Statement of

Michael Greenberger, JD

Founder and Director
University of Maryland Center for Health and Homeland Security
and
Law School Professor
University of Maryland Francis King Carey School of Law

and

Markus Rauschecker, JD

Senior Law and Policy Analyst
University of Maryland Center for Health and Homeland Security
and
Adjunct Faculty
University of Maryland Francis King Carey School of Law

500 West Baltimore Street
Baltimore, MD 21201

before the

**Senate Foreign Relations Subcommittee on
East Asia, the Pacific, and International Cybersecurity Policy**

on

"United States Confidence Building Measures to Respond to Universally Recognized Need for International Cybersecurity Protections"

Thursday, May 14, 2015
Dirksen Senate Office Building, Room 419
10:00am

CHHS
UNIVERSITY OF MARYLAND
CENTER FOR HEALTH &
HOMELAND SECURITY

UNIVERSITY *of* MARYLAND
THE FOUNDING CAMPUS

Introduction

My name is Michael Greenberger. I am the Founder and Director of the University of Maryland Center for Health and Homeland Security (CHHS). I have been assisted in the preparation of this statement by Markus Rauschecker, Senior Law and Policy Analyst at CHHS. I am very pleased to have the opportunity to provide this statement to the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy on the very important topic of "Cybersecurity: Setting the Rules of the Road for Responsible Global Cyber Behavior."

CHHS is an academic consulting institution that provides guidance in planning, training, and exercises relating to the prevention of, and response to, both man-made and natural catastrophes.[1] CHHS consists of over 50 professionals working on over 90 contracts worldwide. Among CHHS' areas of expertise is the law and policy of cybersecurity. We are involved in academic programs[2] and provide advisory services on legal and policy issues relating to cybersecurity.

The Problem

Cybersecurity presents a unique policy challenge given the internet's interconnected global reach and infrastructure. Cybersecurity cannot be ensured through measures based on individual sovereignty or within traditional borders. It is widely recognized that the world-wide scope of the internet makes dealing with the threat of cyber disruption self-evidently international in nature. Solutions to cyber vulnerability are therefore not only substantive in scope, but require international organization, cooperation and response.

[1] More information about CHHS can be found at our website www.mdchhs.com

[2] CHHS is responsible for teaching "The Law and Policy of Cybersecurity" and "Cybercrimes" at the University of Maryland Francis King Carey School of Law; and it has developed cyber specializations for Masters of Science in Law (MSL) and Masters of Law (LLM) degrees.

Unfortunately, the conventional approaches to the solution of other international vulnerabilities do not accommodate themselves to cyberspace. It has been recognized that presently there is not adequate knowledge or agreement on solutions to respond to cyber vulnerabilities, which makes negotiation of effective bilateral or multilateral treaties premature. As our fellow panelist Chris Painter, Coordinator for Cyber Issues at the Department of State, recently stated, the international community is still trying to develop the norms that would be the basis for such treaties.[3]

Disparities in perspectives, as well in the domestic laws of nations in this area, only further complicate the problem. While the temptation exists to find a "silver bullet" response, a global solution of this sort is available neither procedurally or substantively. For example, the oft discussed recommendation of implementing "arms control" in cyberspace is widely recognized as unworkable given the uncertainties in the methods of control.[4] Moreover, it is clear that the problems of cybersecurity not only involve state actors, but private sector actors as well, because much of the world's cyber infrastructure is privately owned and/or operated.

Therefore, the solution cannot be limited to either state actors or private stakeholders alone, but must include a multitude of stakeholders. As the White House has correctly asserted, "the world must collectively recognize the challenges posed by malevolent actors' entry into cyberspace, and update and strengthen our national and international policies accordingly."[5]

While the need for international cooperation to combat cyber threats is widely recognized, it is universally acknowledged that much work needs to be done to promote international solutions. Indeed,

[3] Comments made during a panel discussion at the International Conference on Cyber Engagement 2015, Georgetown University, April 27, 2015.

[4] Christopher Bronk and Dan Wallach, "*Cyber Arms Control? Forget About It*," March 26, 2013, available at http://www.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/

[5] The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, p. 3, available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

enhancing international engagement is a top priority for the Obama Administration.[6] Federal officials are calling for greater international cooperation in cyberspace, with the need being especially evident in the area of cyber crime. For example, national law enforcement agencies need to increase information sharing with international partners to combat international crimes and countries must work together to build up crime fighting capacities.[7]

So, in the face of an overwhelming need and inadequate solutions, the ancient Chinese proverb is apt: a journey of 1000 miles begins with a single step. We therefore advocate that the U.S. State Department lead a cooperative effort working with sympathetic countries and private stakeholders to begin the development of international crisis management protocols and otherwise establish effective norms to combat international cyber vulnerabilities.

The Solution

We endorse the suggestion of prominent cyber experts that a step by step approach should be applied to develop highly recommended international confidence building measures (CBMs) to create an international infrastructure to address cyber vulnerabilities. These CBMs may be created with the support of existing cooperative international entities and private international stakeholder organizations. As a general matter, the United Nations has issued a report endorsing the CBM

[6] See Five Things to Know: The Administration's Priorities on Cybersecurity, available at: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-engage-internationally

[7] "*Federal officials call for more international cooperation in dealing with cyber crimes*," Peninsula Press, February 2014, available at: http://peninsulapress.com/2015/02/14/cyber-crimes-international-cooperation/

approach.[8] But, the most detailed outline or plan for the CBM international approach comes from the Atlantic Council's recent November, 2014 report on this subject.[9]

We agree with the Atlantic Council report's suggestions of the international stakeholders who are likely allies to this U.S. directed CBM approach. It may not be possible to engage each of these stakeholder institutions in the first instance, but we think the U.S. State Department should turn to these organizations to see if it can find significant cooperation on *all* suggested CBM approaches or whether alliances should be formed to address individual recommended CBMs. Whatever approach is taken, the organizing effort must begin promptly. We agree that even if the organizing structure is not "prefect," *i.e*., getting cooperation of all stakeholders, whatever organizing structure that can be assembled will generate by its example and effectiveness greater worldwide support.

As suggested above, the international organizational format must be developed by engaging both sympathetic governmental as well as non-governmental organizations. Examples of international governmental organizations that could promote the CBM approach, would include NATO, the Association of Southeast Asian Nations Regional Forum, the Asia Pacific Economic Cooperation Forum, the Council of Europe, the European Union, the Organization of American States, and the Organization for Security and Cooperation in Europe, each of which has expressed at least a need for international cooperation in this area. Examples of non-governmental organizations that should be consulted include the Internet Society, Internet Engineering Taskforce, and World Wide Web Consortium.

[8] See, "*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*," June 24, 2013, available at: https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf

[9] Healey J., Mallery, J., Jordan, K., and Youd N., *Confidence-Building Measures in Cyberspace – A Multistakeholder Approach for Stability and Security, Atlantic Council*, November 2014, [hereto forth Atlantic Council Report] available at: http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

Additionally, as the Atlantic Council report correctly advises, in cyberspace, important “private-sector actors like the financial system, telecommunications, power grids, and energy infrastructure or critical cybersecurity and information technology companies” must be included in the development of international CBMs.[10] Each of these sectors “has a critical role to play in defending against cyber attacks, so the concept of CBMs must be expanded to include the private sector.”[11]

In its November 2014 report, the Atlantic Council has outlined a series of CBMs in four different areas: 1) Collaboration; 2) Crisis Management; 3) Restraint; 4) Engagement. We agree with each of the recommendations made in the report; however, we would give immediate priority to four measures within the aforementioned areas. These four measures are given priority based on the limited obstacles they face in successful implementation and their relative low funding requirements. We believe that important work has been started in each of these areas we focus upon, yet the full accomplishment of these measures would serve as a backbone to international cooperation and responsiveness.

The four measures we see as priorities are as follows:

1. Promulgating and Implementing Cybersecurity Best-Practices Internationally

   As the cyber threat has grown, many security measures have already been developed to strengthen cybersecurity across sectors. These measures must be better promoted and more widely implemented. Technical regimes may be leveraged to agree and codify best-practices that should be internationally adopted. It is important to note that the international community would not need to establish entirely new practices, but simply

[10] Atlantic Council Report, Foreword.
[11] Atlantic Council Report, Foreword.

adopt and, where necessary modify, existing practices that are generally accepted. Efforts such as the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework[12] provide evidence of best-practices that have been well received internationally across the public and private cyber sectors.

Technical regimes may also be called on to identify the international entities that are already implementing existing best-practices. These findings should be publicized in order to praise entities meeting objectives, but also to demonstrate a lack of compliance by others. Essentially, non-complying entities would be "named-and-shamed" and we believe they would thus be motivated to adopt generally accepted cybersecurity practices.[13]

2. Joint Investigations of Cyber Incidents

The problem of correctly attributing malicious cyber activity is daunting. Determining who was responsible for a cyber-attack is very difficult for many reasons, often including a lack of technical identification capacity. Thus, any international mechanism for collaboration and sharing of identification resources would be highly advantageous.

For this CBM, an international group of technical experts could conduct and oversee joint multinational investigations to determine proper attribution for an attack. These joint investigations will not only foster continued international collaboration on a general level (beyond the specifics of each investigation), but also serve as a deterrent to malicious cyber activity. Malicious cyber activity is often motivated by an attacker's belief that they will

[12] For more information on the NIST Framework, see http://www.nist.gov/cyberframework/index.cfm.
[13] Atlantic Council Report, pages 4 and 16.

remain anonymous. If, however, these proposed joint investigations lead to determinations and methods of attribution, the anonymity is diminished and an attacker may reconsider their intended action.[14]

3. Promoting Collaboration and Communication of Cyber Crisis Response Teams

Given the international scope of cyberspace and cyber vulnerabilities, cyber crisis response teams must be able to quickly and securely communicate with their counterparts in other countries. Interstate and multinational mechanisms must exist for cyber crisis response teams to quickly communicate and share situational awareness. Communication must not only be between state actors, but must also include private sector entities. Basic contact lists and data sharing protocols are part of establishing this CBM.[15]

To test these communications capabilities, periodic exercises should be conducted. [16] At CHHS, we have conducted hundreds of emergency exercises for our clients. Not only do exercises provide a strong foundation to enable effective responses to real crises, but it is our experience that working through exercises establishes bonding connections among responders that serve to reinforce cooperative relationships and responses.

[14] Atlantic Council Report, p. 4.

[15] Atlantic Council Report, p. 7.

[16] Atlantic Council Report, p. 8.

4. Establishment of a Norm to Restrict Certain Targets from Cyber Attack

International law establishes critical cyber targets to be focused upon for protection from attack. This proposed CBM would develop an international norm that on which parts of the cyber infrastructure need heightened protection from attack. As the Atlantic Council states, "the desired end-state of this CBM would be the acceptance of restrictions, akin to those contained in [international humanitarian law] rules, on disruptive attacks on specific assets and entities during peacetime – including but not limited to Internet backbone, major IXPs, finance, aviation, and undersea cables – that would aim to prevent the 'breaking' of the Internet."[17] International actors should collaboratively develop a common understanding of what constitutes critical cyber infrastructure and how those assets should be granted heightened protected status from malicious cyber activity.[18]

Starting on this path of CBM development, allows for a steady progression towards greater stability and security. If these CBM steps are effective and successful, others in the international community will not only adopt the norms established, but likely join in the establishment of the norms. As stated earlier, the U.S. should not wait to establish the perfect international cyber protection organization. It should quickly do what it can on an international basis and rely on successes to further develop international solutions.

No legislation needed

Finally, we believe that the recommendations we are making do not require (indeed may not lend themselves to) legislation; nor do they require anything other than *de minimis* appropriations. We

[17] Atlantic Council Report, p. 13.
[18] Atlantic Council Report, p. 13.

see aggressive congressional oversight of relevant U.S. international agencies as the best method of starting and effectively implementing solutions recommended herein. As to the individual recommendations above, the Atlantic Council emphasizes, and we agree that funds for implementation would be *de minimus*.