Multilateral Approaches for Improving Global Security in Cyberspace

Robert J. Butler and Irving Lachow

INTRODUCTION

Effective cyber security requires that national governments, private companies, and non-governmental organizations work together to understand threats in cyberspace and to share information and capabilities for mitigating those threats. This is necessary because cyberspace is an interconnected environment that provides tremendous benefits to nations, organizations and individuals. Unfortunately, this environment is also a haven for criminals, terrorists, and other actors whose intentions could undermine the value of the cyberspace commons for the majority of its users. If like-minded actors fail to understand and mitigate these risks, they are placing national and economic security in jeopardy.

Global security in cyberspace is predicated on nations coming together with like-minded will, intent, and capabilities to defend against common threats. This article will explore how multilateral approaches can be applied to the cyber security challenge.[1] It begins by describing the importance of principles and norms for building a common understanding of goals, terms and concepts. The article then identifies the key players that must participate in a multilateral framework. Although nation states are the principal actors in our proposed approach, businesses, political and military alliances, and international organizations must all play a role in securing the international cyber ecosystem. Our paper addresses the strengths and challenges that each player brings to the table, and ends with a summary of our findings.

PRINCIPLES AND NORMS

Governments, business, and individuals all derive enormous benefits from cyberspace. While cyberspace is generally a safe "commons," it does contain a number of actors who pose a threat to the well-being of others. Such threat actors include, but are not limited to, nation-state intelligence services, militaries of potentially hostile countries, criminals, terrorists, and "hacktivists" (e.g. Anonymous). The United States has recognized these potential threats as a challenge to its national security and has publicly declared its right to defend itself in cyberspace.[2] However, acting alone is not sufficient. The International Strategy for Cyberspace, released by the White House in May 2011,

makes it clear that, "the world must collectively recognize the challenges posed by malevolent actors' entry into cyberspace, and update and strengthen our national and international policies accordingly."[3] Other nations have expressed similar views. For example, British Foreign Minister William Hague recently stated that, "the constant evolution of cyberspace is introducing additional complexity to foreign affairs. The same digital means that are bringing hope and opportunity to millions around the world and fueling change in the Middle East also empower terrorists, criminals and some states with new means of attack and organization….In this period of uncertainty and turbulence it is important that our foreign policy ranges further afield to look for new partners and to tackle global challenges."[4]

Multilateral actions require a common understanding of terms, goals, responsibilities, and acceptable behaviors. At the state level, principles for behavior in cyber space are defined both by traditional statecraft and by emerging cyber-specific guidelines. For example, the U.S.'s International Strategy for Cyberspace describes several traditional principles of interstate conduct that lay the foundation for behaviors in the cyber realm:[5]

- Upholding fundamental freedoms;
- Respect for property;
- Valuing privacy;
- Protection from crime; and
- Right of self-defense.

The adoption of these principles provides a foundation for common understanding and the potential for multilateral security in cyberspace. It also lays the building blocks for the development of effective public-private coalitions whose actions can improve the security and health of cyberspace. Principles and norms set the stage for nations to establish declaratory policies on what is acceptable and not acceptable in the global commons that is cyberspace.

Although many nations agree on several basic principles of cyberspace, such as those found in the European Convention on Cybercrime, there is also some disagreement about basic tenets underlying behaviors in cyberspace. For example, "governments in Russia and China see internal dissent and anti-government writings disseminated on the Internet as a threat. Both have curtailed free speech

and access to the Internet as part of their vision of 'cyber security.'"[6] Like-minded nations need to encourage other countries to adopt widely accepted principles that support fundamental freedoms and condone criminal actions while being prepared to counter demurring nations if encouragement fails.

While cyber principles and norms provide a good starting place for behavior at the nation-state level, they are not explicitly designed to address the actions of corporations and other private sector actors. However, businesses are frequent targets of both cybercrime and cyber espionage and some of them are growing increasingly capable of responding to such threats either directly or indirectly. For example, Microsoft has demonstrated both the means and the will to take down botnets associated with popular malware such Zeus and SpyEye.[7] New companies are being created for the explicit purpose of taking active steps to defend organizations from cyber threats.[8] In this context, it is important to consider the development of norms for businesses.[9] For example, General Michael Hayden, former Director of the CIA and NSA, has stated that "we may come to a point where defense is more actively and aggressively defined even for the private sector and what is permitted there is something that we would never let the private sector do in physical space."[10] Further, there is the issue of coordination between private and public sector actors. While businesses have the right to defend themselves, private sector actions should not encroach on the legitimate powers and roles of governments without both a clear mandate and legal guidelines that delineate acceptable behavior.[11]

Government actions, however, have the potential to undermine the functioning of the cyber security marketplace, and could possibly even decrease the ability of private sector organizations to defend themselves. For example, assume that a large and sophisticated corporation has developed outstanding intelligence on the behaviors of certain malicious actors. If the government were to deploy a capability that blocked malware emanating from those actors but did so without informing the company in question, the company might detect a change in the actors' behaviors but would not understand why the change had occurred. The corporation in question might take actions assuming that the malicious actors' techniques had changed because they did not know that the government had blocked the malware.[12] This could end up reducing the security posture of the corporation, increasing its costs, or both.

In sum, there is a need to begin developing principles and norms that can create a framework for coordinated multilateral action between states and across public and private sectors. This framework will need to define the proper roles of both public and private sector actors within and across national borders. In the following sections, we examine who these actors are and what short-term actions they can take to foster greater coordinated cyber security actions.

KEY ACTORS

Nation states both alone and through public-private partnerships (PPPs), political and security alliances, and international bodies all play a critical role in global cyber security. This section will explore the specific roles that each of these organizations can and should play on the global stage.

Nation States

Nation-states must take the lead in promoting greater security in cyberspace because they are the main actors for motivating, if not mandating, coordinated security actions. National champions on the international stage are needed to drive agendas, set examples, and educate others with less experience. In order for multilateral cyber security to work, each participating state needs to start by developing and exercising its own unifying national framework for cyber defense. These frameworks must ensure continuity of operations across military, civilian, and commercial networks that are critical to national well-being. Without such a framework, a given nation will find it difficult to coordinate with other actors in the international cyber ecosystem.

In addition to developing a unifying framework, each nation must identify a government organization that is responsible for coordinating its national cyber defenses. This lead organization must be able to coordinate actions both across government entities and between the government and private sector. In addition, the organization must be empowered to quickly coordinate response actions and develop mitigation strategies for parties that are facing concerted cyber attacks. Finally, each nation should provide its lead cyber organization with the necessary legal authorities it needs to conduct its mission.

With authorities in place, national cyber leads need to efficiently and effectively build cyber defense coordinating and synchronization activities around the best technical capacities of the country. National cyber leads must maintain an inventory of national cyber defense capabilities and determine

the best way to align and leverage these capabilities for the betterment of the nation. Further, each country's cyber strategy should be developed with the understanding that nation states, corporations, and international organizations all play a critical role in collective cyber security for the globe. An example of this approach is found in the Dutch Cyber Strategy, which lays out a well-constructed plan for using both public and private sector assets to tackle the cyber security challenge.[13]

The Dutch Strategy begins by describing a series of basic principles:

- Linking and reinforcing initiatives;
- Public-Private partnership;
- Individual responsibility;
- Division of responsibility between departments;
- Active international cooperation;
- Proportionate measures (balancing security and fundamental rights);
- Self-regulation if possible, legislation and regulation if necessary.

To implement these principles, the Dutch government proposes the creation of a Cyber Security Board, comprised of representatives from both private and public sector stakeholders, that reports directly to the Cabinet. They also call for the creation of a new Cyber Security Centre to leverage the "information, knowledge, and expertise" both public and private parties in order to gain insights into "developments, threats and trends." Finally, the Dutch strategy focuses on several key initiatives and identifies the organization(s) responsible for each effort:

- Preparing threat and risk analyses;
- Increasing the resilience of vital infrastructures;
- Improving the capacity to withstand and respond to information and communications technologies (ICT) disruptions and cyber attacks;
- Intensifying investigation and prosecution of cyber crime;
- Stimulating research and education.

Because the majority of cyberspace infrastructure resides in the private sector, nations must develop robust partnerships with businesses, including (but not limited to) Internet service providers (ISPs), software and hardware vendors, managed security service providers, and owners/operations of

critical infrastructures. We will provide three examples of such partnerships: two from the United States and one from Australia.

First, the PPP between the U.S. Department of Homeland Security (DHS) and the Defense Industrial Base (DIB) illustrates how a government can work with ISPs to improve the cyber security posture of a specific infrastructure sector (in this case, the DIB). This PPP began as a Department of Defense pilot that explored how the U.S. government could share threat information with ISPs who could in turn use that information to better protect DIB companies that chose to participate in the experiment. The initial success of the pilot led to formalization of the program, which is now led by DHS. The program is expected to add many more participants and possibly service as a model for other infrastructure sectors.[14]

A second example is a U.S. government-industry partnership to combat botnets. The White House, the Department of Commerce, and DHS are working with the Industry Botnet Group, which represents thousands of companies across the information, communications, and financial services industries, to identify botnets and minimize their impacts on personal computers.[15] This PPP includes initiatives, such as:

- A framework for shared responsibility across the botnet mitigation lifecycle from prevention to recovery;
- A pilot program between the Financial Services Information Sharing and Analysis Center, DHS, and the Treasury Department to share information about botnet attacks;
- An education campaign for consumers supported by DHS, the Federal Trade Commission, the National Cybersecurity Alliance, and several companies;
- Improved information sharing between the FBI, the Secret Service and companies to shut down massive criminal botnets.

A third example is the Australian Internet Security Initiative (AISI). This public-private partnership between the Australian Communications and Media Authority and over 127 organizations, including numerous ISPs, is focused on combating the threat from infected computers:

> The AISI collects data from various sources on computers exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to internet service providers (ISPs) identifying IP addresses on their networks that have

> generally been supplied to the ACMA in the previous 24-hour period. ISPs can then inform the customer associated with that IP address that their computer appears to be compromised and provide advice on how they can fix it.[16]

There are certainly other examples of PPP worth mentioning, but we believe that the three efforts cited here illustrate the level of cooperation that is needed to combat the advanced threats facing the world's nations.

Political and Security Alliances

While nations must develop their own unifying frameworks for coordination of cyber authorities and capabilities, the lead cyber organization in each nation must work with counterparts in other countries to develop a mutual understanding of the authorities, capabilities, and national will that are required to enable coordinated action in cyberspace. This knowledge enables national leads to better understand how to align policies and capabilities within their own country, and it provides a means for each country to define its comparative advantage within the international cyber ecosystem. The need for such cooperation is evident in the priorities that different countries place on various threats. For example, "Germany has determined that botnet infestation of its private infrastructure is a priority for national defense….On the other hand, the United Kingdom has determined the data breaches caused by crime and espionage are its highest priority."[17] The differing priorities of these two countries are leading them to focus on policy and capability development in different areas. If one begins to consider the varying priorities of additional countries, the picture grows increasingly complicated and the need for coordinated action becomes even more apparent.

There is clearly a need for nations to develop a baseline understanding of common threats and capabilities to enable coordinated actions. Formal political and security alliances, such as NATO and ASEAN are one way to achieve that end. On the plus side, such alliances are at least theoretically designed to strengthen the collective security of their members: "Under the presumption that the mission and infrastructure of NATO primarily exist for the purpose of supporting international peace and security, NATO as an organization is in a good position to develop and apply security measures in the case of a [cyber] relevant threat or attack."[18] Indeed, NATO has taken important steps to develop its cyber capabilities, including the creation of a cyber defense center of excellence, the development of a rapid reaction team to assist member states in the event of a significant attack, and the creation of a cyber exercise "designed to give its participants a better understanding of

NATO's Cyber Defense capabilities and to identify areas for improvement within the NATO-wide Cyber Defense community."[19]

On the other hand, there are many reasons why it is difficult for large alliances to develop coherent policies and advanced operational capabilities, starting with the fact that reaching consensus among large numbers of states is challenging in the best of circumstances.[20] ASEAN has done little more than call for the development of a cyber strategy.[21] NATO has taken many steps in the right direction, but its overall capabilities for taking decisive action across the alliance are still limited. Alliance leaders and member nations must increase their knowledge of the threats they face and the capabilities they need to respond to those threats. They must also inventory their collective cyberspace capabilities, and update their organizational structures and processes to enable effective employment of these capabilities. It is important to exercise these processes to identify what works, what doesn't work, and to foster a culture of continuous improvement. Finally, alliance members need to reach a common position on how they are going to deal with complex issues such as cloud computing and information sharing that involve technical, legal, and political aspects.[22] While reaching a consensus on these issues may be difficult, alliances are going to have to operate in a world filled with these technologies – the only question is whether they will decide to respond to the challenge effectively.

Other International Organizations

There are a large number of governance and standards organizations that play a key role in the cyberspace ecosystem, including but not limited to: the International Telecommunications Union (ITU), the International Criminal Police Organization (INTERPOL), the International Multilateral Partnership against Cyber Threats (IMPACT), the European Commission and the European Network and Information Security Agency (ENISA), and technical groups like the Internet Engineering Task Force (IETF). If they wish to participate in multilateral efforts to secure cyberspace, these organizations must define and deconflict their roles and responsibilities so that each specific body contributes its strengths to the broader coalition. In general, roles should be sorted out based on organizational charter and recognized competency to contribute in positive ways to international cyber security.

For example, one area where international organizations can play an important and unique role is in the development and promulgation of standards. Standards can provide guidance on best practices, they can establish metrics by which to assess performance, and they can enable coordinated action by creating agreed-upon lexicons for the sharing of information. Standards can focus on cyber security practices or they focus on technical aspects. Examples of the former include ISO 27002, NIST guidelines, and the *Standard of Good Practice* published by the Information Security Forum. Examples of the latter include the Common Vulnerabilities and Exposures (CVE) dictionary, the Incident Object Description Exchange Format (IODEF), the Secure Content Automation Protocol (SCAP) and the Structured Threat Information eXpression (STIX).[23] Finally, standards for privacy of personal information need to be developed and normalized across nations. For example, privacy laws in the EU and the United States do not always agree in their views of personal information and corporate access to that information.[24]

Other actions that can be taken by international organizations include the development and expansion of legal frameworks for reducing cybercrime, such as the European Convention on Cybercrime, clarification on how international law applies to cyber warfare,[25] and agreement on the global responsibilities of private sector actors, such as Internet service providers.[26]

CONCLUSION

In summary, we advocate a call for greater multilateral action to improve cyber security across the globe. First, like-minded nations should agree on a common set of principles and norms that can enable coordinated action. These guiding concepts need to be developed in a public-private sector partnership that balances privacy, security, and economic livelihood.

Second, nations must develop their own unifying frameworks for cyber defense. A state cannot function effectively in a coordinated manner on the global stage if its own house is not in order. In addition, each nation must identify a lead agency for cyber security, align authorities to that lead, and provide sufficient resources to enable the organization to achieve its mission.

Third, in an increasingly interconnected world, we must realize that norms, national policies, and national frameworks for cyber defense are necessary, but not sufficient. We must go to the next level by linking national plans to coalition planning, exercises, and greater understanding of coordinated

security in cyberspace. These efforts must leverage political and military alliances as well as international organizations (governmental ones and non-governmental ones). They may include activities focused on military, legal, political, economic, and technical aspects of cyber security. We will draw new lessons from these actions that will enhance our ability to share information and act in a coordinated manner at the coalition level while fostering further development of policy and capability delivery within our respective nations. This will begin to change the cyber playing field from one dominated by offensive-minded adversaries to one based on mutually assured defenses.

---

[1] Multilateralism can be defined as "the practice of coordinating national policies in groups of three or more states through ad hoc arrangements or by means of institutions." See Keohane, Robert O. "Multilateralism: An Agenda for Research." *International Journal*, Vol. 45, No. 4 (Autumn 1990), 731

[2] "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, Internet, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (date accessed: 20 August 2012). (hereinafter International Strategy for Cyberspace).

[3] International Strategy for Cyberspace, p.3.

[4] Dave Neal, "William Hague Rings the Cyber Attack Alarm, Again," *The Inquirer*, November 17, 2011 Internet, http://www.theinquirer.net/inquirer/news/2125649/william-hague-rings-cyber-attack-alarm (date accessed 10 June 2012).

[5] See International Strategy for Cyberspace, p. 10.

[6] Martha Finnemore, "Cultivating International Cyber Norms," *America's Cyber Future: Security and Prosperity in the Information Age*, Kristin M. Lord and Travis Sharp, eds., June 2011, p. 89, Internet, http://www.cnas.org/cyber (date accessed: 20 August 2012).

[7] See "Microsoft Takes Down Dozens of Zeus, SpyEye Botnets," 26 March 2012, BLOG POST, Internet, http://krebsonsecurity.com/2012/03/microsoft-takes-down-dozens-of-zeus-spyeye-botnets/ (date accessed: 20 August 2012), and Nick Wingfield and Nicole Perlroth, "Microsoft Raids Tackle Online Crime," *New York Times*, 26 March 2012, Internet, http://www.nytimes.com/2012/03/26/technology/microsoft-raids-tackle-online-crime.html?_r=2&pagewanted=1# (date accessed: 20 August 2012).

[8] See Kelly Jackson Higgins, "Startup Targets the Attackers behind the APT," *Security Dark Reading*, 28 February 2012, Internet, http://www.darkreading.com/advanced-threats/167901091/security/news/232601696/startup-targets-the-attackers-behind-the-apt.html (date accessed: 20 August 2012).

[9] The US Federal Communications Commission and the new US Industry Botnet Group, among others, could be good focal points for coordinating this type of action.

[10] Desire Athow, "Former NSA & CIA Director Suggests Employing Mercenaries for Cyberwarfare," ITProPortal, 1 August 2011, Internet, http://www.itproportal.com/2011/08/01/former-nsa-cia-director-suggests-employing-mercenaries-cyberwarfare/ (date accessed: 20 August 2012).

[11] The U.S. Constitution provides for letters of marquee. In this context, it could be appropriate to have private sector actions in cyberspace approved by the government.
[12] We are grateful to Gary Gagnon, Chief Security Officer and Senior Vice President at the MITRE Corporation for providing this scenario.
[13] European Network and Information Security Agency (ENISA), "Dutch Cyber Security Strategy 2011," Internet, http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011/view (date accessed: 20 August 2012).
[14] Amber Corrin, "DoD to Expand Public-Private Cybersecurity Project," *Federal Computer Week*, April 25, 2012, Internet, http://www.fcw.com/articles/2012/04/25/DOD-expanding-DIB-cybersecurity-pilot.aspx?p=1 (date accessed: 20 August 2012).
[15] Press release, "White House Announces Public-Private Partnership Initiatives to Combat Botnets," 30 May 2012, Internet, http://www.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b (date accessed: 21 August 2012).
[16] Australian Internet Security Initiative, Internet, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 (date accessed: 20 August 2012).
[17] Melissa Hathaway, "Toward a Closer Digital Alliance," *The SAIS Review of International Affairs* 30, no. 2 (Summer-Fall 2010): 21-31.
[18] Eneken Tikk, "Global Cyber Security-Thinking About the Niche for NATO," *The SAIS Review of International Affairs* 30, no. 2, (Summer-Fall 2010): 105-119.
[19] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, "Cyber Defence Exercises," Internet, http://ccdcoe.org/215.html (date accessed: 20 August 2012).
[20] Other factors could include policy or legal roadblocks, differing priorities, funding issues, a lack of personnel with the right skill sets, and many others.
[21] For example, see Wendell Minnick, "Malaysia calls for ASEAN 'Master Plan' to Fight Cyber Attacks," *Defense News*, 3 June 2012, Internet, http://www.defensenews.com/article/20120603/DEFREG03/306030004/Malaysia-Calls-ASEAN-8216-Master-Plan-8217-Fight-Cyber-Attacks (date accessed: 20 August 2012).
[22] For example, see Bob Butler, "Personal Devices in the Workplace: Advantage or Risk?" *SafeGov*, Internet, http://safegov.org/2012/6/14/personal-devices-in-the-workplace-advantage-or-risk (date accessed: 27 June 2012).
[23] We strongly support the move towards information sharing focused on threats because we believe it can enable rapid and coordinated action across multiple organizations. For more information on this standard, see MITRE, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression*, (McLean, VA, 2012). http://measurablesecurity.mitre.org/docs/STIX-Whitepaper.pdf (date accessed 24 August 2012). For further information on the topic of information sharing, see MITRE, *Information Sharing Models: An Overview*, 11-4486, (McLean, VA, 2011).
[24] Bob Sullivan, "Privacy Lost: EU, U.S. Laws Differ Greatly," *MSNBC*, 19 October 2006, Internet, http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.UDOj_90iZic (date accessed: 21 August 2012).
[25] The *"Tallinn Manual" on the Applicability of International Law to Cyber Warfare*, a book sponsored by the NATO Cooperative Cyber Defense Centre of Excellence, is currently in draft. It will be published by Cambridge University Press in 2013.

[26] A detailed discussion of the ISP issue can be found in Melissa E. Hathaway and John E. Savage, "Stewardship of Cyberspace: Duties for Internet Service Providers," March 2012, Internet, http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hathaway-savage.pdf (date accessed: 21 August 2012).