21st Century Defense Initiative
at BROOKINGS

JOHN L. THORNTON
China Center
at BROOKINGS

Cybersecurity and U.S.-China Relations

网络安全与美中关系

Kenneth Lieberthal and Peter W. Singer
李侃如，彼得. W. 辛格

21st Century Defense Initiative
at BROOKINGS

JOHN L. THORNTON
China Center
at BROOKINGS

Cybersecurity and U.S.-China Relations

网络安全与美中关系

Kenneth Lieberthal and Peter W. Singer

李侃如，彼得. W. 辛格

February 2012

Authors' Note

For the last year, the John L. Thornton China Center and the 21st Century Defense Initiative at Brookings have convened a working group on cybersecurity and U.S.-China relations, which the two authors organized and co-chaired. The research was motivated by our sense that: 1) the many policy issues involved in cybersecurity, especially in its impact on foreign relations, were already significant and would grow rapidly in importance in the coming years; 2) that such issues, if not well managed, could provide a major source of international friction, especially in U.S.-China relations; and 3) the newness of the field added a particularly complicating factor, making cybersecurity one of the most important but least understood emerging flashpoints in global security.

A key aspect of the effort was to convene several dozen knowledgeable Americans from both the private and public sector, including the civilian government, military, corporate, think tank, and university communities. With such dynamic and fast-changing events playing out, the Brookings project not only sought to study the key issues in cybersecurity and how they impact U.S.-China relations, but also to break down some of the organizational and bureaucratic stovepipes that have limited leaders and expert groups as they seek to build the type of understanding crucial for developing sound policies.

The working group did not seek to provide final answers to all the various questions that trouble relations in this space. Rather, participants saw a critical need first to build a framework for understanding the key trends and risks in the cyber arena, as a basis for thinking carefully about how to engage most effectively in a U.S.-China dialogue on such issues. The group had a particular focus on how best to think about the cyber realm in ways that might lead to cooperation. A goal was to identify the potential pathways to building norms and enforcement mechanisms, which might both improve safety and security and also reduce the degree of distrust and the potential damage brewing in the U.S.-China relationship in this space and beyond.

By no means would all cybersecurity issues be solved if Washington and Beijing could reach agreement on how to move forward. These issues are of importance in capitals that range from Moscow to Canberra. Indeed, one of the key challenges is that the cyber realm is both global and especially democratic; states, organizations, corporations, and even individuals can have major, global impact. [Examples ranging from an individual's significance like Julian Assange of Wikileaks to the outsized influence that tiny Estonia plays in cybersecurity policy discussions bear this out.]

But the United States and China are the two most significant national players in this sphere. Moreover, these two leading states represent very different views on the proper use and future of the Internet. We therefore feel that thinking through these issues in a U.S.-China context can provide a useful way to develop approaches that should then be discussed more broadly, with the goal of ultimately establishing global norms and implementing mechanisms to bring greater order and security to those parts of the cyber realm where this is feasible.

More importantly, the spillover effect of cybersecurity on the broader U.S.-China relationship is also perhaps more critical than for any other bilateral relationship. This is both because of the enormous importance of U.S.-China relations in the emerging world order and, in turn, the growing role of cyber issues in eroding strategic trust and poisoning public and elite attitudes. If this trend can be reversed through improved engagement by the U.S. and China on cybersecurity, the outcome would be a "triple win." It would bolster U.S.-China bilateral relations, serve as a crucial building block for multilateral efforts in the cyber arena, and also aid in broader US-Chinese engagement on other issues of importance, like global finance and the environment, where the two nations must learn to work better together.

This is not a technical paper for cyber specialists, but rather is intended to be read by a wider audience. Our goal was to craft a work that will be useful to both American and Chinese readers who are interested in the cyber security issue but are not technical specialists in it. We have written this to be of interest to people in the policy world and in the private sector, as well as the wider public. We have drawn from both Chinese and U.S. sources, and we have deliberately sought to avoid finger pointing. Our hope is that this paper—which is being published in both English and Chinese—will help shape useful discussions in the U.S. and China about a dialogue on cyber issues and, most importantly, to encourage both sides to move forward on this critical effort.

The following paper is derived from the authors' own research and from the cybersecurity working group discussions. However, the paper reflects only the views of the two authors who convened the working group meetings.

We are grateful to the participants in the working group sessions, who so informed our efforts with their experience and wisdom. We would also like to thank those who supported the discussion series, including the Markle Foundation and Microsoft, and John L. Thornton for his generous support of the John L. Thornton China Center. We are also grateful to Ella Chou, who aided in the research and then the translation of the report.

The Brookings Institution is a private non-profit organization. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author, and do not reflect the views of the Institution, its management, or its other scholars.

Brookings recognizes that the value it provides to any supporter is in its absolute commitment to quality, independence and impact. Activities supported by its donors reflect this commitment and the analysis and recommendations are not determined by any donation.

Abstract

There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China. And in their relationship, there is no issue that has risen so quickly and generated so much friction as cybersecurity. Distrust of each other's actions in the cyber realm is growing and starting to generate deeply negative assessments of each country's long term strategic intentions.

During 2010-2011 Brookings' John L. Thornton China Center and 21st Century Defense Initiative hosted a working group on cybersecurity and its impact on U.S.-China relations. The following paper draws from discussions in that working group and additional research to suggest how to take the particular characteristics of the cyber security realm into account while fostering U.S.-China cooperation on cybersecurity.

Special Characteristics of the Cyber Realm and U.S.-China Relations

Every policy issue has its own unique contours and problems. But the cyber realm has a number of particular characteristics that significantly challenge current U.S.-China relations and the prospects for reaching a consensus on either norms or cooperative implementing mechanisms.

Varied Terminology

The cyber security realm lacks shared vocabulary with agreed upon meanings for key terms. Even such terms as "information" and "cyber

attack" are used differently within and between the American and Chinese governments. There are, also, many types of "attacks," but there is little agreement on how to characterize and categorize them.

Uncertain Attribution

It is rarely possible to identify with complete confidence the actual initiator of a malicious cyber activity. The ability to capture the operations of another computer and use it to launch activities that its owner does not intend and might even be unaware of further complicates the issue of attribution.

Offense Has the Advantage

The one seeking to penetrate a computer network, at least at present, is at a great advantage relative to the defender. The Internet was designed to share information easily, not prevent its flow. Historically, an imbalance in favor of the offense increases the incentives to act maliciously and quickly, while it also lowers each side's confidence in its ability to deter attack and defend itself effectively.

The Complication of Time

Policy, which often moves at a slower pace than technical innovation, is inevitably at risk of being fundamentally out of synch in dealing with exponential rates of technological change in cyber capabilities. Additionally, at least in policy terms decision-making time is, in effect, compressed in cybersecurity. While proper preparations for an attack may require weeks or months, the actual elapsed time for its successful execution may be counted in nanoseconds. Thus, the normal processes of governments and institutions to decide on responses may simply be irrelevant to the problem. Finally, there is a generational chasm between today's "digital natives," the youth who have grown up in a world where computers have always existed, and anyone from older generations, for whom computers are something to which they have had to adjust (so-called "digital immigrants"). The result is that top level policymakers with the most power are often the most uncomfortable even talking about cyber issues.

Decentralization of Capability

Large human, financial, or physical resources are not necessary in order to act at scale in the cyber realm. This is, moreover, a sphere in which learning can take place at great speed among those on the cutting edge. Never before in history has scalability of a threat been so easy to achieve. Because of this element of scale, the lines between state and non-state actions in the cyber world are often shifting and blurred.

Building a U.S.-China Agenda on Cybersecurity

The above features of the cyber realm make developing an agenda to improve U.S.-China cooperation in this sphere more challenging but not impossible. Any such agenda must be realistic, respecting that each government will protect its ability to use cyber capabilities to carry out espionage activities and to support military actions should they become necessary. It must accept that the two political systems have significantly different views concerning freedom of information in cyber space. It must take into account that each government's decision making concerning cyber activities is fragmented among many bureaucracies and is not well coordinated at any single node in the system. Finally, it must respect the reality that a variety of nongovernmental actors are significant players in each country's use of and deliberations about the cyber realm.

Steps in developing such an agenda should include the following.

Expand engagement to match the growth of the problem

Cybersecurity issues have been discussed in meetings between U.S. and Chinese officials, and there have also been "track two" meetings between key unofficial groups. But the scale of the engagement to date is simply inadequate to the task at hand. The goal should be to develop a broader cadre of people who utilize the same vocabulary, are respected by their own leadership, and have trust in each other's sincerity and gravitas.

Focus initially on building shared aims and identifying activities that both sides deem harmful

To facilitate building mutual confidence, these discussions should focus on activities, such as those that are considered to be criminal in both societies, that do not have a significant political component to them.

Examine models of cooperation

There is deep value in discussing the advantages and disadvantages of applying various models of cooperation to cyber security. Some parallels worth exploring are arms control negotiations, public health, environmental ecosystems, and global finance regimes targeting worldwide crime and terrorist organizations.

Make explicit the norms that are currently built into the global Internet system

The norms and agreements that allow the smooth functioning of the Internet are wide ranging and substantial, but overwhelmingly the system still runs on handshake agreements between the various entities and ISPs that provide the Internet backbone. A cooperative effort to make widely accepted norms explicit can both increase mutual understanding and confidence and also provide a better template for addressing more complex issues.

Address the attribution problem

The centrality of the attribution problem cannot be overstated, and thus it cannot be avoided for long. The objective may best be to find a middle ground between the dangers of anonymity and the positives that come from the freedom of action that currently define the Internet.

Discuss the "red lines" that could provoke major conflict if crossed.

Some argue that nations should continue to stay vague about their escalation paths, but there will be real gains for all players to come to a better understanding of what actions might risk generating a wider conflict. It will not just inform each nation's leaders about their own investments and capabilities that might unintentionally escalate a crisis, but also potentially help generate norms and implementing mechanisms to take at least some such risky actions "off the table."

Conclusion

Establishing greater mutual understanding and trust will be a difficult process. It will require consistent efforts over time, common approaches to structuring the discussion, and the selection of topics that hold the most promise for permitting increasing mutual understanding of perceptions, goals, and acceptable approaches and methods. But developing greater U.S.-China cooperation and understanding on the challenges of cybersecurity is now a necessary step. How these two nations face these issues will be critical not just to the future of the Internet and its billions of users but also to overall global order beyond the world of cyberspace.

Introduction: The Stakes of Cyber Security and U.S.-China Relations

There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China. No other two nations play such dominant roles in critical global issues from peace and security to finance, trade, and the environment. How these two powers manage their relationship will likely be a key determinant of not only their own political and economic futures, but also wider global stability and prosperity.

In the web of relationships that have built up between the U.S. and China, no issue has emerged of such importance, and generated such friction in so short a time span, as cybersecurity. Just a generation ago, "cyberspace" effectively did not exist beyond the nascent links among a limited number of university labs' computer networks. Today, the centrality of cyberspace to our entire global pattern of life is almost impossible to fathom. There are some 4 billion people behind the roughly 50 billion devices that connect to the Internet. They send more than 90 trillion emails a year, and conduct more than two trillion transactions.[1] Domains that range from commerce to communication to the critical infrastructure that powers and protects our modern day civilization all depend on the safe and secure operation of this globalized network of networks.

And yet, concerns over this domain have rapidly moved to the forefront of U.S.-China relations. While both senior policymakers and general publics are struggling to understand the cyber realm's basic dynamics and implications, the issue of cybersecurity is looming ever larger in

U.S.-China relations and is seriously affecting threat perceptions on both sides.[2] Indeed, despite it being such a new issue, the cyber realm is proving to be as challenging as the more traditional concerns that have long dominated the U.S.-China agenda (such as trade, human rights, cross-Strait relations, and regional territorial disputes).

The underlying concern is driven by the fact that the malevolent side of cyberspace has increased hand in hand with the growing scale and use of the benevolent side. There are an estimated 55,000 new pieces of malware found each day and another 200,000 computers worldwide turned into "zombies" (compromised computers under the control of an actor other than the owner) each day. These computers are often bundled together into "botnets," chains of thousands and in some cases even millions of computers externally controlled and often used for nefarious activities.[3]

But even more important than the growing numbers behind the malicious use of the Internet may be the evolution of the cyber threat landscape from one dominated by individual hackers, often motivated by a search for attention, to one driven by complex, organized groups, which range from international criminal networks to state-related espionage and military efforts. The result is that just as the positive side of the cyber domain is rippling out into the physical domain with rapid and often unexpected consequences, so too is the negative side.

The Internet thus may have no formal state borders, but it is increasingly a place that state entities both operate in and care deeply about. In U.S.-China relations, the most recent cyber trends have generally been negative. Stories about suspected "Chinese" attacks on U.S. and allied interests in both the public and private domain have become an almost daily occurrence in the media, and a source of regular discussion within the Washington, D.C. policy community.[4] In 2011, this took on a new level of concern and publicity with several major reported intrusions into American and allied government, military, corporate, university, NGO, and think tank networks. The most notable perhaps was the disclosure of the "Shady RAT" attacks that successfully targeted some 72 governments, international institutions, corporations, and think tanks.[5]

Such incidents have reportedly involved the unapproved copying and exportation of startling amounts and varieties of valuable data. The information accessed ranged from state secrets and weapons technology to business intellectual property and corporate negotiating strategies to personal files and communications of both high ranking and notable individuals and members of the general public. Some claim that if the overall scale of the loss were measured in financial terms, it would be the largest theft in history.[6]

Despite China's own blanket denials of culpability in such actions, the perception is growing at both the popular and elite level in America that the cyber threat from China, while multifaceted, has a large government-directed component. Such incidents are repeatedly described as being different from normal cyber crime in that very specific strategic objectives seemed to have been particularly targeted: inputs into decisions concerning China, monitoring and threatening dissidents who live abroad, proprietary technology of special strategic interest (a frequently cited example is that normal cybercriminals would have little to gain from targeting systems in NASA's Space Shuttle), and military-oriented planning and reconnaissance. The public debate also notes that accessing such networks for theft also can simultaneously lay the potential groundwork for future exploitation and attack.[7]

In short, U.S. concern about cybersecurity has reached a fever pitch—to the extent that the U.S. government's 2011 Office of the National Counterintelligence Executive report specifically names China as the "most active and persistent" perpetrator of cyber intrusions into the United States.[8] In the press, the mood is best captured by the depiction of a cyberattack as a massive pixilated mushroom cloud looming over every American city (as the cover of the July 2010 Economist magazine had it). Similarly, in senior policy circles, malware has been described as "like a WMD [weapon of mass destruction]" (Sen. Carl Levin, chair of Senate Armed Services Committee), able to "destroy our society" (former national security advisor Brent Scowcroft), meaning it should be looked at as "an existential threat" (Adm. Mike Mullen, former chairman of the Joint Chiefs of Staff).[9] Indeed, many are now framing the U.S.-China relationship in this space as a digital echo of the Cold War between the U.S. and USSR of a past generation.[10]

While the Cold War metaphor is certainly a flawed parallel, as scholars at Brookings have recently argued,[11] concern has grown to view the cyber threat on that scale. President Barack Obama's 2011 *Cyberspace Policy Review* declared that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century."[12] And, in turn, there have been a host of new U.S. legislative initiatives and the launch of a new cyber deterrence strategy by the U.S. military to accompany the creation of its U.S. Cyber Command. While it did not specify any individual nation, the Pentagon *Strategy for Operating in Cyberspace* was clearly keyed to China as among the many threats it foresaw in this realm.[13] It sought to lay out a cyber deterrence doctrine clearly targeting state actors, including leaving open the option for escalation to traditional military means in the physical realm if the U.S. ever felt it suffered too dearly in the cyber realm.

Unsurprisingly, Chinese writers and officials have reacted angrily to the above narrative of direct and veiled accusations, describing them as "groundless and reflecting Cold War mentality."[14] In both public and private, Chinese writers and officials assert that it is their systems that are more frequently under attack.[15] The Ministry of Public Security has noted that the number of cyber attacks on Chinese computers and websites has soared by more than 80 percent annually, and, by the raw numbers, China is the world's largest victim of cyberattacks.[16] Indeed, in December 2011, more than a dozen of China's most popular online shopping, microblogging, social networking and gaming websites were hacked, resulting in the release of more than 100 million Internet usernames, passwords and emails.[17]

Even more, many believe that China's systems are more vulnerable than are America's.[18] This assertion has merit, in part because greater use of "pirated" software by Chinese companies and institutions means that their systems typically do not get the same upgrades of protection to evolving cyber threats that normal buyers receive. Some estimate that 10 million or more Chinese computers are currently part of botnets.[19]

Chinese officials and writers also assert that most attacks on Chinese computers originate in the United States, claiming that China has been the target of some 34,000 cyber attacks from the US.[20] While the numbers are arguable, it is undeniable that a large amount of malicious Internet activity emanates from or at least moves through the U.S. For example, security researchers at HostExploit have found that 20 of the top 50 crime-spewing ISPs (Internet Service Providers—the companies that provide access to the Internet) in the world are American.[21] Also, U.S. government agencies like the NSA are active and expert in cyber operations.

Finally, Chinese actors often express a sense of unfairness. Many feel that the U.S. has a too highly privileged position in the global cyber communications world as a legacy of its seminal role in developing the Internet and many related cyber technologies. They note, for example, that of the 13 root servers that are essential to the function of the entire Internet, 10 were originally located in the U.S. (and include U.S. government operators like the U.S. Army Research Lab and NASA), and the other 3 are in U.S. allies (Japan, Netherlands, Sweden). Similarly, ICANN, which essentially manages the protocol addresses so essential to preserving the stability and smooth operation of the global Internet, started out through a U.S. government mandate.[22]

Whichever position one takes, what is even more worrisome is that such tensions and concerns are inexorably growing. The last year has amplified all of these trends. On top of this, both the scale and sophistication of attacks in cyber space has grown, notably in the Stuxnet episode. In this situation, a specially designed computer worm targeted Siemens Supervisory Control and Data Acquisition (SCADA) systems used to run the centrifuges at five Iranian nuclear research facilities. The episode was viewed as a success for counter-proliferation efforts (in that it hampered illegal nuclear weapons research in a highly focused way), but also was described in both American and Chinese circles as an indicator of a new level of threat.[23]

Indeed, two scholars at the Chinese Academy of Military Sciences released a report whose tone effectively captured the perceived level of tension and confusion this issue has generated in such a short period: "Of late, an Internet tornado has swept across the world ... massively impacting and shocking the globe. Behind all this lies the shadow of America. Faced with this warm-up for an Internet war, every nation and military can't be passive but is making preparations to fight the Internet war."[24]

In sum, distrust of each other's actions in the cyber realm is growing between the U.S. and China, and such distrust easily spills over into broader assessments of the other country's long term intentions. It is heightened by the link between the cyber domain and key values like individual privacy on the U.S. side and concerns with internal stability on the Chinese side. Even more, the potentially poisoning effect of cybersecurity on the relationship is occurring at a time when there is genuine uncertainty about the degree and speed of changes in the global balance of power. The disagreements feed into the anxieties on all sides as to whether America and China will have a basically cooperative or antagonistic relationship over the coming several decades.[25]

In traditional relations between two powers, the intersection of capability, vulnerability, and intention directs whether the states look at each other as partners or threats. Thus, the stakes in this fundamental issue could hardly be higher. Policymakers and publics on both sides must face the fact that, at this point, developments in the cyber realm are contributing to tensions rather than enhancing confidence in each side's ability to find ways to cooperate with the other to handle the major issues we collectively face in a changing world.

Special Characteristics of the Cyber Realm and U.S.-China Relations

Every policy issue has its own unique contours and problems. But what is so challenging about cybersecurity is that the cyber realm has a number of particular characteristics that significantly enhance the difficulty of establishing any consensus on norms or cooperative implementing mechanisms, especially between the U.S. and China.

Terms and Frameworks

In any new issue on the international agenda, developing an agreed-upon vocabulary and set of concepts is a requisite step, but one that can require a great deal of time and effort. Whether it is an issue of trade negotiations or nuclear weapons regimes, the basic terms may often seem simple but can prove quite difficult. For example, in one diplomatic meeting between U.S. and Chinese officials, when U.S. representatives first used the term "engagement," the Chinese were said to be baffled about whether the U.S. meant "marriage proposal" or "exchange of fire."[26]

This issue is even more challenging in the realm of cyber, as it involves both highly technical matters and also concepts where even the most basic terms can be loaded with meaning. There may have been debate about what met the definition of a cruise missile, for example, in talks between the U.S. and USSR, but there was no dispute as to whether it was a weapon or not. The same cannot be said about even such notions as "information" in the cyber realm. The provision of news on protests in the Middle East or the connections built across geographic borders via social networking tools have been described by one side as not just benign, but an essential human right.[27] By contrast, the very same thing has been described by the other side as part of an "information attack" designed to undermine state stability.[28] Similarly, "cyber-terrorism" has been used to describe everything from theoretic use of the Internet by terrorist groups to cause physical damage (such as by disrupting the operations of an air traffic control network) to the actual use of the Internet by terrorist groups to recruit members and share information on tactics and operational planning.[29]

A related problem is in differentiating between activities and intent in this space. Too often, the wide array of cyber activities that differ in nature and should be thought through separately are bundled together in discussions of cybersecurity. Take the notion of what constitutes an "attack." In both private discussion and public documents, a variety of like and unlike efforts have all been described as "cyber attacks" simply because they involve the technology of the Internet at some point.[30] The parallel for lumping together any and all malicious activity in the digital realm as similar "attacks" would be to treat the threat posed by a teenager with a bottle rocket, a robber with a revolver, an insurgent with a bomb and a state with a cruise missile as the same phenomenon simply because they all involve the same chemistry of gunpowder.

In essence, cyber attacks involve finding vulnerabilities in computers and computer networks, entering into such networks, and then copying and exporting information from such networks, and/or changing information within such networks. The problem is that this relatively simple notion can encompass a very wide array of actions and results. In a "denial of service attack," the targeted system is not actually penetrated. Rather, it is simply flooded with so many requests from other networks (often botnets manipulating hijacked computers from around the world) that it is overwhelmed and effectively ceases operations. A metaphor would be if the door of one's house was never broken down, but so many unwanted people tried to get in that legitimate guests could not make it through. The cause of such an overwhelming number of requests to enter, though, can vary. It could be anything from unintended poor network management to more purposeful actions like criminal blackmail (groups have threatened such attacks in a form of extortion),[31] political protest (such as recent "Anonymous" group efforts to target companies and institutions it felt were not supportive of Wikileaks)[32] or even strategic goals in the context of a more traditional armed conflict (such as the targeting of Georgian websites during its war with Russia, which limited the Georgian government's ability to communicate with its own populace and international parties).[33] What is more, such denial of service "attacks" are actually one of the most manageable forms of malicious activity, but even they can also serve as part of a broader strategic action—e.g., to multiply the effects of an accompanying attack on infrastructure.

The goals and consequences of attacks that actually enter into a network also widely vary. The goal might be mischief; hackers might be simply "showing off" that they can do so. Or, it might be for criminal reasons, such as to gain components of one's online identity (personal data, passwords, etc.) to use in identity theft crimes, the creation of false accounts and unauthorized transfers of money.

A particularly notable area is espionage-like efforts to gain entry into cyber systems in order to monitor activities there and to extract information. Organizations that have suffered from such entries range from governmental diplomatic bodies to international athletic monitoring organizations. In these cases, the information being monitored and stolen has been strategic. Or, the information might be intellectual property, such as a proprietary product or design, which might have great economic or even national security value. Or, it might be companies preparing their negotiation strategy against a foreign, often state-run, company. Entities that have suffered from such attacks range from consumer goods companies that have seen their designs replicated without payment to oil companies that have had their bidding strategy and drilling secrets taken to aerospace companies that have seen designs of combat aircraft stolen.[34] In short, the expansion of digital data creation, storage and transmission has created an espionage bonanza for both public and private actors—one that is being exploited to a startling degree. Indeed, while the focus of U.S. debate is more frequently on fears of a so-called "digital Pearl Harbor," as described by Secretary of Defense Panetta in his 2011 confirmation hearings, the more serious problem may actually be a long-term economic "death by a 1000 cuts."

Finally, the "attack" might involve not merely entering the system and extracting information, but also changing information within it. Here, too, the goals and consequences might vary widely. Again, the effect might be mere vandalism for mischief or for political purposes, such as defacing a public-facing website of a government institution (which happened in the aftermath of the April 2001 EP-3 incident with China).[35] It might be in the aid or execution of some sort of criminal endeavor, such as changing access or identities to allow criminals through security barriers. Or, it might seek to cause major harm of a strategic nature, such as damaging another country's ability to implement official decisions, to defend itself, or to provide necessary services to its citizens (such as delivery of electric power, health care, etc.). While relatively untested, the types of harms that might result from serious cyber attacks conceptually range from disrupting the adversary's electronic systems and what operations they enable (communications, guidance systems, radar capabilities, etc.) to actual kinetic damage accomplished by using cyber tools to cause an adversary's systems to malfunction or self destruct. A particular worry is those that target infrastructure; for example, actions that remotely open the sluice gates of dams or shut down regional power grids.[36]

Here too, the intent and the originator of the attack matters. Planting malware that degrades the functioning of a physical plant (the most famous example is the Stuxnet virus against the centrifuges in Iran's nuclear program[37]) has been interpreted as everything from an act of "cyber terrorism," to an act of "cyber war," to a lawful activity to enforce international norms in a targeted way that limits loss of life.[38] The "attack" remains in the eye of the beholder.

Such questions of definitions and terms are hugely important in policy discussion. Actors can use the same terms but with a vastly different meaning (sometimes intentional—such as via the phenomenon of threat hyping by organizations, bureaucracies, companies, and individuals that might benefit from greater levels of investment in cybersecurity).[39] But the issue of terms also has importance in domestic and international law. States regularly define the boundaries of criminal activity differently and also attach different degrees of punishment to the same activity. Liberal democracies, for example, tend to view the Internet as a place that should maximize freedom of expression, while more authoritarian states do not presume freedom of expression as a basic right. But the issue is even more complex. For example, the democracies of NATO are deeply aligned on many such issues but could not come to agreement in their own talks over a cyber crime treaty. One of the key issues was that to deny the Holocaust online is a crime in many European states, but not in the US.[40]

Attribution

Beyond just the issue of terminology, however, there are also other dimensions in the cyber arena that are especially consequential to U.S.-China relations and must inform any process aimed at engagement. Put simply, in this dynamic arena, it is necessary to be realistic about what types of activities can potentially be brought under control through agreed-upon actions and what things are effectively beyond the capacity of institutions to control. It is important to appreciate why this is so and, in that context, to focus on those areas that are still potentially subject to meaningful controls. Perhaps the most difficult is the problem of attribution.[41]

The ability to capture the operations of another computer and use it to launch activities that its owner does not intend and might even be unaware of (described inside the field as to "pwn," a computer hacker term meaning to "own") is very well developed and widely used. This often takes the form of creating botnets that link unrelated computers and enable the controller to leverage their combined computing and communications capabilities for a particular purpose. The resulting network of secretly linked devices can easily grow to extraordinary dimensions. For example, three not terribly sophisticated Spaniards allegedly created a global botnet that included over twelve million computers.[42]

In other cases, a controller may seek to capture and leverage only one or a small number of computers. In this case, the major purpose is more likely to be to conceal the controller's identity.

Three key features of this capability to capture and utilize other computers are particularly important. First, there are no geographical limits. For example, a pernicious actor in Brazil can compromise computers in Russia and South Africa to launch attacks on systems in China (one can substitute almost any countries for the ones named here). Second, the owner of a captured computer typically has no idea that the computer is being used by a remote actor for pernicious purposes. And third, when some pernicious activity is perpetrated, sophisticated analysis can typically, at best, identify the computer being used to launch the attack. It is far more difficult to determine whether that computer is, in turn, being remotely controlled and, if so, by whom. Equally, even if it is not being remotely accessed, in many situations (such as a computer being used at a university or an internet café), it will be difficult to determine who the individual behind the computer is, or even what his nationality is or what organization he actually represents. Such information would be crucial in a crisis but is rarely available in a timely manner. In short, it is typically not feasible to identify the underlying command structure behind an attack with complete certainty. Instead, painstaking forensics may be a key driver to understanding the full chain of events.

It does not take much imagination to see how pernicious the resulting problems can be. Since many are inclined to assume that the Chinese government is behind most insidious activities that are launched by computers located in China, for example, bad actors elsewhere may be inclined to capture Chinese computers to use in their activities, and vice versa for the U.S. This same logic, though, also enables Chinese bad actors to deny responsibility, arguing that activities launched from China almost certainly are being perpetrated by others who want to take advantage of the widespread suspicions of China. And the same type of misdirection can be argued regarding computers physically located inside the U.S.

The issue of attribution is further complicated by the difficulty of establishing complicity. An effort might be attributed to an actor emanating from a certain geographic locale, but it is even more difficult to establish a formal role of a government as perpetrator or sanctioner of the operation. That is, the situation often parallels that of maritime security in centuries past, where the lines between what was criminal piracy and what was state-sanctioned privateering often proved fuzzy.[43] There have been frequent reports of "patriotic hacker" communities and other non-state groups, including student and even cyber criminal groups that have been mobilized by their governments for such purposes of deniable, but directed, attack.[44] Thus, in certain cases where the local state government may be needed to investigate and then prosecute those behind questionable cyber activity, the victims perceive that some elements of the state are actually a willing accomplice or planner of the attack, and thus unlikely to assist. An example would be the DDoS attacks on Estonia. Many believed Russian security services actually instigated them and thus that Russia was certainly not interested in finding and stopping the perpetrators.[45]

Attribution is further complicated by the fact it is quite difficult initially to determine even whether a packet is intended to be "hostile" or not (as one expert put it, "Packets are not like ICBMs"). A DNS query, for instance, may be a legitimate look up attempt or it may be an attempted penetration. And, even in the latter case, it may be a legitimate DNS lookup or it may be part of a large scale DDoS attack. On top of this, once malware enters into a system, it does not necessarily bear a telltale sign of where it was designed and sometimes even what its actual intent may be. Unlike fissionable materials, for example, where each nuclear reactor has a distinctive "signature" that typically permits tracking the origins of the material, even when malware is uncovered it usually does not point a finger at a particular culprit.

The long-running effort to figure out the origin and intent of the Conficker worm illustrates this problem. The worm was one of the most effective in recent history, assembling a global botnet of some 7 million compromised computers in networks that ranged from the British Parliament to Southwest Airlines to the French and German military to scores of computers in China (one security expert called it "the Holy Grail of a botnet"). Yet, even as the worm spread, investigators could only sift through the data for clues to its origin, which still left them uncertain. In one breakthrough, they found certain programming linked to a Ukrainian language keyboard. But, even then, they could not conclude whether this meant the malware was designed in Ukraine or whether the clue was a clever attempt at misdirection.[46]

Offense Has the Advantage

In any issue of security, there is a premium on defending oneself to make attack less effective and potentially creating some form of deterrence to dissuade future attacks. The challenge in the cyber security domain is that the one seeking to penetrate a computer network, at least so far, is at a great advantage relative to the defender.

At its most basic level, the Internet was designed to share information easily, not prevent its flow. Similarly, most of the products and systems that link into this network of networks were not designed with security embedded into them. Rather, there are many vulnerabilities that can be exploited. Moreover, even the very manner of updating and "patching" security vulnerabilities relies on the ready flow of information to let users know about new risks and how to fix them.

Many feel that this trend will only continue, with the relative advantage of the offense in the cyber realm growing further. The technical tools for penetration and extraction without (or at least before) detection continue to improve exponentially. Even more, the tools exist now for turning other electronic devices that people have in proximity to their computer networks into espionage platforms. Keylogger technology, for example, can be used to remotely track the buttons one uses on the keyboard through malware inside the computer. Other malware may remotely turn on the camera and microphone of a computer or other device in a room to monitor what is happening.[47] In Oct. 2011, it was revealed that such malware had even penetrated the supposedly secure networks used to control U.S. military drones.[48]

Passwords are, moreover, increasingly vulnerable. Technology to break passwords has reached the point that most passwords other than very sophisticated "highly secure" ones can be compromised by those with the available advanced tools.[49] In addition, at some administrative level in networked organizations, there are one or more files that contain the passwords of everyone who uses that network—and those files can themselves be compromised.

More broadly, the sophistication of approaches to gaining unapproved access is increasing more rapidly and effectively than is generally appreciated. A particularly worrisome change in the environment of cybersecurity has been the rise of what are known as "advanced persistent threats," or APTs. Rather than the randomized, quick hit attacks of the past, in an APT operation a specific individual or organization is identified by a group, and the sort of complex resources and techniques traditionally used by espionage professionals are used to go after the targeted network over an extended period of time. An APT features teams of professionals with varied skill sets (intelligence gathering, infiltration, exfiltration, etc.) working together. The target's internal organization, chain of command, norms of behavior, and even social dynamics are studied and mapped out to figure out who matters and who does not and what key vulnerabilities can be compromised. Social networking, in particular, has allowed people to share more and more about themselves online. But it has also created enormous new sources of detailed data on individuals that is used, in turn, to develop pathways and strategies to penetrate computer networks to which those individuals—or their online "friends" or friends of friends—have access.[50]

In sum, while there are cyber defenses that are very sophisticated and fairly widely deployed, it is usually more challenging to prevent, and even detect, malicious activity of a sophisticated nature. Indeed, even the defense method of "air-gapping" one's computer networks has not proved to be a remedy. The Iranian facilities hampered by Stuxnet were not directly connected to the Internet but still had malware enter them (probably by naïve individuals bringing across software physically).[51] The same has happened on multiple occasions to U.S. defense networks, in one case when users literally plugged in memory sticks they had found in a parking lot (thought to have been distributed by a foreign intelligence organization) into computers on classified networks.[52] Constant efforts are needed, therefore, to build user awareness, upgrade defensive capabilities, and ascertain what data has been lost or compromised. But a basic reality of cyber security at this point is to accept the cold hard fact that the defense is at a disadvantage. It is telling that even the vaunted U.S. National Security Agency, arguably the most sophisticated entity in the world at cyber issues, operates on the assumption that its networks are compromised—but most other agencies and users around the world do not.[53]

Historically, an imbalance in favor of the offense raises the incentives to act maliciously and at a quicker pace, while it also lowers each side's confidence in its ability to deter attack and defend itself effectively. Such real or perceived advantages of offense over defense can be destabilizing and make trust building all the more difficult.[54]

Time in the Cyber Realm

"Time" is a curious notion in the cyber realm. Take, for example, the notion of a "zero day" attack. This is an attack that occurs on or before the first (or "zeroth," so called by the numbering system used in computer programming) day that the user is even aware of the vulnerability that the attacker is exploiting. Thus, there can be an indeterminate period of time that elapses between when malware is actually inserted into a network and when some observable development triggered by that malware. This again complicates efforts to determine attribution with a high level of confidence.

As an illustration, the Stuxnet virus was thought to have begun taking effect on the Natanz nuclear centrifuges in Iran in mid-2009. But the virus wasn't discovered until June 2010, not by the Iranians, but by a Belarusian cybersecurity firm. That the malware was designed to target industrial processes wasn't understood for another month, this time discovered by U.S. cybersecurity researchers. Even then, the specific target the malware was actually going after was widely debated, with researchers believing it to be anything from Iran's Bushehr nuclear power plant to an Indian satellite that had dramatically failed on launch. It wasn't until November 2010, after a full year, that researchers at a German industrial security firm and an American cybersecurity firm pieced together that Stuxnet had been specifically designed to go after the frequency converter drives used in the nuclear centrifuges at Nantanz (causing them to randomly speed up and slow down, effectively wrecking their ability to produce refined uranium fuel).[55] Up to then, the Iranian targets, in the words of one researcher, had "no clue of being under a cyber attack." Instead they were just continually replacing broken centrifuges with new ones, in what the expert called a cyber form of "Chinese water torture."[56]

But the problematic issue of time in cyberspace hits hard in three additional ways. The first is the constant growth and evolution of technology and how we use it. Information technology is an ever changing domain where the hardware and software, and the threats and responses to them, may become quickly outdated. Most malware was originally designed for computers operating off of fixed lines, for example. Today, much of computer activity is moving onto mobile devices, and the threats are following.

Even what constitutes the internet itself is evolving in a fundamental way. It is becoming far more personalized, where rather than just passively receiving online information, the individual users are creating and tailoring sites to their personal use, as well as revealing more of themselves online. The accelerators in this evolution range from social networking sites like Facebook in the U.S. and RenRen in China to microblogs like Twitter and its Chinese equivalents Tencent and Sina. Indeed, microblogs (called Weibo) have taken off to the extent that the total number of registered in China hit 550 million at the end of 2011.[57] In addition, our world is becoming re-architectured into "an Internet of Things," where more and more of the goods and services we use in our daily lives, from the food we buy at a store to the electrical power in our homes, are being linked into the online world via everything from RFID tracking codes to smart electricity grids.

This rapid change is fundamentally increasing the ability of outside actors to acquire detailed information about individuals unimaginable in the past and thus to leverage cyber activities to have ever greater impact in the real world. The problem is that, while the cyber realm is moving at an exponential pace, the policy world often moves at a slower (or even glacial) pace. Thus, it is inevitably at risk of being fundamentally out of synch.

On top of this natural evolution, there is proliferation. Any new cyberweapon used in a successful attack usually remains on the network, left there for others to copy. Many thus believe that known threats should not be publicly identified, as to do so is to let their makers (and would be copycats) know they need to evolve and move on.[58] But this, in turn, makes collaborating about solutions and spreading protective measures more difficult.

Secondly, decision making time is, in effect, compressed in cybersecurity, at least in policy terms. Governments are used to operating on a scale of days, weeks, and months as they make their policy deliberations and decisions. In the cyber realm, while proper preparations for an attack may require weeks or months, the actual elapsed time for its successful execution may be counted in nanoseconds. Thus, the normal processes of governments and institutions to decide how to respond may simply be irrelevant to the problem. This raises the need for prior planning and preparation. But fully automated responses rest on the assumption that the nature of an attack can be anticipated (and therefore recognized instantaneously) and that the automated response can be calibrated so that it does not in itself risk doing greater damage if the initial signal of an attack proves to have been wrong. History suggests that both of these are very shaky assumptions.[59]

There is also a generational dimension to the issue of time in the cyber realm. There is a clear break between today's "digital natives," the youth who have grown up in a world where computers have always existed and thus are a natural aspect of their world, and anyone from older generations, for whom computers are something to which they have had to adjust (so-called "digital immigrants").

People of any age can use and act inside cyberspace—and indeed, one of the great benefits of the realm is how it allows users to extend beyond their physical limits. But the very best innovators are typically those of the younger generation, who grew up in a cyber environment, are deeply engaged with it, and have natural talent for developing new approaches in this space. Thus, much of the innovative capability in cybersecurity is in the hands of individuals who are too young to have moved very far up institutional hierarchies. To put it another way, few American or Chinese policymakers in their 40s will have gone through their university training even using a computer. Even the few that did so used computers that, at the time, were not linked to the internet and had far less power than what a child's toy has today. And, the most senior leaders in their 60s and 70s likely did not even become familiar with computers until well into their careers, and many still today have only the most limited experience with them.

The result is that the policymakers most likely to be in positions of power are often the most uncomfortable even talking about these issues (here too, the metaphor of an "immigrant" is useful, as the senior leader discussing cyber issues often feels like a stranger in a new land, unable to speak the language, and thus more likely to keep silent for fear of embarrassment or misunderstanding). This disadvantage of time and experience also affects their sense of control. Often, the people on the front line of cyber issues are able to do far more than their elders in supervisory or policy development roles can fully understand. Many of these young innovators, moreover, thrive in the cyber realm for the very reason that they do not easily fit into old organizational structures and bureaucracies. This aids their creativity, but also means that they often do not understand or accept the old procedures and models of what used to be right or wrong.

Decentralization

It was noted earlier that cyberspace is populated by both public and private actors. This raises an additional problem of decentralization and scale.

While the impact of individuals is often overstated in cyber security (the best types of malware often require the cooperation of multiple experts skilled in a variety of areas rather than the popular trope of a single teenaged hacker in his parents' basement), the cyber realm is one in which small groups can potentially generate enormous consequences. In software programming, the productivity difference between a good and an elite programmer can be orders of magnitude. This means that governments cannot simply throw money and manpower at the problem. The cybersecurity expert who discovered Stuxnet, for example, has discussed how he would rather have 10 experts of his own choosing versus all the resources of the U.S. Cyber Command at his disposal.[60] While this is debatable, the fact is that small groups or organizations can be meaningful in a manner unimaginable in earlier times. New malware can be extremely harmful on a global scale and yet be developed and deployed by only a few people.

But the key is not just these groups' power, but their ability to share it. Those same groups or individuals can, if they wish, almost instantaneously communicate knowledge of how to create any new capability to millions of others. For example, it may have taken the combined efforts of a team of experts to build Stuxnet, but within weeks of its discovery, an Egyptian blogger had posted a how-to guide for this new cyber-weapon online.

The proliferation can take two paths. Many might only be able to use the new capability "as is," as security experts lament that a number of infrastructure companies have still to plug vulnerabilities that Stuxnet exploited.[61] Others, however, might learn from the new cyberweapon and be inspired to build even more sophisticated advancements. Duqu, for example, is a new worm that uses Microsoft Windows-exploiting code similar to Stuxnet, such that many are calling it "son of Stuxnet," with the idea that it must be the next version designed by the same team. However, while there are key similarities, experts also have noticed key differences and thus now believe that it was more a case of inspiration than evolution.[62]

In short, the cyber realm does not require large human, financial, or physical resources in order to act at scale. It is, moreover, a sphere in which learning can take place at great speed among those on the cutting edge. Never before in history has scalability of threat been so easy to achieve.

The multiplicity of actors issue grows even more difficult with the problem of affiliation (closely related to the previously discussed issue of attribution). Unlike in the sphere of military activities, where mature states have a monopoly on the large scale use of force, in the cyber realm capabilities are typically widely distributed and do not often reside in organizational hierarchies. Many hackers form virtual communities with a loose or nonexistent inherent hierarchy or fixed membership. While some efforts are described as perpetrated by "patriotic hackers," whose activities often have state sponsorship or at least cognizance, membership in hacker communities is often transnational. The "Anonymous" movement, for example, has brought together disparate groups that collectively agree to a target (usually some entity the group believes is harming digital freedom, which has ranged from authoritarian governments to credit card companies that were not allowing donations to Wikileaks) and mobilize the global "hacktivist" community to enter and/or overwhelm a target's networks.

Most worrisome, though, is an underground black market-based approach to creating and distributing malware, in which transnational criminal groups buy and sell specialized cyber capabilities.[63] Just as in the physical realm, these same criminal groups have been suspected of, on occasion, acting on behalf of states, especially in efforts of espionage and warfare.

The lines between state and non-state actions in the cyber world are thus often shifting and blurred, and the above-noted difficulties in exercising effective control over front-line developers of new cyber techniques, even among state actors, contributes to this permeability between the state and non-state sectors. This both aggravates the problems of attribution and provides states with plausible deniability when they are accused of malicious activity in the cyber realm.

But just as there is no one focal point on the side of malicious actors, there is also decentralization in the institutions to which one might turn to deal with them. A variety of state and non-state entities provide some form of Internet governance (from ICANN to the ITU), but no one organization is central to Internet governance on the international level.

The same holds true within states. A complaint frequently levied by U.S. leaders from both the private and public sector is that the Chinese decision making system, especially in cybersecurity, is quite opaque to them.[64] There is a comparative lack of transparency in China's computer network operations, and when the U.S. officials and private sector leaders do want to reach out to Chinese counterparts to coordinate, cooperate, or simply provide information exchange on matters of mutual interest, they are not quite sure which institution and which individual is the appropriate node—or even whether the Chinese themselves know. But the same can be said by Americans of their own nation's cybersecurity efforts. A wide set of U.S. agencies and actors believe themselves to be the lead in cybersecurity, but their capabilities and jurisdictions vary greatly. Rather than being well coordinated, each nation's cybersecurity efforts could be better described as nascent and ad hoc. This is not a recipe for easy cooperation.

An additional complication is that in U.S.-China relations since the 1970s, the U.S. State Department and Chinese Foreign Ministry have been the primary ministry level vehicles through which the two nations have managed their relationship, a natural aspect of the centuries-old practice of diplomacy. But, in the 21st century, this presents a mismatch to the problem. The reality is that neither of these agencies has any significant power over their own country's internal deliberations on cybersecurity, nor any depth of expertise on the topic itself. So the two agencies that have been the usual intermediaries for U.S.-China relations have not yet been effective players on this issue of rapidly growing importance between the two nations.

Bottom Line: What Would A U.S.-China Agenda Look Like in Cybersecurity?

All the major countries of the world are engaged in various forms of cyber security activities as part of state-directed efforts. All have built cyber based capabilities and requirements into their governmental processes, military capabilities, and economic activities. Every major state is, therefore, vitally concerned with the security of its own cyber activities and its capacity to understand what others are doing in this realm.

But uncertainties abound in this space, especially between the U.S. and China. As explained above, many of these uncertainties will be difficult if not impossible to reduce substantially. Neither attribution nor institutional control problems are likely to diminish significantly anytime soon on their own. And thus this sphere is one in which suspicions and fears understandably easily mushroom.

This does not mean that a pure focus on competition, which would only further fuel suspicions and insecurity, is the answer. Rather, an agenda for cooperation can be built that is realistic in recognizing the above difficulties but still provides a basis for serious U.S.-China discussions about common steps to take in the cyber realm. It can respect that each government will protect its ability to use cyber capabilities to carry out espionage activities and support military activity should that become necessary. It can recognize that the two political systems have significantly different views concerning freedom of information in cyber space. It can be sensitive to the fact that in each government decision making concerning cyber activities is fragmented among many bureaucracies and is not well coordinated at any single node in the system. And finally, it can acknowledge the reality that a variety of nongovernmental actors are significant players in each country's use of and deliberations about the cyber realm.

Expand Engagement

Cybersecurity issues have been discussed in official meetings between U.S. and Chinese officials, and there are known to be a limited number of "track two" meetings of an unofficial nature between key individuals.[65] But the scale of the engagement today is simply inadequate to the task at hand. During the Cold War, Soviet and U.S. interlocutors who specialized on nuclear talks numbered in the hundreds, and the wider leadership was comfortable with the terminology and concepts of the field. By contrast, the numbers of those engaging on these issues between the U.S. and China today are nowhere near that scale, and the wider leadership of both sides remains far more comfortable using a Cold War vocabulary of ICBMs and deterrence than it does ISPs and cybersecurity. The goal should be to develop a broader cadre of people who utilize the same vocabulary, are respected by their own leadership, and have trust in each other's sincerity and gravitas.

In any such effort, substantial time should be allowed to develop mutual understanding and trust. Whether the setting is an unofficial track two, an official track one, or the new variety of "track 1.5s" (where some serving government officials particiapte in a non-governmental dialogue), a good initial approach is to have each side explain its own views on a core set of issues, with questions and discussion focused on increasing mutual understanding of these views and the premises and experiences that lie behind them.

This is not a stage that should be rushed. One of the most important and difficult dimensions of moving toward agreements in cyberspace is understanding the perspectives that the other side brings to the table—its goals, fears, suspicions, assumptions, and approaches. Explanations by each side of how they came to a certain viewpoint can then move towards how the collective group can address some common problems—and of the most difficult obstacles and concerns they might encounter. The idea is to gradually move the discussion in the direction of having both sides sit on the same side of the table addressing a common concern, rather than limiting the meetings to a structure that encourages adversarial negotiations.

Focus initially on activities that virtually all states deem harmful and discuss both principles and methods to reduce the harm

All states have strong interests in establishing credible limits to certain types of harmful activities that can be developed and acted upon. Where states agree on what constitutes harmful activity (called by some "double crimes," in that they are recognized by both sides), they should be able to find ways to cooperate to deal with those activities, given the inherently transnational nature of the cyber world. To be constructive in building mutual confidence, these discussions should focus on activities that do not have a significant political component to them (such as criminalization of free speech). Examples of topics include dealing cooperatively with criminal activity such as child pornography or human trafficking. These are obvious examples of a type of activity that most states regard as clearly criminal but which in the cyber realm has an international character to it. Discussions and negotiations that initially focus on finding cooperative ways to define and deal with double crimes may, therefore, become a good first step in the process of understanding mutual goals and concerns, facilitating efforts at norm building and enhancing the basis for mutual trust.

The focus should remain on mutual interests, even as the discussion begins to turn to more political or contentious areas. For example, while the U.S. and China may not yet see eye to eye on various cybersecurity issues, they clearly have a joint interest in distinguishing a cyber attack from the unintentional consequences of some more benign activity and ensuring the protection of information and communications that are important to trade and economic stability.

Examine models of cooperation

As a new space in international relations, there are characteristics peculiar to the cyber realm that limit the applicability of any particular previous model for how to approach the negotiation. This does not mean that the past isn't a useful guide for moving forward. As the American writer Mark Twain once put it, "History doesn't repeat itself, but it does rhyme."

One way to build mutual understanding and cooperation is to jointly discuss in detail the advantages and disadvantages in applying potentially useful existing models of cooperation to discussions of cyber security. One such model to consider might be the effectiveness of Track IIs in arms control negotiations, especially at the nuclear level.[66] While there are obvious limits, this has the benefit of being a proven area, and one in which many U.S. policymakers have had experience. The challenge, however, must be to both recognize that Chinese counterparts may not have the same experience, and that the parallel of arms control or even trade talks immediately puts the discussions into a competitive framework.

An alternative way of thinking about cybersecurity is to regard the cyber realm as more like an ecosystem. Rather than a competition between two actors, it is a vast domain that is made up of multiple actors that interact and even compete, but all of whom depend on the overall health of the system.[67] This would make public health the more apt parallel. Such a new way of framing the issue allows the sides to examine both the mutual risks and the cooperative measures that can be taken at the global, state, and public-private level to ensure the health of the system (which is in every group's interest). For example, the future of a healthy cyber ecosystem will rely less on each side's building up offensive capability than on cooperative engagement in information sharing and defensive measures, as is the case in fighting infectious disease.

Finally, the actors might absorb the lessons learned to date from dealing with global terrorist finance. Just as international banks have been held responsible for not processing transactions that may be for terrorist organizations, there might be measures by which the key intermediaries in cyberspace, ISPs, might take on more responsibility for the malicious activity that uses their services. The idea is not to equate them with villainy but rather to explore what can be learned from the successes (and failures) of warnings to international financial institutions to stop processing financial transactions of terrorist organizations.[68]

Cooperatively address key principles and approaches

No agenda of building cooperation in this space can move forward very far without some kind of discussion on how the sides view the key aspects. There does not have to be complete agreement on the various terms and definitions and the like. Instead, the focus should be on identifying not only the areas that might lead to agreed principles and approaches, but also the key questions and principles that are too difficult to resolve. Discussions of intractable arenas can deepen mutual understanding of the differing underlying assumptions and concerns that make them so difficult, and thus, to some degree, increase the prospect for addressing some of these issues—or at least of somewhat limiting their negative effects—over time.

Moreover, while there may not initially be any basis for agreement on the most contentious areas, there may emerge agreement within even the contentious areas on underlying concerns to both parties. For example, there may be wide disagreement on what constitutes an "attack," but coming to agreement on the definition of certain types of targets could prove very useful. For example, mutual agreement on what constitutes "critical infrastructure" might end up making it easier to protect such infrastructure than it is to disable it.[69] This is analogous to what happened in nuclear arms control in which the parties did not always agree but found common interest in seeking to limit weapons that created an incentive to strike first or destabilize relations, such as MIRVs.[70] While likely all major powers want to be able to use cyber attacks to disrupt their enemy's critical infrastructure in case of war, they also have a shared interest in promoting "defense dominance" in this realm. Similarly, declarations of "no first use" (a position taken by China in nuclear issues) could have some salutary effect in building mutual confidence.[71]

Make explicit the norms that are currently built into the global internet system and devise ways to cooperate on low level violations

The norms and agreements that allow the smooth functioning of the Internet are wide ranging and substantial, but overwhelmingly the system still runs on handshake agreements between the various entities and ISPs that provide the Internet backbone. A cooperative effort to make widely accepted norms explicit can both increase mutual understanding and confidence and also provide a better template for addressing more complex issues.

With basic agreement on the common existing norms of the system, better ways can be designed to cooperate in addressing low level violations in cyber space, such as the ubiquitous problems associated with spam.[72] Spam may sound like a nuisance issue to senior policymakers, but it actually is one of the key issues clogging the Internet and keeping it from providing maximum advantage in communication and innovation to all users, whatever their nationality. More pertinently to cybersecurity, high end threats consistently use low end appearances as disguises to gain access. It is also one of the key aspects of the offensive advantage. Those tasked with defending even advanced networks (such as critical infrastructure, defense contractors, or government agencies) have noted that they spend vastly more time, effort, and money on activity to address the type of generic problems of spam and low-level worms that hit all users of the Internet than they do on the APTs that are targeting their secrets and hold the potential for far greater harm. Developing robust approaches to dealing cooperatively with low end threats can, therefore, have significant payoffs across the board.

Focus on the attribution problem

The centrality of the attribution problem cannot be overstated, and thus it cannot be avoided for long. There might be greater concord in seeking to find a middle ground between the dangers of anonymity and the positives that come from the freedom of action that so defines the Internet. For example, there may well be technical and policy ways to establish a mechanism by which one could know that messages A and B were sent by the same person (a useful tool for identifying and sifting out malicious actions) without knowing who that person was. Even if there is no way adequately to address the attribution problem, discussion of the issue, its consequences, and how to cope with it can itself be of value in enhancing mutual understanding and trust.

Discuss the "red lines" that could provoke major conflict if crossed

Cyber war, like cyber crime, is a realm in which there may be real gains for all players to come to agreement on what actions might risk generating a wider conflict. This is useful not only for each side to know, so as to avoid investing in and using capabilities that would unintentionally escalate a crisis, but also to try to generate certain norms and implementing mechanisms to take such risky actions "off the table." Any such agreements—and even the process of negotiating them—can increase mutual understanding, decrease distrust, and make each country less inclined to react precipitously to any indication of danger.

The Cold War provides examples of the problem of lack of clarity in such "red lines" of behavior. In 1962, the U.S. and USSR had not effectively communicated to each other their red lines on where nuclear weapons might be located and what behavior would trigger escalation. That is, neither side was happy about the other developing such capabilities, but each side unintentionally deployed them in a manner (the U.S. putting missiles into Turkey and the Soviets into Cuba) that raised the level of tension and provoked a reaction well past what they expected. The outcome was the Cuban Missile Crisis, where competition moved into destabilization and near thermonuclear war.

Today, the U.S. and Chinese doctrines in cyber space are quite similar in their deliberate vagueness and, indeed, quite parallel to the situation in the late 1950s and 60s. For example, the U.S. Defense Department cyber strategy published in 2011 announced a new doctrine, arguing that harmful action within the cyber domain can be met with a parallel response in another domain.[73] This has come to be known as "equivalence."[74] Aiming for such flexibility is certainly sensible from one angle, but problems emerge when it is weighed through the lens of a competition between two states. Substitute the words "conventional" and "nuclear" for "cyber" and "kinetic" and the new doctrine is fundamentally similar to the 1960s nuclear deterrence doctrine of "flexible response" that possibly helped lead to the Cuban crisis. The Chinese cyber strategy is even more opaque, much like the Soviet nuclear strategy was to U.S. leaders at the time.

Coming to such agreements on red lines of behavior is surprisingly possible even in the most contentious realms. For example, much of the pernicious state-sponsored activity in the cyber realm today is related in some way to espionage. But even at the height of the Cold War, the CIA and KGB were able to come to an informal set of agreements to avoid certain types of behavior. Neither side liked the other stealing secrets from it, but the two agencies were able to communicate a set of activities and targets that were to be avoided by both in order to keep their competition in the espionage realm from escalating into something more serious.[75]

In short, no one should expect all disagreements to be easily resolved or the two sides to give up their core interests or values, nor that certain codes of conduct won't change as situations evolve. Rather, the goal is to communicate one's interests and values effectively. Many believe that this will actually be in each party's own interest, as it will aid their respective deterrence strategies. As General James Cartwright (ret.), former Vice Chairman of the Joint Chiefs of Staff, and one of the key figures in the development of U.S. cybersecurity strategy, notes, "You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you."[76]

Most importantly, it will clarify to each side the paths of behavior that will be viewed as egregious and provoke serious tension and responses that neither side wishes to see happen. That is, even if no formal agreement is possible, there is great value in having serious discussion to start the process of communicating each side's "red lines," what they would view as unacceptable behavior in the cyber realm that could lead rapidly to a crisis. This discussion is important in that it will inform the policymakers that there are legitimate concerns on each side and potentially provide some clarity on prospective escalation paths that can then be avoided.

There is also a critical potential side benefit of such a discussion about red lines and escalation paths. It can also promote healthy attention to the issue *within* each government. It will allow leaders to better understand not just what the other side is thinking but also what their own agencies and related non-state entities might be doing and the potential consequences. This is something that most senior policymakers on both sides are not sufficiently focused on at present.

Conclusions

The U.S.-China relationship is among the most important in the world. Both sides draw great benefit from the smooth functioning of the Internet. But the issue of cybersecurity threatens to become a major source of friction. The danger is that the technology that so connects the world will instead drive these two nations apart.

Given what is playing out, it is especially important that Washington and Beijing begin to build the bases for greater mutual understanding, cooperation, and development of common norms in how they deal with the many issues emerging in cybersecurity. Such bilateral efforts certainly should not stand in the way of various multilateral initiatives along similar lines, but focused bilateral dialogue is of great potential value.

No one should expect the issues to be resolved any time soon. Any discussions in the cyber realm must take account of the relative newness of this issue (even terminology concerning key concepts is not fully standardized), the dearth of effective coordinating mechanisms within both national polities, and the high level of mutual suspicion that already exists concerning motives and activities in this space. The potential of cyber space for espionage is so overwhelming that it is unrealistic to seek cooperative agreements to govern this part of the problem. The same is likely true of issues in which there are serious disagreements over values, such as the extent to which citizens should be free to voice views that the government considers harmful to stability. But the fact that the arena has so many daunting characteristics does not in any way reduce the importance of working to build greater understanding and cooperation in this space. Instead, it should make the ongoing failure to develop cooperative approaches and common norms all the more disturbing.

Establishing greater mutual understanding and trust will be a difficult process. It will require consistent efforts over time, common approaches to structuring the discussion, and selection of topics that hold the most promise for permitting increasing understanding of perceptions, goals, and mutually acceptable approaches and methods. The path will be a challenging one for both U.S. and Chinese experts and officials, but important things cannot be accomplished without a dedicated effort.

And, it is an effort that must begin soon. In Chinese there is a proverb, "Ice does not freeze three inches thick from one day's cold." This adage is akin to the proverb in English that "ancient Rome was not built in a day." These old sayings still hold true, even more so in the fast-moving world of cybersecurity.

The U.S. and China relationship is critical both to the Internet and its billions of users, as well as to overall global order beyond the world of cyberspace. If these two nations are to set both realms towards a more positive future, then facing the challenges of cybersecurity is an imperative today.

Endnotes

[1] “Security in Embedded Devices,” McAfee presentation, June 22, 2011.

[2] Richard D. Fisher, Jr. “Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People’s Republic of China (PRC),” Testimony before House Committee on Foreign Affairs, Oversight and Investigations Subcommittee, Hearing on “Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology.” April 15, 2011; Larry M. Wortzel. “China’s Approach to Cyber Operations: Implications for the United States,” Testimony before House Committee on Foreign Affairs, Hearing on “The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade.” March 10, 2010. Shen Yi, “网络安全与中美安全关系中的非传统因素 (Cyber Security and the Non-traditional Elements in Sino-U.S. Relations),” 环球视野 (Global View) 322 (4, 2010) http://www.globalview.cn/ReadNews.asp?NewsID=22733.

[3] Marc Brown, “Embedded Device Security in the New Connected Era,” *Electronic Engineering Journal*, accessed Sept. 26, 2011, http://www.eejournal.com/archives/articles/20110818-windriver/.

[4] Examples include attacks on Japan’s biggest defense contractors such as Mitsubishi Heavy Industries starting from August, 2011; cyber attacks on Google and other 34 companies in January that lead to Google’s exit from China; hacks into Canadian government computers in January; a major breach of IMF in June; Sources: Hiroko Tabuchi, “U.S. Expresses Concern About New Cyberattacks in Japan,” *New York Times*, September 21, 2011, http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html. http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all. Greg Weston, “Foreign Hackers Attack Canadian Government,” CBS News, Feb 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html. David E. Sanger and John Markoff, “I.M.F. Reports Cyberattack Led to ‘Very Major Breach,’” *New York Times*, June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

[5] David E. Sanger and John Markoff, “I.M.F. Reports Cyberattack Led to ‘Very Major Breach,’” *New York Times*, June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

[6] Ibid.

[7] Michiko Kakutani, “The Attack Coming From Bytes, Not Bombs,” *New York Times*, April 26, 2010, http://www.nytimes.com/2010/04/27/books/27book.html?pagewanted=all

[8] Office of the National Counterintelligence Executive, “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,” October 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[9] Nominations of Vice Admiral James A. Winfield, Jr., and Lieutenant General Keith B. Alexander Before the Senate Armed Services Committee, 111th Congress, available at http://armed-services.senate.gov/Transcripts/2010/04%20April/10-32%20-%204-15-; Karen Parrish, “Mullen Offers 40 year Perspective on Social, military Issues,” American foreign Press Service September 23, 2011.

[10] Former National Security Adviser Brent Scowcroft, for instance, describes the Cold War and cybersecurity as “eerily similar,” while journalist David Ignatius summed up his meetings with top Pentagon officials in an article titled “Cold War Feeling on Cybersecurity.” David Ignatius, “Cold War Feeling on Cybersecurity,” *Real Clear Politics*, August 26, 2010, http://www.realclearpolitics.com/articles/2010/08/26/cold_war_feeling_on_cybersecurity_106900.html.

[11] Noah Shactman and PW Singer, “The Wrong War,” *Government Executive*, Oct. 15, 2011 http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx.

[12] Ronald Deibert, “Tracking the emerging arms race in cyberspace,” *Bulletin of the Atomic Scientists*, January/February 2011 vol. 67 no. 1, p. 1-8 available at http://bos.sagepub.com/content/67/1/1.full

[13] Department of Defense, *Strategy for Operating in Cyberspace*, July 2011, available at http://timemilitary.files.wordpress.com/2011/07/d20110714cyber.pdf.

[14] Jiang Yu, a representative of the Chinese MFA, as quoted in “Also China Denies Pentagon Cyber-Raid,” http://news.bbc.co.uk. September 4, 2007.

[15] An example is “China was accused time and again for launching cyber attacks abroad but there was never any solid proof. Actually, China has become a victim of such repeated claims.” Su Su Hao, an expert on international security at the China Foreign Affairs University, in Ai Yang, “Nation needs ‘more Internet security,” *China Daily*, Dec. 29, 2010.

[16] Ai Yang, Ibid.

[17] Lea Yu and Xuyan Fang, “100 Million Usernames, Passwords Leaked” (Caixin Online: December 29, 2011): http://english.caixin.com/2011-12-29/100344138.html.

[18] “2011年6月2日外交部发言人洪磊举行例行记者会(June 2, 2011 Ministry of Foreign Affairs Press Conference with Spokesperson Hong Lei),” accessed September 26, 2011, http://vancouver.china-consulate.org/chn/fyrth/t827448.htm. Zhang Zhaozhong, “中国服务器网络安全面临很大威胁 (China’s Servers Network Security Faces Great Danger),” Xinhua News, May 18, 2010, http://news.xinhuanet.com/mil/2010-05/18/content_13511986.htm. “专访国家互联网应急中心:中国是黑客攻击的最大受害国 (Exclusive Interview with State Internet Emergency Center: China is the Biggest Victim of Hacker Attacks),” Xinhua News, January 22, 2010, http://news.xinhuanet.com/politics/2010-01/22/content_12859136_1.htm.

[19] Shaun Waterman, “China Open to Cyber-attack,” *The Washington Times*, March 17, 2011, accessed September 26, 2011, http://www.washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=all. “著名IT杂志称：中国已成为黑客攻击热门目标 (Famous IT Magazine Claims: China is a Heated Target for Hackers),” Renmin wang, accessed September 2, 2011, http://it.people.com.cn/GB/42891/42894/3308326.html.

20 “中国是”间谍软件”最大受害国 美国攻击最多 (China is The Biggest Victim of Spyware, Most Attacks Origin from U.S.),” Xinhua News, April 10, 2009, accessed September 26, 2011, http://news.xinhuanet.com/mil/2009-04/10/content_11163263.htm.

21 Noah Shachtman, “Pirates of the ISPs,” Brookings Cybersecurity Paper, June 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cybersecurity_shachtman/0725_cybersecurity_shachtman.pdf

22 “谁掌控了我们的服务器 (Who Controls Our Servers),” *International Financial News*, August 20, 2009, 2. http://paper.people.com.cn/gjjrb/html/2009-08/20/content_323598.htm.

23 “The FP Survey: The Internet.” *Foreign Policy*, September/October 2011. P 116; Wu Zhenglong, “震网的警示 (Stuxnet’s Caution),” Jiefang Daily, February 10, 2011, 4.

24 Ye Zheng and Zhao Baoxian, writing in the China Youth Daily, as reported in “Chinese Military Scholars Accuse U.S. of Launching Internet War,” NPR, Oct. 11, 2011 available at: http://www.npr.org/blogs/thetwo-way/2011/06/03/136923033/chinese-military-scholars-accuse-u-s-of-launching-Internet-war.

25 Chen Qun, “奥巴马政府的网络安全战略分析 (Analysis of Obama Administration’s Cyber Security Strategy),” *Contemporary International Relations* 01, 2010: 11-16. Cai Cuihong, “试析“9·11”后美国国家信息安全战略 (Analysis of Post 9/11 U.S. National Information Security Strategy),” *Fudan American Review*, 00, 2006. James A. Lewis, “Cyber Security and U.S.-China Relations,” *China U.S. Focus*, July 6, 2011, accessed September 26, 2011, http://www.chinausfocus.com/peace-security/cyber-security-and-us-china-relations/. Adam Segal, “The Role of Cyber Security in U.S.-China Relations,” *East Asia Forum*, June 21, 2011, accessed September 26, 2011, http://www.eastasiaforum.org/2011/06/21/the-role-of-cyber-security-in-us-china-relations/.

26 King Jr., N. and J. Dean (Dec. 7, 2005). Untranslatable Word in U.S. Aide’s Speech Leaves Beijing Baffled; Zoellick Challenges China To Become ‘Stakeholder’; What Does that Mean? *The Wall Street Journal*.

27 Hillary Rodham Clinton, “Remarks on Internet Freedom, ” January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

28 Dmitri Alperovitch, and Ralph Langner. Transcript of “Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch.” Washington, DC, September 20, 2011. Alperovitch references discussions with the Chinese Foreign Ministry where they declared that rumor spreading on Facebook that causes social unrest in China would be considered a cyber attack.

29 FBI distinguishes mere terrorist use of information technology from a terrorist attack coupled with the use of the Internet—only the later is considered “cyber-terrorism.” Evan Kohlmann broadened the definition because, in his view, the online terrorism community overlaps with the real-world one. Keith Lourdeau, “Testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security,” February 24, 2004, http://www2.fbi.gov/congress/congress04/lourdeau022404.htm. Eben Kaplan, “Terrorists and the Internet, ” Council on Foreign Relations, last modified January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-Internet/p10005.

30 See for example, William Lynn, “Defending a New Domain,” *Foreign Affairs*, Oct. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

31 “Germans Fear Cyber-crime as Digital Blackmail Grows,” Reuters, June 30, 2011, http://in.reuters.com/article/2011/06/30/idINIndia-58011620110630.

32 Robert Mackey, “‘Operation Payback’ Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks,” *New York Times*, December 8, 2010, http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/.

33 John Markoff, “Before the Gunfire, Cyberattacks,” *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

34 Christopher Drew, “ Stolen Data Is Tracked to Hacking at Lockheed,” *New York Times*, June 3, 2011. http://www.nytimes.com/2011/06/04/technology/04security.html.

35 Christopher R. Hughes and Gudrun Wacker, *China and the Internet: Politics of the Digital Leap Forward* (London: Routledge, 2003), 145.

36 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 198.

37 William J. Broad, John Markoff and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

38 George R. Lucas, Jr. “Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets.” Presentation at Society of Philosophy and Technology conference, University of North Texas, May 28, 2011.

39 Jerry Brito and Tate Watkins, “Loving the Cyber Bomb: The Dangers of Threat Inflation in Cyber Policy,” MercatusCenter Working Paper, April 2011, http://mercatus.org/sites/default/files/publication/WP1124_Loving_cyber_bomb.pdf

40 Peter R. Teachout, “Making Holocaust Denial a Crime: Reflections on European Anti-Negationist Laws from the Perspective of U.S. Constitutional Experience,” *Vermont Law Review* 30 (2006): 655-692.

41 Even the U.S. government’s 2011 counterintelligence report that pointed a strong finger at China repeatedly indicated that absolute certainty with regard to attribution is not currently achievable. Office of the National Counterintelligence Executive, “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,” October 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

42 Teresa Larraz, “Spanish “Botnet” Potent Enough to Attack Country: Police,” *Reuters*, March 3, 2010, accessed September 26, 2011, http://www.reuters.com/article/2010/03/03/us-crime-hackers-idUSTRE6214ST20100303.

43 Singer and Shachtman, 2011.

44 Carr, J. (2008, October 17). *Project Grey Goose Phase I Report*. Retrieved from http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report; Krekel, Bryan. “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” Northrop Grumman Corporation, 9 October 2009.

45 “War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?”. *The Economist*. July 1, 2010. http://www.economist.com/

46 For more on this, see Mark Bowden, *Worm: The First Digital World War*, (Atlantic Monthly Press, 2011).

47 Larry Magid, “Many Ways to Activate Webcam sans Spy Software”, *cnet News*, February 22, 2010, accessed September 27, 2011, http://news.cnet.com/8301-19518_3-10457737-238.html; Lech Janczewski and Andrew M. Colarik edited, *Cyber Warfare and Cyber Terrorism*, (London: IGI Global, 2008), 311.

48 Noah Shachtman, “Exclusive: Computer Virus hits U.S. Drone Fleet,” *Wired Danger Room*, Oct. 10, 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

49 John W. Rittinghouse and Bill Hancock, *Cybersecurity Operations Handbook: The Definitive Reference on Operation Cybersecurity* (Digital Press, 2003), 42-45.

50 A good description of a APT is in Mark Clayton, “US oil industry hit by cyberattacks: Was China involved?” *Christian Science Monitor*, January 25, 2010. http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved.

51 “The Stuxnet Outbreak: A Worm in the Centrifuge,” *The Economist*, September 30,2010, http://www.economist.com/node/17147818.

52 William J. Lynn III, “Defending a New Domain: The Pentagon's Cyberstrategy,” *Foreign Affairs*, September/October 2010.

53 As the director of the U.S. National Security Agency (NSA) Information Assurance Directorate, Debora Plunkett, says, “There's no such thing as 'secure' any more. The most sophisticated adversaries are going to go unnoticed on our networks. We have to build our systems on the assumption that adversaries will get in. We have to, again, assume that all the components of our system are not safe, and make sure we're adjusting accordingly.” Quoted in Jason Mick, “NSA Switches to Assuming Security Has Always Been Compromised,” Daily Tech, Dec 17, 2010.

54 Michael Brown et al, *Offense, Defense and War* (Cambridge, MA, MIT Press, 2004).

55 Mark Clayton, “How Stuxnet cyber weapon targeted Iran nuclear plant,” *Christian Science Monitor*, November 16, 2010, http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

56 Mark Clayton, “How Stuxnet cyber weapon targeted Iran nuclear plant,” *Christian Science Monitor*, November 16, 2010, http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

57 http://thenextweb.com/asia/2011/11/11/importance-of-microblogs-in-china-shown-as-weibos-pass-550-million-users/

58 Kim Zetter, “Fearing Industrial Destruction, Researcher Delays Disclosure of New Siemens SCADA Holes,” *Wired*, May 18, 2011, accessed September 27, 2011, http://www.wired.com/threatlevel/2011/05/siemens-scada-vulnerabilities/.—Use of term: “not publicly identified”, is that referring to the practice of “responsible disclosure”—as followed by Symantec, etc.? Or as NTBugtraq form of disclosure? See Scott Berinato, “Software Vulnerability Disclosure: The Chilling Effect,” *CSO Security and Risk*, January 01, 2007, http://www.csoonline.com/article/print/221113 and Stephen A. Shepard, “Vulnerability Disclosure: How Do We Define Responsible Disclosure?” SANS Institute, 2003.

59 David Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and its Dangerous* Legacy (New York: Doubleday, 2009).

60 Ralph Langner. Transcript of “Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch.” Washington, DC, September 20, 2011.

61 Ibid.

62 Tom Espiner, "McAfee: Why Duqu is a big deal, ZDNet UK, 26 October, 2011. http://www.zdnet.co.uk/news/security-threats/2011/10/26/mcafee-why-duqu-is-a-big-deal-40094263/

63 "Security in Embedded Devices, McAfee presentation, June 22, 2011.

64 See Carolyn Bartholomew, *2009 Report to Congress of the U. S.-China Economic and Security Review Commission*, (DIANE Publishing, 2010), 170.

65 Track 2s are intended to be kept out of the public limelight, but there has been reporting on the efforts in Joseph Menn, "Agreement on Cybersecurity "Badly Needed," *Financial Times*, Oct. 12, 2011.

66 Louis Kriesberg, *Constructive Conflicts: From Escalation to Resolution*, 3rd ed. (Lanham, MD: Rowman & Littlefield, 2007), 239

67 Department of Homeland Security, *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*, March 23, 2011, p. 2 available at http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

68 United States House Financial Services Subcommittee on Oversight and Investigations, testimony by Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury, 109th Congress, 2nd Session, July 11,2006, http://financialservices.house.gov/media/pdf/071106sl.pdf (accessed Oct. 7, 2011); Sue E. Eckert, "The U.S. Regulatory Approach to Terrorist Financing," in *Countering the Financing of Terrorism*, ed. Thomas J. Biersteker and Sue E. Eckert (New York: Routledge, 2008); Phil Williams, "Warning Indicators and Terrorist Finances," in Jeanne K. Giraldo and Harold A. Trinkunas, *Terrorism Financing and State Responses: A Comparative Perspective* (Stanford, CA: Stanford University Press, 2007).

69 Robert Radvanovsky and Allan McDougall, *Critical Infrastructure: Homeland Security and Emergency Preparedness*, 2nd ed. (Boca Raton, FL: Taylor & Francis, 2010), 3; Zhang Chenfu and Tang Jun, "信息化风险管理：基本战略与政策选择 (Informationization Risk Management: Basic Strategy and Policy Choices)," *Chinese Public Administration* 260, no. 2 (2007): 52-54.

70 Stanford Arms Control Group, *International Arms Control: Issues and Agreements*, 2nd ed. edited by Coit D. Blacker and Gloria Duffy (Stanford: Stanford University Press, 1976), 237.

71 This is an area to explore further in both research and mutual discussions, as a counter argument can be made that without an ability to identify origins, a declaratory policy could potentially do harm, such as if you suspect the other side of breaking its solemn word. But, in turn, it would raise the costs both internally and externally of breaking such declared policy.

72 Karl Rauscher and Zhou Yonglin, "Fighting Spam to Build Trust," EastWest Institute and Internet Society of China joint paper, May 2011. Available at http:// www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=130065

73 DOD strategy: Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, accessed Oct. 7, 2011, http://www.defense.gov/news/d20110714cyber.pdf.

74 Amy F. Wool, “U.S. Nuclear Weapons: Changes in Policy and Force Structure,” *CRS Report for Congress*, Jan. 23, 2008, accessed Oct. 7, 2011, http://fpc.state.gov/documents/organization/101742.pdf.

75 Mendez, *The Master of Disguise: My Secret Life in the CIA* (New York: William Morrow Paperbacks, 2000), 348.

76 As quoted in Andrea Shalal-Esa, “Ex-U.S. general urges frank talk on cyber weapons,” Reuters, Nov. 6, 2011.

About the Authors

Kenneth G. Lieberthal is director of the John L. Thornton China Center and senior fellow in Foreign Policy and Global Economy and Development at Brookings. Lieberthal was a professor at the University of Michigan for 1983-2009. He has authored 17 books and monographs and over seventy articles, mostly dealing with China. He also served as special assistant to the president for national security affairs and senior director for Asia on the National Security Council from August 1998 to October 2000. His government responsibilities encompassed U.S. policy toward Northeast and East Asia.

Peter W. Singer is the director of the 21st Century Defense Initiative and a senior fellow in Foreign Policy at Brookings. Singer's research focuses on three core issues: the future of war, current U.S. defense needs and future priorities, and the future of the U.S. defense system. Singer lectures frequently to U.S. military audiences and is the author of several books and articles, including *Wired for War: The Robotics Revolution and Conflict in the 21st Century.*

BROOKINGS
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu