CYBERPOWER AND NATIONAL SECURITY

NATIONAL COMMITTEE ON AMERICAN FOREIGN POLICY

SUMMARY OF A ROUNDTABLE

(Including Policy Observations)

HELD IN
NEW YORK CITY

October 17, 2012

Our Mission

The National Committee on American Foreign Policy (NCAFP) was founded in 1974 by Professor Hans J. Morgenthau and others. It is a nonprofit activist organization dedicated to the resolution of conflicts that threaten U.S. interests. Toward that end, the NCAFP identifies, articulates, and helps advance American foreign policy interests from a nonpartisan perspective within the framework of political realism.

American foreign policy interests include:

- preserving and strengthening national security;
- supporting countries committed to the values and the practice of political, religious, and cultural pluralism;
- improving U.S. relations with the developed and developing worlds;
- advancing human rights;
- encouraging realistic arms control agreements;
- curbing the proliferation of nuclear and other unconventional weapons;
- promoting an open and global economy.

An important part of the activity of the NCAFP is Track I½ and Track II diplomacy. Such closed-door and off-the-record endeavors provide unique opportunities for senior U.S. and foreign officials, think-tank experts, and scholars to engage in discussions designed to defuse conflict, build confidence, and resolve problems.

Believing that an informed public is vital to a democratic society, the National Committee offers educational programs that address security challenges facing the United States and publishes a variety of publications, including its bimonthly journal, *American Foreign Policy Interests*, that present keen analyses of all aspects of American foreign policy.

CONTENTS

Letter From The President

Dear Reader,

Cyber warfare, a man-made theater of combat in contrast to the four natural domains—land, sea, air, and space—debuted in 2007, when Estonia's Internet infrastructure was attacked and overwhelmed. In 2008, a U.S. Department of Defense laptop was infected by malware that overwhelmed much of the Department's unclassified military network. This attack was followed in 2010 by, among other attacks, the Stuxnet assault—which played havoc with Iran's centrifuge programs. The rapidly mounting attacks that emanate from state and non-state actors led U.S. Secretary of Defense Leon Panetta to warn in October 2012 that we may face a "Cyber-Pearl Harbor."

At present, the United States is in the fortunate position of being relatively well-prepared to withstand cyber attacks on our infrastructure and enjoys effective retaliatory abilities to use against aggressors. But the advantages we now enjoy are sure to erode.

As this new domain of warfare is surely a jungle, the goal is to reach agreements on norms and treaties for regulating the maze of cyberspace. In the meantime, the United States would be well-advised to further develop effective defensive and offensive capabilities. Toward that end, enlisting the help of our private sector and coordinating policies with friends and allies is a must. The National Committee on American Foreign Policy has also learned from experience the necessity of engaging adversaries.

I thank the presenters at this closed-door and off-the-record roundtable on "Cyber-power and National Security," The Honorable Franklin D. Kramer, Lt. Gen. Harry D. Raduege, Jr. (USAF, Ret.), Marcus H. Sachs, and Dr. Adam Segal. This roundtable could not have taken place without the support of Mutual of America and the hard work of Ms. Edythe Holbrook, Ms. Camino Kavanagh, and Mr. Igor Kharkov.

Sincerely,

George D. Schwab

George Schwab

Cyber-related Challenges: Implications for American Foreign Policy, National Security & Sovereignty

The first speaker focused on the nature of the cyber problems that have emerged, giving particular attention to the strategic threats posed by cyber espionage and threats to critical infrastructure and highlighting the types of domestic and international responses needed to deal with these problems.

The Attack Problem

The first speaker outlined the main problems that have emerged in relation to cyber, including problems related to privacy, free speech, crime, espionage, and critical infrastructure. He noted that the national security area faces two main problems: the espionage problem and the attack problem. There are also several types of attacks: remote attacks (e.g., the Chinese attacks on Google and scores of other U.S. companies in 2010 and the more recent Night Dragon attacks on oil and gas companies); near-end attacks (e.g., the Stuxnet attack on Iranian nuclear centrifuges or attacks on U.S. classified systems, some of which date back to 1998); insider attacks (e.g., Wikileaks or the recent insider attacks on the Saudi Aramco oil company that wiped the data from 30,000 computers); supply-chain attacks (e.g., the infecting of software at the production stage so that a computer is automatically conscripted as a "Botnet" without the owner's knowledge).

Secretary of Defense Leon Panetta's recent speech focused sharply on the attack problem, particularly the risk that certain attacks could bring down U.S. critical infrastructure with huge consequences for U.S. national security.[1] In reality, however, evidence that this type of attack has occurred or that it will occur is limited. A major attack would be evident. Indeed, if the United States were subjected to a major attack, the attack would manifest itself in a range of ways and different vulnerabilities would be exploited. A major cyber attack would most likely be associated with a kinetic attack, and it would occur under a set of geopolitical circumstances that would signal that something major was under way. In this regard, the speaker stressed the importance of understanding the scenario, understanding signals, and understanding the circumstances under which a major attack might occur as an effective means to implement appropriate preventive measures.

Attribution has been an important problem. At the same time, however, media and state officials are increasingly attributing attacks to different countries (for example, the recent attacks on the Bank of America were attributed to Iran, while a recent intelligence report placed Russia and China at the center of economic espionage attacks). Greater certainty about the perpetrators of attacks can help in terms of de-escalation and deterrence.

Non-state actors such as terrorists pose a different set of challenges. For the most part, important terrorist groups do not currently have the capability to

[1] See: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all

conduct a major attack against the United States. They can, however, hire criminal networks that do have the capacity to develop sophisticated capabilities. Recent testimony by the Department of Justice laid bare how terrorists have, in effect, attempted to seek the support of criminal groups to develop sophisticated cyber capabilities.[2]

The speaker stressed that if this is the landscape—different types of attack capabilities, with countries and people who might want to use them against the United States, a country that, because of its dependence on cyber, is extremely vulnerable to attack—a set of interdependent responses needs to be developed. These responses would require the participation of a broad range of actors from the public and private sectors and from the technical, political, diplomatic, economic, and security spheres; they would require strategic decisions on how to take advantage of capacities and capabilities that are already available; such responses would also require a significant amount of work at the international level with both allies and adversaries.

Building Resilience

On the technical side, the speaker stressed the importance of developing resilient systems and opening up the space for cooperating with like-minded nations. In building resilience, separating the different types of problems is important. While protection of intellectual property is important, once it is done, it is done. In comparison, protecting operating systems or critical infrastructure is much more complex and requires building resilience into the systems. If an electricity grid is brought down through an attack, significant effort needs to be made to keep it down because electricity grids have built-in protection to handle blackouts. Significant capabilities, including insider intelligence, would be needed to bring down and keep down an electricity grid. Hence, in entering into conflict with an adversary, what is critical is to keep all or most systems operating at a minimal level. For this, system resilience is required.

The speaker noted that a range of actions can be taken to build resilience into systems. For example, the Australians launched a campaign entitled "Top 4 Mitigation Strategies to Protect Your ICT System," which includes patching systems as soon as they have been attacked.[3] This, however, presents its own set of problems, not least because those who run the electrical grid need to maintain a lot of reliability; before they patch the system, they need to make sure they don't undermine the reliability of the rest of the system. Rather than the 48 hours suggested by the Australians, reliably patching an electrical grid while maintaining the integrity of the system might take up to one month. Solving this timing issue remains a significant challenge. Other technical solutions include integrity checks—making sure your system is good, that it meets standards, and that it is checked periodically.

[2] http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

[3] The Top 4 mitigation strategies referred to are: i) Patching systems; ii) restricting administrative privileges; iii) application white-listing; and iv) creating a defense in-depth system. See www.dsd.gov.au/publications/Top 4 Mitigation Strategies to Protect Your ICT System.pdf.

The main problem with technical efforts to build resilience is that they have not been brought together under an architecture that really makes them work. There is no one set of standards providing guidance to companies on how they ought to pull together existing capabilities or that highlights the capabilities that could be made available through R&D. In this regard, an important question is who should be setting these standards, government, industry, or a combination of both.

Public-Private Partnerships for Standard Setting

The speaker referenced the legislative package that is pending approval in Congress, suggesting that rather than covering the 18 critical infrastructures as the current package does, a more strategic approach would be to prioritize efforts. The focus could perhaps be on developing standards for core critical infrastructure such as the electricity grid, telecommunications, financial, and transportation systems, and then gradually develop standards for the remaining infrastructure. Standard development should involve the private sector, not just because they "own" the systems, but also because they have the expertise and the access to much operational information that the government may not. Companies like Verizon and other Internet service providers (ISPs) can observe a lot of irregular activity on their systems, but they do not have the authority to do much about it. It may well be the case that they should not operate without government involvement or approval—for example, should private companies be permitted to enter into somebody's server to clean out viruses or attack vectors? Or, how far outside their own borders can the private sector, the military, or the police work? Agreement on "rules of engagement" is urgently needed. In short, public-private partnerships for the development and adoption of standards that continue to foster innovation, and are flexible enough to be adapted when necessary, are crucial.

Working with Like-Minded Nations

The speaker stressed the importance of working at the international level, suggesting the establishment of a group of like-minded countries that draw in strategic decision makers from the public and private sectors to develop standards and build operational capacities. He noted that such a body could be developed along the lines of the voluntary Financial Stability Board—which emerged from the Basel agreements.[4] A "Cyber Stability Board" could focus on standard-setting and could initially include countries that have a tradition of working together such as the United States, the U.K., Canada, Australia, France, Germany, the Republic of Korea, and Japan. In the absence of such a body, the current ad hoc approach will continue, and the involvement of institutions that are not well-suited to deal with the current set of problems will increase.

Working with Non-Like-Minded Nations

The speaker also emphasized the importance of working with non-like-minded countries, China and Russia, for example, on issues of strategic

[4] The Financial Stability Board (FSB) was established to coordinate, at the international level, the work of national financial authorities and international standard-setting bodies and to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies in the interest of financial stability. See: www.financialstabilityboard.org

import such as economic and industrial espionage. Since these are sensitive issues, seeking common ground on issues of mutual concern such as terrorism or cyber crime is important. At the same time and despite the launching of formal diplomatic processes and Track I½ and Track II processes with Russia and China, agreement even on these less-sensitive issues is a long way off, with much work remaining to the done.

The Importance of Sovereignty

The speaker noted that it is also important to elevate current thinking on questions of sovereignty and cyber to the international level. For example, if enough evidence exists that a country, individual, or group of individuals is engaged in cyber espionage, the United States could use approaches that are common in the public health arena. For example, during an outbreak of SARs, people are placed in quarantine and borders become important. The speaker questioned whether this is something that could be applied to cyber—i.e., placing those who propagate viruses in quarantine. He also cautioned that such a move would require congressional approval and would most likely spark controversy and be contested since freedom of expression would be curtailed as would the free flow of information. The speaker also suggested that thought be given to the possibility of promoting a cyber sanctions regime, similar to the counterterrorism and non-proliferation sanction regimes. Such cyber sanctions would give the president the authority to issue sanctions against persons, companies, or governments that use cyber as a means of "attacking" the United States.

The Importance of Strategy

On a final note, the speaker observed that while many of these attacks happen via cyber, it is improbable that a major attack on the United States would elicit a cyber response. Rather, a more strategic approach would need to be employed. Such an approach would place the protection of the U.S. economy (not just individual companies and agencies) at its center. It would include diplomatic, economic, kinetic, and cyber efforts. It would focus on strengthening domestic capabilities and capacities, working with other countries to develop standards, and working internationally to find common interests with adversaries.

❖

WHY INTERNET GOVERNANCE MATTERS

The second speaker presented on the history of Internet governance, shifting trends, the increasing interests of states in governing the Internet, and the risks that this poses to the current model of Internet governance.

The second speaker began his presentation by clarifying the distinction between the Internet and cyberspace, noting that the general tendency is to conflate the two terms. While the Internet is part of cyberspace, there is a lot more to cyberspace than just the Internet. For example, radar systems, air traffic control systems, inter-banking networks are not part of the Internet, but they are part of cyberspace. The Internet is what individuals interface with most and has been the main growth area over the past two decades.

The Current Model of Internet Governance

The speaker's presentation focused mainly on Internet governance rather than the broader concept and reality of cyberspace. He touched on the origins of the Internet and how it developed from experiments, originally within the Defense Advanced Research Projects Agency (DARPA; ARPANET). He stressed that what is often forgotten is that the technology underlying the Internet, the actual protocols and the software—what makes the Internet work—have their roots in the 1970s and have remained largely unchanged. Indeed, the code that we use to inter-operate, e.g., the protocols that allow Verizon to talk to AT&T, British Telecom, China Telecom, etc., the protocols that allow us to use Google, YouTube, etc., are more than 35 years old. While some new protocols have been developed, the basics of the Internet remain the same. The Internet arose from academic research and experimentation. The governing model that underpinned the original Internet reflected its experimental nature.

The same experimental, academic-based governing model is in force today. However, the question of whether we want the Internet to remain an experiment forever is gaining significant traction. The alternative would be to "lock it down" through standards and regulation, but this might inhibit flexibility, innovation, and learning from experimentation. At the same time, the current loose technical standards pose risks, as they allow for malicious behavior and permit criminals and spies to take advantage of the lack of security. Hence, significant tension has emerged between openness and innovation and security.

The speaker highlighted the fact that older parts of cyberspace have already been locked down via standards and regulation. For example, the world of telephony has been "locked down" since the 1950s when agreement was finally reached on voltage levels, frequencies, rates, tariffs, and tolls between countries that exchange phone calls. The same process occurred earlier with the telegraph and radio. Today's Internet is not really like the telegraph, the radio, or telephones. Nonetheless, there are increasing calls to apply these old regulatory models to the Internet, subjecting the Net to trade agreements and rules—old thinking of taxation and boundaries. This frustrates users as the Internet tends to be governed by the people who use it—people choose what they want to do on the Internet and do not look to governments to control or limit their capabilities.

The speaker noted that the question of personal choice and personal freedoms is making countries with authoritarian tendencies nervous, especially since the Internet can empower citizens. Other nations embrace the Internet and related freedoms. But even in the United States, indecision is increasing about what citizens are free to do, and whether to attempt to control and govern the Internet. For example, the U.S. Federal Communications Commission (FCC) is seeking to find relevance with respect to oversight of domestic Internet technical operations. Part of what is frustrating the FCC is the 1996 Telecommunications Act, which stated that the Internet should remain unfettered, that it should not be placed under government control.[5] There are exceptions made, of course, for law enforcement and protection of children, but, in general, the Act states that the Internet should be allowed to function unfettered in the United States. Notwithstanding, much has changed since 1996, especially in the aftermath of 9/11. Several bills aimed at regulating the Internet have been tabled in Congress. These include the Stop Online Piracy Act (SOPA), the Protect Intellectual Property Act (PIPA), and the Cyber Intelligence Sharing and Protection Act (CISPA). Many have not advanced because of resistance from industry or from civil society. (A final push by the Senate to pass their comprehensive cyber security bill during the November 2012 lame duck session was not successful either.)

The Internationalization of Internet Governance

At the international level, a specialized agency of the UN—the International Telecommunications Union (ITU)—is the global governing body for the electrical side of telecommunications and sets the standards that allow people to use technology to talk to one another, make phone calls, etc. The Internet has transcended all those rules, allowing people to make calls using the Voice Over Internet Protocol—VOIP (like Skype or Vonage) from computer to computer free of telephony charges. Many in industry and governments are bothered by this ability to communicate using systems that bypass traditional voice phone calls rules and tariffs.

Meanwhile, developing countries are voicing increasing concerns about the digital divide that has emerged and are requesting support in terms of fiber optic cables, wireless, etc., and the sharing of technology. They are also calling for a stronger role for government in determining standards for how the Internet is run. While much room exists for discussion on these issues, the speaker also stressed that many countries would like their own physical social constitutional norms to apply to cyberspace within their borders. In essence, they would like to place jurisdictional boundaries on the Internet, so that they can also have a say in controlling content. This is problematic, as the Internet does not have boundaries unless they are artificially imposed (e.g., China's Great "Firewall").

The speaker mentioned that, in December 2012, an important conference will be held in Dubai. The International Telecommunications Union (ITU) will host the World Conference on Information Telecommunications (WCIT), during which the International Telecommunications Regulations (ITRs) will

[5] Article 230(b) of the Telecommunications Act of 1996 states that it is the policy of the United States, "to promote the continued development of the Internet and other interactive computer services and other interactive media [and] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."

be reviewed.[6] The review of the ITRs will include determining whether standards and regulations that govern telegraphy, radio, and telephony can be extended to the Internet and subject to the ITU's oversight. The speaker stressed that this is a crucial question and could create significant tension between states that have very different views about how to make the technical side of the Internet work. He also questioned whether such government involvement is really necessary, since most technical problems are generally resolved through informal collaboration between technical experts, not between politicians and diplomats or the military.

The Future of Internet Governance

Part of the governance challenge is that governments do not know how to react in situations that emerge in cyberspace. For example, if an important technical hitch is encountered or a technician misbehaves, affecting people across the globe, what should be the response? Should it be more governance, more diplomacy? Or should we seek new solutions for these challenges that have emerged in the synthetic world we have created called cyberspace? The speaker suggested that, sooner or later, we will reach the point when everyone can communicate and can conduct all their business via the Internet. When this happens, we may find ourselves questioning the role of traditional governance and the relevance of our governments. The first nation that figures out the answer to that question—i.e., the role nation-states can play in such a world—will dominate for the rest of the century. For the United States (and its allies), determining a winning response is paramount. The alternative would be to let another nation or group of nations get the upper hand. The United States would then spend the rest of the century playing catch-up. This, the speaker noted, is the current situation of Internet governance.

❖

IS CYBERSPACE A WAR ZONE?

The third speaker focused his presentation on the three levels of warfare—tactical, operational, and strategic—describing current threats and responses within each of these levels and tabling some initial recommendations for how to move current discussions forward.

The third speaker commenced his presentation with a reference to how interest in cyber has changed. Indeed, just five years ago, very few people were talking about cyber; today, some 29 derivatives of cyber exist—a whole lexicon of terminology has since been created around cyber and the whole world is talking about it. The speaker noted that cyberspace is referred to as a "fifth domain," joining the strategic ranks of land, air, sea, and space. The

[6] ITRs serve as "the binding global treaty outlining the principles which govern the way international voice, data and video traffic is handled, and which lay the foundation for ongoing innovation and market growth." According to the ITU website, "[t]he ITRs were last negotiated in Melbourne, Australia, in 1988, and there is broad consensus that the text now needs to be updated to reflect the dramatically different information and communication technology (ICT) landscape of the 21st century. See: http://www.itu.int/en/wcit-12/Pages/default.aspx.

international community has had a lot of time to develop standards, laws, and rules of engagement (RoE) for behavior and operations in the other domains. We have yet to do the same for cyberspace, which, in contrast to the other domains, is man-made and, accordingly, poses additional challenges. He presented cyber warfare within the context of the three levels of warfare:

Tactical Level—War with a Small "w"

The speaker noted that this level of warfare is experienced daily. Every day is a tactical-level battle for companies, governments, and private citizens who are hit by attacks. Technical experts spend their days fighting adversaries on the network and protecting systems from advanced persistent threats (APTs)—attacks and fraudulent activity—and from attempts to extract intelligence and obtain intellectual property. This, the speaker noted, is a very low level of "warfare." It is a "cold cyberwar" of attrition. At the same time, a lot of damage is being done and can have serious effects.

Operational Level—Cyber "Warm War" with a Small "w"

This level of cyber warfare includes the occasional significant attacks that make the front pages of the *New York Times* and the *Wall Street Journal*—for example, the recent denial of service (DoS) attacks that were carried out against Bank of America and other banks. For the military, it was the attacks that led to operation "Solar Sunrise" in 1998 that made the Department of Defense wake up to its vulnerabilities.[7] The attacks on Estonia in 2007 were also significant: the entire nation, which depends extensively on cyber, was pretty much shut down for a short period. Since then, illicit hackers have continued to hone their skills and abilities. Today, these skills are employed in sophisticated attacks or the use of sabotage tools such as Stuxnet, which damaged Iran's nuclear centrifuges at Natantz; or extraction tools such as DUKU and FLAME, which are said to have mapped U.S. gas pipelines and potential choke points. The speaker referred to this as the "warm" level of cyber warfare. It has provoked political tension on international and domestic fronts. Internationally, tension is emerging between nations as increasing evidence is emerging that some countries are developing and using these sabotage and extraction attack tools. Domestically, this "warm war" is giving rise to a new form of political contestation: an enormous amount of cyber-related legislation is being drafted, debated, and defeated. In 2011, some 85 pieces of legislation were tabled; this year, some 40 pieces have been tabled. Tension among and between members of Congress and between Congress, the private sector, and civil society over what should or should not be included in these pieces of legislation is rising.

At this level, and also at the tactical level, cyber is gaining importance within the legal sector. Lawyers' professional organizations need to understand the issues in order to be able to advise their clients, while a need to know how to argue these issues in litigation also exists. Common terminology is urgently required.

[7] While it was initially assumed that the attacks emanated from a state actor or terrorist group, operation Solar Sunrise investigations revealed that the attackers were actually two teenagers from California and one from Israel. For further information, see: http://www.wired.com/threatlevel/2008/09/video-solar-sun/

Strategic Level, Cyber Hot War, War with a Capital "W"

The speaker noted that this level of cyber warfare involves military confrontation. At this level, much work is needed to ensure that such confrontation is avoided. What distinguishes this type of cyber warfare from the other two? One, a cyber "hot war" would involve devastating, long-term effects. An attack at this level would lead to the 5Ds: death, destruction, damage, disruption, and devastating economic loss. Two, this kind of cyber warfare would require congressional approval (in the other four domains—land, air, sea, and space—Congress is [at least in theory] supposed to declare when the United States is officially at war). A major challenge with cyber would be determining the identity of the enemy. Declaring war against a virtual activity is very difficult. The speaker noted that preventing cyber war/deterrence has three requirements:

- Resilience: a resilient network can help deter someone from attacking you. Attackers know that if they persist and cannot gain access or disrupt a system, they will have to give up or eventually get caught by law enforcement.
- Recognition: knowing who is attacking you, who the enemy is. The capabilities to enable such recognition need to be developed and implemented.
- Retaliation (attack capability): the United States won the cold war through a nuclear stand-off. If we can develop a capability and send signals that we have it and are willing to use it (as is increasingly being reported today), we could end up in a situation of mutually assured disruption (a MAD theory of cyberspace).

On a final note, the speaker mentioned the ongoing work of the EastWest Institute, including its annual Worldwide Cybersecurity Summit (Dallas in 2010, London in 2011, New Delhi in October 2012); its Track II work with both Russia and China, and the development of a common lexicon on cyber with Russia.

❖

THE ROLE OF CYBERSECURITY IN U.S.-CHINA RELATIONS: COMPETING INTERESTS & STRATEGIES

The fourth speaker discussed Chinese interests and behavior in cyberspace from an economic, military, and political perspective and how these interests differ from those of the United States. The presentation also focused on U.S. efforts to engage China and prospects for change in Chinese behavior.

Common and Conflicting Interests

The fourth speaker opened by referencing the U.S. International Strategy for Cyberspace, which states that the United States has a stake in "an open, secure and global" Internet and cyberspace. He then noted that China shares some common interests with the United States in this area.

An Open Internet

The speaker observed that China's Great Firewall immediately suggests that the United States and China do not share common interests about openness on the Internet. China's principal objective is to ensure that information from the outside does not get in and it has pretty much succeeded in keeping information out: Google, Twitter, Facebook are all blocked. The Chinese Internet is, however, becoming more open as, even in closed systems, controlling all activity and content is impossible. This has resulted in a constant "cat and mouse game" between the government, whose aim is to control information, and Chinese bloggers who wish to spread it.

A Secure Internet

The speaker noted that the United States and China do have a shared interest in having a secure Internet. Chinese cybercrime, Chinese crime directed at Chinese companies, Chinese criminal hackers—all are increasing. The Chinese are particularly worried about terrorist attacks on their infrastructure. The challenge is that the United States and its allies constantly use the term "cyber security," referring to the security of the Internet's architecture and ensuring point-to-point free flow of information. The Chinese and the Russians, however, use the term "information security," which includes the security implications of the content that flows on the Internet. For the Chinese, the threat is not only the hacker in the basement, but the threat of information security to regime stability. These different goals, different nomenclature, and different definitions have rendered discussions with the United States difficult because the United States is unlikely to trade Internet freedom for Internet security.

Global Standards and Interoperability

The speaker stressed that developing global standards is important to business expansion and innovation. On this point, he noted that the Chinese are of two minds. Central policymakers are worried about the longer-term impact of technological dependence on the West. Their strategy for achieving independence is through a policy focused on indigenous innovation—the creation of Chinese competitors to U.S. companies. This is already happening in the technical cyber security realm through MPLS,[8] encryption, etc. Chinese firms are of two minds on this policy, however.

Competing Visions of Internet Governance

The United States has a vision of Internet governance that is multi-stakeholder, bottom-up, academic, transparent, and involves non-state actors. This approach is anathema to the Chinese as their goal is to reassert state sovereignty over Internet governance. They are trying to achieve this goal

[8] Multi-Protocol Label Switching

through the ITU and other platforms. In short, the United States and China share few interests and certainly disagree on how to shape Internet governance. The speaker raised the question of why the Chinese are trying to shape the Internet—noting that they are doing so because they can and also because they are seeking economic, military, and political advantage.

The Economic Perspective

From an economic perspective, clearly the Chinese do not want to be dependent on the West. This is a very legitimate side of China's technology policy and to that end, the country's leaders plan to increase R&D spending to 2.1 percent of GDP this year and to 2.5 percent by 2020. Indeed, China plans to be a significant power in innovation by 2049. China has a human resource advantage. This year, some six million college students will graduate, 60–70 percent of them in science and engineering. The illegitimate part of China's innovation policy, however, remains the theft of intellectual property (IP). As noted earlier, IP theft happens in the traditional way as well as through cyber espionage. The latter has been said to represent the greatest transfer of wealth in history.[9] China engages in such theft because it can and because limited risk is involved.

The Military Perspective

Militarily, China sees itself as the weaker power—especially in a force-on-force possible engagement with the United States. Over the past twenty years, it has been considering issues such as how to attack U.S. weaknesses, how to develop an asymmetrical strategy. The Chinese have observed the use of asymmetrical strategies to counter ballistic missiles, for example, by targeting aircraft carriers in the sea, in satellite programs—and now in cyber. For example, all the Chinese open source writings from military analysts suggest that one way to impede the United States is by making sure that supply ships do not rendezvous on schedule. There is a strategic element in this behavior: if the Chinese are in our networks and leave little hints behind that they were there, they are sending a reminder or signal to the United States that if a regional conflict should arise and if it escalates, we Chinese can do something about it.

The Political Perspective

China is using cyberspace to respond to many of its domestic political concerns. For example, the issue of Tibet remains an important political concern. Tibetan activists are often drowned by spam sent by Chinese hackers, emails are hacked, and think tanks focusing on Tibet are attacked. China uses hackers as proxies to either silence or shape debate within and outside its own cyberspace.

Chinese Views of U.S. Behavior

According to the speaker, China considers much of the U.S. position on cyberspace and the Internet to be hypocritical. While the United States has

[9] This statement was made by U.S. Army Gen. Keith B. Alexander, Director of the National Security Agency (NSA) and Commander of the USCYBERCOMMAND at an American Enterprise Institute (AEI) event on July 9, 2012.

said that it wants a peaceful cyberspace, China accuses the United States of militarizing the Net through the establishment of the U.S. Cyber Command and the development of capabilities such as Stuxnet. China also assumes that U.S. intelligence agencies are in their networks and that the United States is spying on them all the time. Such suspicions may have a strong foundation since at one point 95 percent of Chinese government offices were using the easily penetrable (and pirated by them) Microsoft Word software. The United States will only discuss economic espionage, refusing to talk about political or military espionage.

China views the ongoing Huawei debate as particularly hypocritical, first because they believe it was begun by Cisco Systems, which has its own vested interests, and, second, because almost all the threats discussed about Huawei—the insecurity of its supply chain, the unreliability of its middle managers, the insider threat—can characterize any telecommunications company in the world.

As noted, China is not comfortable with the current system of Internet governance and views the refusal of the United States to negotiate a new deal as the United States wanting to preserve a status quo that only benefits the United States. However, most other countries, including India and Brazil, which in many ways are becoming more important than China, are insisting on change. In essence, the United States has not yet put anything positive on the table.

U.S. Engagement with China

Deterrence

The establishment of the U.S. Cyber Command and Secretary of Defense Panetta's speech warning of an imminent "cyber Pearl Harbor" were part of it.[10] Secretary Panetta basically said that the United States is getting better at resolving attribution and will respond. Many interpret the secretary's speech as an attempt to deter Iran, but the speech was also directed at China.

Naming and Shaming[11]

After the attack on Google two years ago, U.S. government officials would refer to nation-states being behind the attack but would not name a specific country. They would then call experts to confirm their suspicions. Today, no

[10] Defense Secretary Panetta spoke of an imminent "cyber Pearl Harbor" warning that the United States was "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government." The speech was given at an event held at the Intrepid Sea, Air and Space Museum in New York on 11 October 2012. See http://www.nytimes.com /2012/10/12/world/panetta-warns-of-dire-threatofcyberattack.html?pagewanted=all&_r=0

[11] Harvard Professor and strategist Joseph Nye has talked about "high-cost" cyber deterrence strategies such as "naming and shaming" the country where the attack originated: a country that engages in such attacks might be regarded as a risky place to do business, to invest, to keep one's money. He notes, however, that making that kind of subtle deterrence work requires a much better ability to attribute an attack to a specific nation, and maybe to specific actors inside that nation. David E. Sanger (2012-06-05). *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Kindle Locations 4280-4282). Random House, Inc. Kindle Edition.

calls to experts are made—U.S. officials have readily identified China as the perpetrator of cyber espionage attacks.[12]

Official Dialogue Channels

Cyber now forms part of the strategic economic dialogue with China. Both secretaries Clinton and Panetta raised cyber issues with their counterparts during their last meeting.

Track II Processes

Different Track II processes with China have already been launched, including those facilitated by the Center for Strategic and International Studies (CSIS) and the EastWest Institute (EWI). The goal is to find some areas of commonality upon which cooperation can be established. Other Track II efforts include joint reports or joint initiatives such as a recent EWI report—"Fighting Spam to Build Trust"[13]—which focused sharply on the question of "dual illegality." The problem with dual illegality collaboration is that, in some cases, what China identifies as criminal behavior, the United States views as politically motivated behavior. In addition, coordination has not been very good with the FBI and the Department of Homeland Security, while communication between U.S. and China Computer Emergency Readiness Teams (CERTs) is nonexistent.

Prospects for Change in China's Behavior

The speaker noted that for now and probably in the immediate future, China views the United States as more vulnerable than itself. Partly because of the nature of the U.S. economy, its military, and partly because of China's Internet infrastructure. China's Internet has fewer access points; accordingly, controlling it is easier. That will change over time, not least because China's economy is expanding and becoming increasingly dependent on the Internet for growth and, thus, will eventually need to open up. Indeed, Chinese business wants innovation in this space, and China's military—the PLA—wants to become a Net-centric fighting force. It wants to look like the United States, so it is developing relevant capabilities.

Over time, this race to match U.S. technological superiority might lead to what was referred to earlier as mutually assured disruption (MAD), with both sides considering nonaggressive action in cyberspace as the best course. For now, however, China still sees the United States as the more vulnerable, which could very well lead to reckless behavior triggering or escalating an existing crisis. The Chinese see taking out U.S. systems as a low-cost endeavor. Accordingly, the United States will need to determine how to signal that this is not the case.

China's behavior may change over time because (even though there is currently no evidence) factions might emerge within the its government

[12] For example, both China and Russia were openly named in the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage published in November 2011 by the Office of the Director of National Intelligence.

[13] http://www.ewi.info/fighting-spam-build-trust

who believe that hacking long term is not in China's interest and that creating their own standards and cutting themselves off from the rest of the world is not going to help China's growth. These factions might push for more openness. In addition, there are also those who do consider (and worry about) China's relationship with the United States, the EU, and Japan—the country's most important economic partners.

On a final note, the speaker stressed the importance of examining how China participates at the global level. China is no longer a revolutionary power or state; rather, it is a status quo power and generally does not like portraying itself as playing outside the global order. This became very clear with the issue of proliferation. China's behavior was and is not perfect in certain decisions about Iran, but tracking China's behavior in missile control shows that their behavior at the international level has shifted. Looking to the future, the main challenge will be to determine whether we can define common norms with China for operating in cyberspace. The speaker noted that the United States has been actively attempting to do so. The signals, however, are not particularly encouraging. For example, a couple of weeks ago, Harold Koh, a State Department legal adviser, gave a speech on the Laws of Armed Conflict (LOAC) and their applicability to cyberspace, noting that the U.S. position is that they *are* applicable.[14] China, on the other hand, believes that the LOAC do not apply to cyberspace; that cyber is a new area and that new treaties are required.[15] These opposing positions are difficult to bridge. In the long term, what will be more important will be to bring emerging large democracies such as India, Brazil, Indonesia, and South Africa on board and focus discussions on values and reaching common ground on norms. These are all long-term goals and will take some time to achieve. In the short term, the speaker recommended that the United States focus on developing resilience and defenses and identifying entry points for working with China.

❖

QUESTION & ANSWER SESSION

On China

The first question raised the issue of China's efforts in cyberspace and whether these are centralized or coming from different quarters; whether the United States is aware of the people involved; and whether efforts have

[14] See remarks of Harold Hongju Koh, the U.S. Department of State's Legal Advisor on "International Law in Cyberspace" at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012 at http://www.state.gov/s/l/releases/remarks/197924.htm

[15] In November 2011, China and Russia backed by Takikistan and Uzbekistan tabled a proposal for an International Code of Conduct for Information Security. The Chinese-Russian proposal discusses the security challenges cyberspace presents to the international community and proposes the need to establish rights and responsibilities of states in protecting information networks and cybernetworks. The proposal says states should respect domestic laws and sovereignty, but also calls for a multilateral approach within the framework of the United Nations to establish international norms and settle disputes about cyberspace. See: Letter to the UN General Assembly from China, Russia, Tajikistan and Uzbekistan: http://www.citizenlab.org/cybernorms/letter.pdf

been made to recruit them. One of the speakers noted that to his knowledge, strategic goals are set at the top, but below that, control and coherence of effort are more complicated despite China's centralized and heavily controlled political structure. What is apparent, however, is the merging of criminalized and espionage networks. SIGINT (Signals Intelligence) could possibly help identify individuals and networks as they all must log in and log out of systems at some stage. If individuals are identified, sanctions could be used against them. To date, the United States has a mediocre record at both identifying and recruiting Chinese hackers.

On the Advantages and Disadvantages of Operating in a "Cyber Jungle"

One of the participants commented on how the United States, China, and Russia tend to demonstrate intractability on different cyber-related issues in a range of fora, including on cyber terrorism, cyber crime, and cyber warfare. For example, Russia has been pushing for the adoption of an international convention that includes references to terrorism and cyber crime, as well as to broader conflict.[16] The U.S. position is that such a convention is unnecessary as these issues are already addressed in existing treaties and conventions. Meanwhile, the private sector has emphasized that the United States has no interest in regulating cyberspace since the United States benefits more than any other country from the cyberspace "jungle," from the "fog" or "chaos" that has emerged in relation to the domain. The United States is more advanced in terms of offensive capabilities, has more effective penetrating capabilities, and, therefore, has limited interest in regulating the space. The United States also has other advantages in the cyber "jungle," including that cyber, the Internet in particular, allows the United States to promote democracy in parts of the world where political leaders are trying to censor information. Without this "jungle," the Arab Spring might not have come about. Both China and Iran are deeply concerned about this "jungle" and are trying to contain it.

The participant then questioned whether the United States is really a victim, as it often makes itself out to be [referencing Secretary Panetta's speech on an imminent "cyber Pearl Harbor"] or whether it actually has the upper hand and really just has to lower the risks involved and upgrade the advantages. Speakers responded that, indeed, countries like China and Russia also take advantage of the "jungle" that is cyberspace as it allows them to engage in actions that would otherwise be unacceptable. One speaker in particular emphasized that it is, however, important to remedy some of the chaos, to give some order to the "jungle" so we can actually see what is happening in cyber. It is an awkward position—U.S. foreign policy (like that of China, Russia, and others) prefers the smoke as it covers otherwise unacceptable actions, but officially and diplomatically, the United States must maintain the stance that there are different ways of seeking solutions.

[16] In addition to the aforementioned Code of Conduct that it tabled with China, Russia has also developed a draft concept for a Convention on International Information Security. Presented to an international meeting on information security in September 2011, the draft convention focuses on provisions to reduce information flows that could produce social unrest or other destabilization in countries. For the draft convention see: http://www.citizenlab.org/cybernorms/russian.pdf

On the Role of the Private Sector

One of the participants raised the question of what private sector companies—Google, Microsoft, Verizon, etc.—are actually thinking and doing about cyber threats. One of the speakers responded that their voices are becoming part of the crucial conversation, and they are increasingly insisting that the Internet should not be regulated or locked down through treaties and conventions—especially in the context of international peace and security, where the role technology companies play is unclear. Other questions that remained unanswered related to the role of the private sector in cyber diplomacy and in discussions on international treaties, etc., with the insistence that something new needs to be developed.

At the operational level, more discussion on the role of the private sector is urgently needed as companies do not necessarily want to become combatants, yet are heavily involved in defending systems or are increasingly asked by government to remove content or defend sites from specific content. Some firms are becoming involved in offense, operating like mercenaries or defense contractors, and making money from the alleged threat of "cyberwar."

On the Role of the Military

Questions were also raised about the role of the military in responding to cyber challenges, not least because the United States and Russia generally send military representatives to meetings attended, for the most part, by law enforcement and intelligence representatives. One of the speakers stressed that, at least in relation to the United States, the DoD is deeply involved because it has been the target of attacks since as early as 1998 and has developed significant expertise in the areas of defense, offense, exploitation, and resilience. The Department of Homeland Security was only established in 2003 and is still developing expertise in these areas.

Another participant raised the question of whether the United States currently has the capabilities to fight and win a simultaneous preemptive cyber war against Russia and China. One speaker responded that the United States does have tremendous capabilities and has been developing them over the past fourteen years, but other countries are also developing them.[17] How a preemptive attack would play out is unclear, however.

On the Role of the Legislature and Lessons from Other Regimes

One of the participants raised the question of whether too much is being made of the extent of the threat in cyberspace, referring to similar concerns that emerged about the creeping weaponization of outer space and unfounded warnings of a potential "Pearl Harbor" in outer space just a decade ago.[18] The participant also questioned whether the current use of a war lexicon—cyberwar, deterrence, cyber MAD, cyber cold war, hot war,

[17] UNIDIR and CSIS are currently undertaking an assessment of national capabilities, doctrine, organization, and building transparency and confidence for cyber security.

[18] A presidential commission chaired by former Secretary of Defense Donald Rumsfeld warned in 2001 that the United States is "a prime candidate for a space Pearl Harbor."

etc.—is pushing the militarization of the domain as had been the case with outer space. Regarding the role of Congress, the participant questioned what the current political will is in relation to responding to cyber threats, suggesting that lessons might be drawn from the Nunn-Lugar legislation on Cooperative Threat Reduction (CTR). This legislation addressed itself predominantly to the United States and Russia drawing down nuclear arsenals after the cold war.[19] Today, discussions are being held on the possibility of extending the Nunn-Lugar CTR package to include coalitions of like-minded nations. With obvious differences, the term "CTR" certainly seems to apply to the cyber arena. In this regard, the participant questioned whether there is any impetus in Congress to adopt some form of a CTR for cyber? Is there political will to do so? Is it a feasible proposition?

One of the speakers responded that given the current impasses in Congress on cyber-related legislation, a CTR for cyber is highly unlikely. At present, the only point there has been agreement on, and which flows through each of the 40+ pieces of legislation being debated in Congress, is the provision to share information between the private and public sectors. However, the actual scope of information sharing is bogging down even that agreement. In addition, major differences have emerged between those who are pro-standards and recommendations and others, such as the US Chamber of Commerce, that oppose standards and recommendations. The question of who is responsible for protecting civilian infrastructure also remains a challenge.

Another participant raised the issue of awareness of the challenges within Congress. Speakers highlighted the challenges of working with staffers within the Senate. The National Cyber Security Alliance (NCSA) established Cyber Security Awareness Month and is also engaging members of Congress and staffers through workshops, etc. Staffers are ultimately responsible for drafting legislation, but most senators' briefings by the intelligence services are classified, thus staffers are not privy to vital information. Reference was also made to the importance of developing public-private partnerships at the state and city levels—including as a means to share the cost burdens of responding to cyber attacks.

At the international level, and as noted earlier, Track I ½ and Track II diplomacy processes can play a significant role, as they can foster dialogue on these issues in support of formal diplomatic processes, such as the U.S.-Russia agreement to establish a cyber "hotline"—a crisis communications line similar to the one established during the cold war. The Nunn-Lugar process started through Track I and Track II processes and gradually led to the CTR. One participant raised the question of whether, given its experience in Track II processes, NCAFP could play a role, particularly in fostering dialogue with China on cyber issues as it is evident that crisis communication is not in place.

[19] See http://www.dtra.mil/Missions/nunn-lugar/nunn-lugar-home.aspx

Speakers responded that even discussions in Washington about cyber incident response plans are more focused on domestic responses rather than international responses and that much more structured dialogue at the international level is required. Discussions with China have already commenced on pre-positioning and how and who to engage, but it is clearly an area where the NCAFP could also play a role. Working with like-minded countries such as Australia could also be advantageous. Another speaker stressed the importance of linking to government efforts, at least partly because if Track II efforts are to be useful, it is important to understand what discussions are already under way. That knowledge would help define entry points and assess the added value of engaging; it would also enable analysts and participants to report on the outcome of discussions. A forthcoming EWI report, "Priorities for International Communications," will be able to shed additional light on potential entry points for Track II processes.

Examples of ongoing formal diplomatic processes at the international level that require further discussion in order to understand their implications include: the work of the Group of Governmental Experts (GGE) taking place within the UN General Assembly's First Committee on Disarmament Affairs, which is focusing on reaching agreement on norms and confidence-building measures in cyber space,[20] regional-level discussions that the Organization for Security and Co-operation in Europe (OSCE), the ASEAN Regional Forum (ARF) are hosting on confidence-building measures and other related issues.

❖

POLICY OBSERVATIONS

Cyberspace is a highly complex environment that not only challenges our domestic security with respect to proper online behavioral norms, but also tasks the international community with re-examining traditional methods of diplomacy, trade, and law enforcement. The millisecond nature of online transactions works against the classic security framework that depends on lengthy discussions for conflict resolution or delays of weeks or months to resolve trade issues. Instead, a new approach that recognizes and leverages the attributes of cyberspace is needed. National security interests in a cyber-centric world must recognize that:

- Cyberspace is a synthetic domain that does not understand historical separations of societies based on land features, cultures, religion, or ethnicity;

[20] See the following articles for additional background on the UN GGE process:
http://www.unidir.org/bdd/fiche-article.php?ref_article=3179;
http://munkschool.utoronto.ca/canadacentre/research/developments-in-the-field-of-information-and-telecommunication-in-the-context-of-international-security-work-of-the-un-first-committee-1998-2012/; and
http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

- Attribution of threats and threat actions are difficult and sometimes impossible because of the anonymous nature of the Internet; however, that same anonymity makes cyberspace attractive to those seeking increased interaction of all kinds;

- Value is everywhere online; its accessibility is simultaneously a benefit and a vulnerability;

- Attacks can range from simple denial of service to theft of intellectual property to physical damage and possible loss of human life;

- The cost of an attack to the attacker is extremely low compared with the cost borne by the victim;

- The highly interconnected nature of cyberspace allows risks accepted by one user to also become risks that must be accepted by everybody else;

- Military, criminal, espionage, and adolescent malicious behavior in cyberspace use identical tools and techniques that are readily available to anybody online;

- Cyber weapons and tools are readily available and use the same hardware and software components that average citizens use for online commerce;

- Awareness of online threats and vulnerabilities is fairly low;

- Most developed societies are irreversibly dependent on cyberspace for economic, domestic, and national security; and,

- No organization or person owns, rules, or governs cyberspace—its success is the result of an approach that is unfettered from traditional government oversight.

THE HOST, THE PRESENTERS, AND OTHER PARTICIPANTS

The Host

Dr. George D. Schwab
President, NCAFP

The Presenters

The Honorable Franklin D. Kramer
Distinguished Fellow, Atlantic Council

Lt. General Harry D. Raduege, Jr. (USAF, Ret.)
Chairman, Deloitte Center for Cyber Innovation

Marcus H. Sachs
Vice President of National Security Policy, Verizon Communications

Dr. Adam Segal
Maurice R. Greenberg Senior Fellow, Council on Foreign Relations

Other Participants

Professor Giuseppe Ammendola
New York University

Mr. Kevin Backus
Director of Equities Research and Trading, BGC Financial

Mr. Randolph Bell
Managing Director, The International Institute for Strategic Studies – U.S.

Mr. Carter Booth
Trustee, NCAFP

Mr. Sidney J. Caspersen
Assistant Commissioner, NYPD

John V. Connorton Jr., Esq.
Trustee, NCAFP
Partner, Hawkins Delafield & Wood LLP

Captain Peter A. Garvin
Military Fellow, U.S. Navy, Council on Foreign Relations

Mr. Thomas Glynn
Captain, NYPD

Mr. Thomas E. Graham
Managing Director, Kissinger Associates, Inc.

Ms. Edythe M. Holbrook
Trustee, NCAFP

Richard R. Howe, Esq.
Trustee and Treasurer, NCAFP

Mr. David P. Hunt
Chairman, Charles Pratt & Co.

Ms. Angela Kane
High Representative for Disarmament Affairs, United Nations

Ms. Camino Kavanagh
PhD Candidate, Department of War Studies, Kings College
Fellow, Canada Center for Global Security Studies, Munk School, University of Toronto

Mr. Igor Kharkov
NETSEC Group Manager, Thomson Reuters

Mr. Peter Maass
Author and Journalist

Ms. Hatice U. Morrissey
Vice President, Trustee, NCAFP

The Honorable Matthew Nimetz
Trustee, NCAFP
Advisory Director, General Atlantic

Mr. Charles Ortel
Managing Partner, Newport Value Partners, LLC

Ms. Missy Owens
Director of Public Affairs and Government Relations, The Coca-Cola Company

Mr. William M. Rudolf
Executive Vice President, NCAFP

Dr. David Scharia
Security Council Terrorism Committee Executive Directorate, United Nations

Mr. David C. Speedie
Senior Fellow & Director, U.S. Global Engagement, Carnegie Council

National Committee on American Foreign Policy, Inc.

FOUNDER – Dr. Hans J. Morgenthau

MORGENTHAU AWARD RECIPIENTS

KENNAN AWARD RECIPIENTS

THE WILLIAM J. FLYNN INITIATIVE FOR PEACE AWARD RECIPIENTS

GLOBAL BUSINESS LEADERSHIP AWARD RECIPIENTS

21ST CENTURY LEADER AWARD RECIPIENTS

OFFICERS 2012

TRUSTEES

BOARD OF ADVISERS

NATIONAL COMMITTEE ON
AMERICAN FOREIGN POLICY, INC.
320 Park Avenue
New York, N.Y. 10022
Telephone: (212) 224 1120 • Fax: (212) 224 2524
E-Mail: contact@ncafp.org • Web site: http://www.ncafp.org