over cyber security must move from the margins to the mainstream, both within agencies and by national and international leaders themselves. By bringing cyber security to center stage across both public and private enterprise it will attract the extended global expertise of both sectors to develop truly innovative, continuously evolving solutions.

Topic 3 - Critical Cyber Infrastructure Protection

The timely sharing of information about cyber vulnerabilities and attacks among private companies and with the government can help mitigate losses, but must be actively encouraged and facilitated more so than at present to enhance the cyber preparedness of government and the critical infrastructure.

With the convergence of cyber and communications, the traditional Federal Government need for communications networks to maintain a continuity of government and operations, has evolved into a public-private imperative to promote survivability of the circuits on which the interconnected network of information systems depend, and upon which critical infrastructure relies.

Standards and best practices generated by a public-private collaborative process, tailored to the needs of individual sectors, can help crystallize the business case for resource allocation to risk mitigation, and inform the debate and decision-making about the possible need for regulation.

Critical infrastructure protection requires not only preparedness for response to threats, but also a collaborative public-private effort, facilitated by government, to develop and conduct risk assessments to inform and prioritize national and sectoral risk mitigation. Some of the issues that are important to cyber critical infrastructure protection – such as control systems risk — require a long-term, public-private collaborative commitment to identify and develop, and eventually deploy, mitigating measures.

Topic 4 - Potential Thresholds of War in Cyberspace

In the current environment there is no consensus as to what constitutes an act of war in cyberspace. We need to clarify what differentiates cyber war from a less severe cyber threat. To this end, the U.S. should undertake to establish a real "line in the sand" beyond which cyber attacks would clearly constitute an act of war. The level at which this threshold is set is less important and is ultimately a policy decision; however it needs to be established. That would allow formulation of contingencies plans and when the need arises, the processes necessary to respond.

In the process of defining cyber warfare, as in other cyber security initiatives, partnerships are critical. Strong ties need to be forged between governments and private sector owners/operators of networks as well as between the governments of various states. Open communications among trusted powers, agencies and groups will allow for building broad agreement on the identification of unacceptable behavior and the design of proportionate responses.

The UN Charter provides the most useful and widely accepted framework for drawing the distinction between "war" and "not war" in the conventional sense. For this reason its principles should be extended to define cyber war and determine appropriate responses. Despite its unique nature, the laws of war should apply to cyber space as it does to war in all other domains. For this reason we must identity how the principles of self-defense, proportionality and sovereignty apply in cases of cyber attack.

Topic 5 - National Perspectives on Infrastructure Protection, Cyber Crime, and the Potential for War in Cyber Space

Many of the recent developments in cyber crime and cyber security threats are developing abroad. These threats fall into a spectrum of ranging from state level action to criminal activity carried out by groups or individuals.

Especially informative regarding cyber-crime is the case of Brazil, which faces a significant problem with large gangs operating primarily via cell phones. In such countries, cell phone attacks are a far greater problem than computer-based cyber attacks and the result is the same or worse. Gangs from within Brazilian prisons shut down vital government-provided functions across a major metropolis, such as public transportation and firefighters. The Brazilian government was caught by surprise and is beginning to respond to the threat. In addition, Brazil is suspected of being a primary global source of botnets – i.e., networks of software robots run autonomously and automatically to deny services or distribute malicious code. Brazil's experience is an indication of the future of cyber crime.

Russia's main concern is the use of the cyber domain for state-on-state hostilities. Her main interests are preventing an 'arms race' in cyber space and limiting the aggressive use of cyber technologies. Russia did not address its internal governance or criminal concerns but focused on the international issues of making the Internet more secure and establishing legal and other preventative measures against the hostile state-on-state use of information and communications technologies (ICT)

India is rapidly becoming a global cyber power and has great potential to shape the future of the cyber security environment. It claims to have a low level of cyber crime because the user community values the positive benefits of connectivity more than its unlawful use. India has well developed national regulatory governance and laws but has not ventured far into international governance. If indeed genuine, India’s efficiency in mitigating cyber security threats could be one model for an international framework.

Perhaps more than any other country China exhibits cultural and political acceptance of cyberspace as a legitimate and necessary tool of international relations. China is poised to further these goals by taking advantage of its position at the headwaters of the global hardware and software supply chain to infuse an array of cyber systems with access points for its own state-directed activities. China also knows that malicious use of cyber power is a double-edged sword that can disrupt its own processes due to either internal or external anti-government activities.

Topic 6 - Institutional/Multilateral Governance Initiatives

There are clear gaps in the institutional and multilateral effort to counter cyber threats. Solutions will have to emanate from a variety of levels ranging from multinational organizations to individual innovators. As the global technological leader, the United States must take the lead to enhance the strength of multinational cyber security organizations if that is to happen.

The private sector continues to determine the level of cyber governance in the United States. It already addresses many cyber security problems both across various industries and in concert with governments. Private industry has the expertise and organizational flexibility to deal with problems that bureaucratically normalized responses are too cumbersome to address.

Notwithstanding this reality, national governments and ICANN should tap into the talent of individual experts and even amateurs to provide a stream of solutions for evolving and anticipated cyber problems. By outsourcing to the competitive private market, governments will seed informal collaborative networks that can develop the best solutions to a problem for minimal cost.

CHALLENGES IN INTERNATIONAL CYBER SECURITY

Center for Technology and National Security Policy
National Defense University
29-30 April 2009

29 April 2009 – Day 1

0815 – 0830 Welcome: Dr. Hans Binnendijk, Director, CTNSP

0830 – 0915 Keynote Address: LTG Keith B. Alexander, Director, National Security Agency, Chief, Central Security Service
Topic: **A U.S. Perspective on International Cyber Security**

0915 – 1045 **Panel One**: **The International Challenges of Crime, Security and Governance**
Panel Chair: Dr. Stuart Starr, CTNSP
Panel:
Mr. Mark Rasch, Consultant (formerly DoJ)
Topic: **Taking the Measure of Cyber Crime**
Mr. Ed Skoudis, SANS Institute
Topic: **Security in Cyber Space: How Good is it?**
Ms. Jody Westby, CEO, Global Cyber Risk
Topic: **State of Cyber Governance**
Mr. Rich Baich, Principal, Security & Privacy Services, Deloitte & Touche LLP
Topic: **An Industry Perspective on Cyber Security Challenges**

1045 – 1100 Break

1100 – 1230 **Panel Two**: **Policy Challenges in Defending Against Cyber Attacks**
Panel Chair: Mr. Terry Pudas, CTNSP
Panel:
Brig Gen John Davis, Cdr, JTF GNO (*at 1200)
Topic: **Bunkering the .mil Domain Against Unclassified Access**
Mr. Jim Christy, Special Agent (Ret), Dir, Futures Exploration, DoD Cyber Crime Center
Topic: **Power of Digital Forensics**
Dr. Michael Nelson, Georgetown University
Topic: **Sanctuaries on Servers Shared by Legitimate Activities**
Dr. Eneken Tikk, NATO Cyber Center of Excellence
Topic: **Identification of Attack Sources and Attribution Factors**

1230-1400 Luncheon Keynote Speaker:
Introduction: Dr. Hans Binnendijk, Director, CTNSP
Keynote Address: General James E. Cartwright, Vice Chairman, JCS
Topic: **The Potential for Warfare in the Cyber Domain**

1400 – 1530 **Panel Three**: **Critical Cyber Infrastructure Protection**
Panel Chair: Mr. Andy Purdy
Panel:
Mr. William Nelson, President and CEO, FS-ISAC
Topic: **Banking Systems Protection**
Mr. Michael Assante, VP/CSO, N.A. Electric Reliability Corp.
Topic: **Power Grids Systems Protection**
Mr. Brenton Greene, VP, Northrop Grumman
Topic: **Communications Systems Protection**

Ms. Jenny Menna, Acting Director, Critical Infrastructure Cyber Protection & Awareness, DHS
Topic: **Critical Cyber Infrastructure Protection**

1530 – 1700 **Panel Four**: **Potential Thresholds of War in Cyberspace**
Panel Chair: Dr. Dan Kuehl, IRMC
Panel:
Ms. Maeve Dion, George Mason School of Law CIP Program
Topic: **Defining Responses to Cyber Incidents -- Legal Frameworks**
Dr. Gary Sharp, DoD General Counsel Office
Topic: **Potential Acts of War in Cyberspace**
Maj. Gen. Koen Gijsbers (NL Army), ACoS C4I, NATO ACT
Topic: **NATO Cyber Defense Policy**
Mr. Mark Hall, OASD (NII)
Topic: **Drawing a Line in Cyber Sand**

30 April 2009 – Day 2
0820 – 0830 Welcome: Hon. Franklin D. Kramer
0830 – 0900 Keynote Address: Lt. Gen. (Ret) Harry Raduege, Jr., Deloitte & Touche LLP
Topic: **Coalescing International Cyberspace Governance**

0900 – 1030 **Panel Five**: **National Perspectives on: Infrastructure Protection, Cyber Crime and the Potential for War in Cyber Space**
Panel Chair: Dr. Chuck Barry, CTNSP
Panel:
Dr. Itamara V. Lochard, The Fletcher School of Law & Diplomacy
Topic: **A View on Brazil**
Mr. Nandkumar Saravade, Inspector General of Police (Ret), India
Topic: **A View from India**
Dr. James Mulvenon, Defense Group, Inc
Topic: **A View on China**
Dr. Alexey Salnikov, Institute of Information Security, Moscow
Topic: **A View from Russia**
1030 – 1045 Break

1045 – 1215 **Panel Six**: **Institutional/Multilateral Governance Initiatives, Today and Tomorrow**
Panel Chair: Mr. Hal Kwalwasser
Panel:
Prof. Jonathan Zittrain, Harvard Law School
Topic: **The Future of the Internet and Governance**
Mr. Paul Twomey, President, ICANN
Topic: **Global Governance and Cybersecurity**
Dr. Rex Hughes, Director, Cyber Security, Chatham House UK
Topic: **Europe and Cyber Governance, Crime and Security**
Mr. Richard Beaird, Department of State
Topic: **The Future of Governance from a U.S. Perspective**

1215 – 1300 **International Cyber Security: Reflections for the Future**
Concluding Keynote Speaker: Mr. John Grimes, ASD (NII)