A FUTURE CHALLENGES ESSAY

Cybersecurity Treaties
A Skeptical View

by Jack Goldsmith

Koret-Taube Task Force on National Security and Law
www.futurechallengesessays.com

task force on national security and law

Prospects for a cybersecurity treaty seem to have improved in the last year. The Russians have long proposed a cyberwarfare "arms-limitation" treaty. Until recently, the United States has balked at the proposal. But the U.S. government is in the process of reconsidering its position.[1] Last June, National Security Agency (NSA) Director Keith Alexander said of the Russian proposal: "I do think that we have to establish the rules, and I think what Russia has put forward is, perhaps, the starting point for international debate."[2] Former NSA and Central Intelligence Agency Director General Michael Hayden made a similar proposal in late July.[3] The United Nations recently reported progress on cybersecurity treaty talks, and the North Atlantic Treaty Organization and the International Telecommunications Union are also exploring possible cybersecurity agreements. Many commentators think that such agreements are necessary and inevitable.

This essay sounds a skeptical note. Part I explains why international cooperation is thought to be a central solution to the cybersecurity problem. Part II sketches the cautionary lessons to be gleaned from our experiences with the Cybercrime Convention. Parts III-V examine three major hurdles to a global cybersecurity treaty: the lack of mutual interest; the problems the United States has in making concessions adequate to gain reciprocal benefits; and the problem of verification. Part VI briefly considers the feasibility of narrower and softer forms of cooperation.

I. The Demand for International Cooperation

Cyber attacks and cyber exploitations from around the globe are growing in number and sophistication, and governments, especially ours, are worried. Defenders against such attacks often cannot quickly or easily tell when their systems are attacked or exploited. When defenders discover an attack or exploitation, the computer or geographical source often cannot be ascertained quickly or precisely. If a computer or geographical source is identified, it is hard to know whether a computer somewhere else is responsible. Even if one has certain knowledge about which computer in the world was the ultimate source of the attack or exploitation, it is often hard to know whether the human agent behind it is a private party or a government. If the latter,

HOOVER INSTITUTION
STANFORD UNIVERSITY

it is sometimes also hard to determine the state affiliation. And even if geographical location, precise identity, and state affiliation are known, the human and computer agents of attack or exploitation are often located beyond our borders, where law-enforcement capacities are weak and military capacities cannot be used except in the most extreme circumstances.

These and other factors have enabled and emboldened untold thousands of actors from abroad—states, criminals, hackers, and, potentially, terrorists—to steal or destroy valuable digital assets inside the United States. The United States arguably has more to lose from cyber attacks and exploitations than any other nation because it is among the most dependent on the Internet and related computer/communications systems, and has more of its wealth embedded in these systems. The U.S. government's recent foray into international negotiation on this issue appears to reflect a judgment that it cannot adequately protect its critical infrastructure and other digital assets without international cooperation. And in truth, every advanced nation faces that problem to some degree.

Many believe that an important part of the solution to these challenges is an international treaty that does some or all of the following: (1) limits what states can do to one another in the cyber realm; (2) imposes on them duties to ensure that private actors within their borders do not engage in certain bad cyber acts; (3) establishes mechanisms of interstate cooperation to track and redress malicious cyber operations; (4) clarifies definitions (such as which acts constitute war and various crimes) in order to prevent mistaken interpretations and prevent misunderstanding or escalation; and (5) creates an international organization to facilitate cooperation and monitoring.

An international treaty on cybersecurity might cover any number of substantive topics, ranging from cyber-arms control to cyber crime and mutual assistance to the regulation of cloud computing or the software supply chain. The hurdles to all such treaties are similar (though not identical). To make the problem concrete, I will focus primarily on a proposal by Richard Clarke and Robert Knake (C&K) that in many of its details is similar to the recently expressed views of General Michael Hayden.[4] C&K argue that a cyber treaty should ban cyber attacks on civilian targets but not on military targets or cyber exploitation. Such a treaty, they argue, would protect the United States' vulnerable, privately owned networks but would allow the country to maintain its lead in what it is good at, "cyber war against military targets."[5] C&K do not propose to ban cyber espionage, because the United States depends so heavily on electronic and related means of spying, and because verification of and attribution for espionage are too difficult in any event. They acknowledge that cyber espionage might be mistaken for military attacks and could be destabilizing. But they nonetheless oppose its international legal regulation, because "an arms control agreement limiting cyber espionage is not clearly in [the United States'] interest, might be violated regularly by other nations, and would pose significant compliance-enforcement problems."[6]

The remainder of this paper explains why I believe an international treaty of this sort is not feasible.

II. The Cautionary Tale of the Cybercrime Convention

Calls for international treaties to govern harms caused over the Internet are not new.[7] Since the early 1990s, Internet experts have worried about the fact that the net is a borderless medium over which people can communicate globally and instantaneously in ways that seem to resist geographically based regulation. One worry was that a national government could do nothing to stop a content provider on the other side of the globe from making content available locally (via a website or e-mail), violating local laws regulating intellectual property, libel, crimes of various sorts, and much more. This concern was that the net would undermine national sovereignty. A different and somewhat antithetical worry was that since websites could appear everywhere in the world, every nation might try to regulate every web transaction, leading to multiple and inconsistent regulation of the same activity that would stifle free speech and Internet commerce. The concern here was that nations exercising sovereignty to combat local Internet harms would destroy the global resource.

The answer to both problems, it was widely believed, was international agreements. International treaties could establish global norms that would tamp down on both harmful Internet communications and harmful national over-regulation of the global resource. And yet, despite years and years of loud discussion and all manner of cross-border digital clashes, the nations of the world have agreed on only a single treaty regulating cross-border Internet harms or the cross-border regulation and sharing of electronic information: the Council of Europe's Cybercrime Convention.

That convention establishes a "a common criminal policy aimed at the protection of society against cybercrime."[8] It requires signatories to adopt legislation banning various computer crimes, including illegal access and interception, data and system interference, misuse of devices, forgery, fraud, child pornography, and intellectual-property offenses. It also requires countries to adopt laws concerning the investigation of computer-related crimes, and to cooperate in the investigation and prosecution of such crimes with other countries (i.e., via extradition and mutual law-enforcement assistance).

The Cybercrime Convention is widely viewed as unsuccessful. It achieved "consensus" on computer crimes only by adopting vague definitions that are subject to different interpretations by different states. Even with vague definitions, many nations conditioned their consent on declarations and reservations (the United States had more than a half dozen) that further diluted the scope of covered crimes, making the treaty's obligations even less uniform and less demanding. While the mutual assistance mechanisms in the treaty improve on what came before, they do not work well. The duty to cooperate contains large loopholes for requests that prejudice such essential interests as national sovereignty and security.[9] As a recent National Research

Council study concluded, "[A] signatory nation may decline to cooperate with its obligations under the convention on fairly broad grounds, and the convention lacks an enforcement mechanism to assure that signatories will indeed cooperate in accordance with their obligations."[10] As a result, signatories often flout or ignore the cooperation provisions.

Despite the general weaknesses of the treaty and the relatively sparse demands it makes on nations, few have ratified it. Every nation was invited to join, but only the United States and two-thirds of Council of Europe states have ratified the treaty. Notable COE holdouts include Belgium, Georgia, Greece, Ireland, Poland, Russia, Sweden, Switzerland, Turkey, and the United Kingdom. The treaty has not gathered support outside of the COE because many nations do not like its definitions of crimes (for example, the criminalization of intellectual-property violations), its general Western focus, or its (weak) sovereignty-intrusive cooperation mechanisms.

To get a flavor of how some non-Western states view similar matters, consider the International Information Security agreement among the Shanghai Cooperation Organization nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan). The SCO agreement emphasizes state security and state control over information technologies and threats. It lists as major threats the "dominant position in the information space" of Western nations and the "dissemination of information harmful to the socio-political systems, spiritual, moral, and cultural environment of the States."[11]

The Cybercrime Convention experience teaches that nations significantly disagree about what digital practices should be outlawed and are deeply skeptical about even the weakest forms of international cooperation in this area. It is a cautionary tale for those who believe in the feasibility of a broader cybersecurity treaty involving more nations and covering more ambitious topics that bear a closer relationship to sovereignty and national security.

III. Non-alignment of Interests

One prerequisite to a treaty—at least among powerful nations—is the possibility of mutual gain. Otherwise, there is no incentive to enter into the contract or to comply with it. For most cybersecurity issues, it is not clear that a mutually beneficial deal is possible in theory, even assuming that the massive verification problems (discussed below) can be overcome.

Consider C&K's proposal. It is crafted to dovetail with what is best for the United States, without consideration of other nations' interests. Such a treaty has no chance of adoption. As the SCO agreement makes plain, there are deep and fundamental clashes not only over what practices should be outlawed but also and more broadly over what the problem is. A ban on attacking civilian targets might well serve U.S. interests on balance, because we are deeply dependent on our civilian networks and

as a general matter do not attack (as distinct from exploit) other nations' civilian *targets*. But Chinese civilian networks, according to C&K and many others, are more secure than ours and less depended on by the military. China would probably gain relatively little and lose a lot from an agreement that banned targeting of civilian infrastructure targeting but not military assets. It would thus have little interest in signing on. Similarly, while the United States is indeed unlikely to give up any of the NSA's cyber-exploitation capacities, many nations subject to NSA snooping (but not good—or not *as* good—at snooping themselves) have no interest in a carve-out for state-sponsored snooping. There are similar fundamental clashes over the desirability of intellectual-property protection, freedom of speech and free access to information, the nature and scope of needed security carve-outs, state control over the network, and much more. These disagreements are hard to bridge.

One response to this argument is that even with these clashes of interests, there are still opportunities for agreement to secure the basic infrastructure of the Internet on which all nations depend and from which they all benefit. For example, C&K propose to ban cyber attacks on banks.[12] The United States does not attack banks and thus would lose nothing from promising not to do so. And perhaps other nations also have no interest in attacking (as opposed to stealing from) banks, because all nations would lose a lot if the international banking system went down. So perhaps nations' interests align in the protection of certain discrete infrastructures. And perhaps this natural conversion of interests could be concretized and strengthened by an international agreement.

Even here, though, the supposed alliance of interests is misleading. Set aside the significant verification problems, and just focus on China's interests. China is committed to the deployment of malicious agents inside our critical infrastructure (including banking systems) to make up for its relative weakness in traditional military capabilities in the event of a hot war.[13] Combining this consideration with its relatively powerful control over its own critical infrastructures, China might think itself relatively better off, vis a vis the United States, by not giving up cyber threats against civilian infrastructures, including banking. Similarly, Iran or North Korea might want to maintain the threat of shutting down our electricity grid—even if doing so heightened the vulnerability of its own grid.

These points become even stronger when one considers that our adversaries might think, based on credible public sources, that the United States is deeply self-constrained in its use of cyber weapons by its interpretation of the laws of war, the Title 10 v. 50 debate, and other legal factors. Because the threat of U.S. cyber attack is already weak, at least short of a hot war, our adversaries might think they gain relatively little from a cybersecurity agreement to refrain from using offensive weapons. This consideration is probably only heightened by the United States' sudden and seemingly panicked rush of interest in international treaties.

The general point here is that even if every nation would to some degree benefit from protection of interconnected computer and communication infrastructures, those potential benefits by themselves do not necessarily imply that there is space for cooperative agreement. The distributional consequences of any such agreement may be such that some nations will be willing to risk the threats to infrastructures from non-cooperation because the threats fall asymmetrically on their adversaries. This relative-gains problem is a frequent hurdle to arms control and security agreements.[14] It is also a frequent hurdle to international agreements about the regulation of telecommunications technology that relates to national security.[15] It has special salience in the cybsersecurity context, because the United States, as explained above, is asymmetrically vulnerable to cyber attack.

The fundamental clash of interests will also matter in a different way. Assume for the moment that every nation in the world would benefit from a ban on certain forms of cyber attack and that every nation can perfectly monitor every other's compliance with a cybersecurity treaty. It does not follow that nations will cooperate. An important prerequisite to cooperation is that nations must agree on what counts as cooperation. For example, if two nations agree simply to not engage in "hostile activity," or to reduce their nuclear arsenals to a "reasonable level," without further definitional clarity, then even with perfect verification, they will have a hard time cooperating around these norms.

The reason is that "hostile activity" and "reasonable levels" are vague terms subject to many different interpretations. If what is banned is unclear, misinterpretations and disagreements will invariably occur, even if each side knows precisely what the other is doing. These misinterpretations and disagreements, in turn, are significant hurdles to the trust and perceptions of mutual compliance that are essential to mutually constrained cooperation. To avoid this problem, arms-control treaties use very precise technological definitions about which weapons are banned and what can be done with certain weapons.

These considerations matter because the cybersecurity context is and will remain bedeviled by two types of definitional difficulty. The first arises from the nature of the activity itself, which makes precise definitions of weapons, effects, and targets difficult. Offensive cyber weapons are guarded secrets because knowledge about the weapon enables the building of defenses and because revelation about attack capabilities would reveal a lot about exploitation capabilities. Even if nations revealed their cyber weapons, they take variable and changing forms. A weapons ban is thus hard to articulate. So is an effects ban, because (among other reasons) the effects of a cyber attack are unusually difficult to anticipate. In the cyber world, red lines are hard to draw. Targets (e.g., civilian infrastructure) sound like a more manageable category but often are not. In part, that is because of dual military and civilian use of the same communications infrastructure.

A more discreet ban on targeting a "banking network" might be easier to make precise, though hard questions will arise about when and where the banking network intersects with other and government networks. Even a ban on banking network attacks would not, under any extant proposal, ban cyber exploitation of these targets. This means that penetration of the banking network would still be allowed for purposes of espionage and theft. As discussed below, the similarity between attack and exploitation agents is one of many factors that confound verification.

Definitions in this context will be hard for a second reason more closely related to the fundamental clash of interests. When nations disagree sharply over the matter to be regulated, they tend to agree (if at all) in vague generalities that are not terribly useful for fostering true cooperation. The Cybercrime Convention deals with 1990s-era cyber-crime problems, and even today we cannot even achieve precise definitional agreement on those relatively benign matters. It will be significantly harder to achieve such agreement and clarity in the cybersecurity context. And that, in turn, will be a fundamental hurdle to cooperation.

IV. The Problem of Mutual Concession

C&K's proposal for a treaty that would benefit the United States and harm our major adversaries reflects a set of blinkered assumptions common in Washington discussions about the international dimensions of the cyber threat. Secretary of State Hillary Rodham Clinton wore similar blinkers in her January 2010 speech on "Internet freedom." Alluding to the China-Google kerfuffle, she warned that "Countries or individuals that engage in cyber attacks should face consequences and international condemnation." She added that, "In an Internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons."[16]

Both C&K's proposal and Secretary Clinton's speech are blinkered because they assume that (a) the United States is a major victim of the cyber threat rather than a part of the problem, and (b) American cyber activities abroad are legitimate, while those of adversaries in the United States are not.

The problem with those assumptions is that the United States is widely viewed as a major source of cyber attacks and exploitations, as well as a major spur to the cyber-arms race. We have the biggest private botnets in the world. They are used for cyber attacks and exploitations around the globe, and the government has done practically nothing to clean them up. The government subsidizes a robust "hacktivist" community that uses digital tools for such activities as circumventing content filters in the networks of authoritarian states. It views these activities as benign, but the Chinese consider them on a par with the Google hack. In addition, the U.S. government has famously prodigious cyber-exploitation and cyber-attack capacities. All of these reasons, and more, explain why an early-2010 study by McAfee, the computer security company, concluded that more information-technology experts from critical infrastructure firms around the

world expressed concern about the United States as a source of computer network attacks than about any other country.[17]

For our government to receive the concessions and relief that it thinks international cooperation by treaty can bring, it must be willing to clamp down on some, probably many, aspects of its many public and private cyber activities. But no one in Washington has indicated publicly which cyber operations the United States might terminate in exchange for reciprocal concessions. Indeed, there is no public indication that Washington is seriously interested in the question. Until the United States gets serious about which concessions that are attractive to our adversaries it is willing and able to make, American talk of a cyber-arms agreement is empty. We aren't going to get restraint from our adversaries unless we restrain ourselves, and in a significant way. (And agreeing to forgo activites that we are already known not to engage in does not count as a concession that will induce reciprocity.)

It is hard to imagine that the United States is willing to engage in the types of self-constraint that would be needed to induce mutual constraint from our adversaries in the cyber context. Our government is not going to give away any of the NSA's exploitation tools. Nor will it give away offensive cyber weapons in the absence of significant verification mechanisms that, as discussed below, simply are not available. On the private side, serious regulation of our huge private botnets would be very expensive and controversial. It might happen one day, but not any time soon. Even more controversial and less likely is any attempt to crack down on Internet hacktivism and the development of hacktivist tools that are mechanisms to promote free speech and free thought. Finally, as also discussed below, any conceivably effective verification regime would require deep government monitoring of, and activity in, the private network; that would be enormously controversial and, depending on how it is done, might raise significant Fourth Amendment concerns.

This is as good a place as any to discuss growing calls for what James Lewis describes as "a norm making a state responsible for cyber-actions taken from its territory."[18] This proposal comes in various flavors. Some propose that a nation should be responsible for all attacks originating from its borders, while others would extend the obligation even to attacks that merely transit through a nation's borders. Others would place an absolute obligation on nations to stop the cyber attack or be penalized; others would merely place the burden of proof on nations to show that they are not responsible.[19]

The basic idea behind all of these proposals is to ameliorate the attribution problem by eliminating the "It wasn't us, it was private hackers" defense that Russia and China have invoked when criticized for cyber attacks from within their borders. As General Hayden recently argued, the penalty for a nation that failed to stop cyber attacks from their borders might be, as one journalists summarized his remarks, "some kind of cyber exile or a response that would thwart the flow of the Internet

from the suspect country in a way that would slow their cyber commerce and ability to communicate."[20]

Some problems with these state responsibility proposals have already been identified above. One is that nations like China might benefit a great deal more than they lose from the state-actor uncertainty and have little interest in this approach. We cannot assume that our adversaries will unilaterally disarm. A related problem is that the state responsibility norm to which nations might agree will not be limited to preventing attacks on infrastructure; China and its friends will also be interested in preventing "attacks" from hacktivists wielding anti-censorship weapons. Yet another difficulty is that no nation will be able to stop or investigate all malicious activity coming from across its borders, so any such duty will have to be limited to some type of serious attack. But attacks by agents emanating from one nation to do harm in another do not self-identify themselves as "serious attacks" or "attacks on civilian infrastructure." It is hard to know how the scope of the duty to keep malicious activity from leaving one's borders will be defined and implemented.

Another problem with the state-responsibility proposal concerns the enormous scope of government involvement in the network required to enable a nation to prevent or pursue a cyber attack emanating from its borders (including one that merely transits through the nation). At a minimum, and focusing only on attacks with known signatures (as opposed to zero-day attacks and advanced persistent threats), it would require a workable EINSTEIN 3-like intrusion prevention system to be implemented throughout the private network. Such a system might place sensors at all communication points entering and exiting the United States, as well as at each Internet Exchange point among Internet-backbone providers and between those providers and major cloud-service providers and large private firms involved with critical infrastructure. The government would be involved in identifying or coordinating both the signatures that triggered intrusion in such systems and the responses to such intrusions. Even this civil-libertarian nightmare would not be enough, because the most sophisticated attacks, and the ones the United States cares most about, are not caught by signature-based systems. Precisely what nations will be required to do to find and stop these attacks is unclear.

The United States might one day be willing to accept comprehensive U.S. government monitoring and 24/7 real-time police or military pursuit in the private network in exchange for a serious clamp-down on malicious activity from Russia and China. But the idea is unthinkable today. This highlights a paradox about the U.S. attitude toward the security/privacy tradeoff in the cybersecurity context. What we need to do to protect ourselves in the cyber realm is in deep conflict with our commitments to limited government and private control of the communications infrastructure. The Chinese government, by contrast, controls its networks extensively. The state responsibility proposal emanates from American authors with close associations

with the U.S. government, but in fact China can much more readily assert state responsibility over Internet communications emanating from its borders.[21]

V. Verification

The final and most obvious hurdle to any cybersecurity agreement is verification. It is central to any arms control or security treaty that asks one nation to restrain its offensive or defensive capabilities in exchange for mutual restraint from its adversary. The absence of a dependable verification regime will kill a security treaty—even if other hurdles to cooperation, such as those outlined above, are overcome.

Verification is hard because attribution is hard. A thoughtful adversary can hide its tracks by routing attacks or exploitations through anonymizing computers around the globe. Even if one knows which computer in the world is behind an attack or exploitation, that fact alone does not indicate who, or even which country, is responsible for the aggression. The Information Warfare Monitor traced the computer source of "Ghostnet" to China, but could not determine whether the plot was controlled by the Chinese government or by private actors in China. Nor could it rule out the possibility that "a state other than China" was behind the plot, using agents to launch the operation from Chinese territory in an attempt to "deliberately mislead observers as to the true operator(s) and purpose of the *GhostNet* system." We still don't know who is behind the Conficker worm or the July 2009 denial-of-service attack on South Korea and the United States. Nor, more recently, do we know for sure who is behind the Stuxnet worm.

To say that attribution is hard is not to say it is impossible. Sometimes traceback and related forensic tools can provide good-enough attribution. And human and other forms of non-electronic intelligence can help. But even taking into account these and other tools, the attribution of a sophisticated attack is neither fast nor certain. In other words, verification will often not be immediate or certain.

No rational government, and certainly not the United States, should give up major cyber-exploitation or cyber-attack capabilities in exchange for mutual restraint from our adversaries in the absence of better verification capabilities. The reason is simple: we cannot assume that our adversaries will comply with any agreement. As Stewart Baker, former Assistant Secretary for Policy at Homeland Security, has argued:

> *[The] Pentagon would be exquisitely sensitive to arguable violations of international law in carrying out operations in cyberspace. Our guys would sit with their fingers poised over the "return" button for hours while the JAGs were trying to figure out whether the Belarussian remarks in committee were a consensus or an individual interpretation of article 42bis. And nobody else*

> *would give a damn what the treaty said, because they wouldn't expect to get caught and because even implausible deniability can't be rebutted with the certainty needed to make a legal case, let alone send missiles in response.*[22]

Baker's last point is important and worth fleshing out. Cooperation in the prisoners' dilemma–which in some form is what these cybersecurity agreements would seek to address—depends on credible retaliation when there is breach. Uncertainty in attribution makes retaliation for breach much harder for any president or general to order. ("Sir, we are 38 percent sure the Chinese did it.") This in turn makes retaliation less credible to some probably large degree, which in turn invites breach and unravels cooperation.

C&K weakly propose to address verification with what they call an "International Cyber Forensics and Compliance Staff." This international organization would have inspection teams to determine the origins of an attack and would place traffic-monitoring equipment inside national networks.[23] If one looks at the comparatively modest inspection regimes under, say, the Chemical Weapons Convention, and considers the skepticism that regime continues to generate, it is hard to imagine that powerful nations would ever give any such international organization the independent technical capacities to rummage through domestic networks. Indeed, not even C&K think such an organization, if it works, would provide "high confidence verification," and in the end they say it would be useful only to "contribute to an international norm against cyber attacks."[24]

Two other issues related to verification warrant brief mention. The first is that even if we have perfect attribution, we often cannot publicly reveal the evidence of attribution because doing so would disclose our espionage and attribution capabilities and render them less useful. To the extent that this is so, it makes the public-shaming aspects of a verification regime less robust.

The second issue arises from the fact that the agents that facilitate cyber espionage and those that facilitate cyber attacks are hard, if not impossible, to distinguish in advance. No one proposes banning cyber exploitation; it is too central to the national security of powerful nations, especially the United States. This means, however, that no one is considering a prohibition on the incursion into civilian networks, for such a prohibition would require a ban on exploitation. It also means that we cannot be sure we can tell whether the logic bombs and related agents we find in our civilian infrastructure are agents of attack or exploitation—until, of course, they are used in that way. In other words, in many instances, verification of a treaty breach might only come after the attack occurs. If there is a first-mover advantage in cyber attacks (which seems plausible and probably obvious), a post-attack response may not worry the attacker much. This situation contrasts with many arms-control treaties, where the latency period between breach and reconstitution of the banned offensive forces is typically months or years, giving the defender time to prepare for the breach. With cyber

attacks the latency period will often likely be zero, the latency risk very high. That makes an agreement to refrain hard to reach.[25]

VI. Softer and Narrower Cooperation

This paper thus far has focused on hurdles to legally binding multilateral agreements among adversaries. This section comments briefly on the feasibility of softer and narrower forms of cooperation.

James Lewis acknowledges that verification of compliance will not work, but he nonetheless thinks that cybersecurity treaties can promote cooperation. Even in the absence of compliance verification, he argues, "multilateral agreements could increase stability and reduce the risks of miscalculation or escalation by focusing on several specific areas: confidence-building and transparency measures, such as increased transparency in doctrine; creation of norms for responsible state behavior in cyberspace; and expansion of common understandings on the application of international law to cyber conflicts, or development of assurances on the use of cyberattacks."[26]

The possibility of softer norms of this sort—whether embodied in a treaty or in a less formal document—is frequently mentioned, and the subject warrants a more extended discussion than I can here give it. My skepticism can be summarized as follows: in the absence of decent verification, we cannot be confident that transparency measures are in fact transparent, or that revealed doctrine is actual doctrine. Nor can norms get much purchase in a world without serious attribution and verification; anonymity is a norm destroyer.

Another frequently mentioned possibility is a narrower treaty for cooperation among like-minded states. "The more signatures of an attack one can see, and the more intrusions one can trace, the better one's defenses will be," says Deputy Secretary of Defense William J. Lynn III. He proposes that "[j]ust as the United States' air and space defenses are linked with those of allies to provide warning of attack from the sky, so, too, can the United States and its allies cooperatively monitor computer networks for intrusions."[27] Such cooperation among like-minded nations diminishes two of the hurdles mentioned above (non-mutual interests and verification). But some aspects of the mutual-concession problem remain—most notably, the intrusive steps required by the U.S. government in the private network.

Conclusion

This paper has argued that the fundamental clash of interests concerning the regulation of electronic communications, the deep constraints the United States would have to adopt to receive reciprocal benefits in a cybersecurity treaty, and the debilitating verification problems will combine to make it unfeasible to create a cybersecurity treaty that purports to constrain governments. The point of this essay has not been to

be skeptical for skepticism's sake but rather to inject a bit of sobriety into the growing enthusiasm for an international solution to our cybersecurity difficulties. If I am wrong about the feasibility of a meaningful cybersecurity agreement, then consider this paper a roadmap to some of the hurdles to such a treaty. If I am right, one might conclude that other approaches, including unilateral strategies to prevent an attack, and defensive strategies of resilience in the face of an attack, are comparatively more fruitful than they now seem.

Acknowledgments

The author would like to thank Stuart Baker, Jon Lindsay, Eric Posner, Hoover Task Force members, and workshop participants at Stanford Law School, for comments, and Merritt Baer, Matthew Bobby, Oliver Day, and Eric Powell for research assistance. An earlier version of this paper was presented at a workshop entitled "The Intelligence Community and Cyberspace: Traditions, Boundaries, and Governance," held at CENTRA Technology, Inc., on August 9, 2010. This work was funded by the Office of Naval Research under award number N00014091059. The opinions, conclusions, and recommendations expressed are the author's alone and do not necessarily reflect the views of the Office of Naval Research.

Notes

1 See, e.g., John Markoff and Andrew W. Kramer, "In Shift, U.S. Talks to Russia on Internet Security," *The New York Times*, December 12, 2009, www.nytimes.com/2009/12/13/science/13cyber.html?_r=1.

2 "U.S. Cybersecurity Policy and the Role of U.S. Cybercom," Center for Strategic and International Studies Cybersecurity Policy Debate Series, June 3, 2010, transcript, www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf.

3 Jaikumar Vijayan, "U.S. Should Seek World Cooperation on Cyber Conflict, Says Ex-CIA Director," *Computerworld,* July 29, 2010, www.computerworld.com/s/article/9179873/U.S._should_seek_world_cooperation_on_cyber_conflict_says_ex_CIA_director.

4 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Ecco, 2010); Kim Zetter, "Former NSA Director: Countries Spewing Cyber Attacks Should Be Held Responsible," *Wired* (blog), July 29, 2010, www.wired.com/threatlevel/2010/07/hayden-at-blackhat/.

5 Clarke and Knake, *Cyber War*, 242.

6 Ibid., 236.

7 See e.g., Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006).

8 Council of Europe, "Convention on Cybercrime," Preamble, *opened for signature* November 23, 2001, C.E.T.S. No. 185 (*entered into force* July 1, 2004).

9 Council of Europe, "Cybercrime," Preamble, Art. 27(4).

10 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 7–24.

11 Agreement Between the governments of the memberstates of the Shanghai Cooperation Organization on Cooperation in the field of International Information Security (date unknown). www.sectsco.org/EN/show.asp?id=95; www.sectsco.org/EN/show.asp?id=224

12 Clarke and Knake, *Cyber War*, 245–46.

13 Ibid., 53.

14 See Eric A. Posner, "Terrorism and the Laws of War," *Chicago Journal of International Law* 5, no. 2 (Winter 2005): 423–34. For further discussion of the relative-gains problem generally, see Robert Powell, "Absolute and Relative Gains in International Relations Theory," *American Political Science Revie*w 85, no. 4, (December 1991): 1,303–20; Joseph Grieco, "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism," *International Organization* 42, no. 3, (Summer 1988): 485–507.

15 See Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics* 43, no. 3 (April 1991): 336–66.

16 Hillary Rodham Clinton, "Remarks on Internet Freedom" (speech), Newseum, Washington, DC, January 21, 2010, transcript and Adobe Flash video, www.state.gov/secretary/rm/2010/01/135519.htm.

17 Stewart Baker, Shaun Waterman, and George Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (McAfee, 2010), 30.

18 James A. Lewis, "Multilateral Agreements to Constrain Cyberconflict," *Arms Control Today* 40 (June 2010), under "Obstacles to Agreement," www.armscontrol.org/act/2010_06/Lewis; see Clarke and Knake, *Cyber War*.

19 Lewis, "Multilateral Agreements;" Zetter, "Countries Spewing Cyber Attacks Should Be Held Responsible;" Clarke and Knake, *Cyber War*.

20 Zetter, "Countries Spewing Cyber Attacks"

21 I thank Stewart Baker for helping me formulate the ideas in this paragraph.

22 Stewart Baker, "Going Wobbly on Russia's Cybersecurity Disarmament Proposal?" *The Volokh Conspiracy* (blog), June 6, 2010, volokh.com/2010/06/06/going-wobbly-on-russias-cybersecurity-disarmament-proposal/; see also Stewart A. Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* (Palo Alto: Hoover Institution Press, 2010), 231.

23 Clarke and Knake, *Cyber War*, 251.

24 Ibid., 253.

25 See David Elliot, "Weighing the Case for a Convention to Limit Cyberwarfare," *Arms Control Today* 39 (November 2009), under "Arms Control Models," www.armscontrol.org/act/2009_11/Elliott.

26 Lewis, "Multilateral Agreements to Constrain Cyberconflict," under introduction.

27 William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 104–5.

Copyright © 2011 by the Board of Trustees of the Leland Stanford Junior University.

This publication is for educational and private, non-commercial use only. No part of this publication may be reprinted, reproduced, or transmitted in electronic, digital, mechanical, photostatic, recording, or other means without the written permission of the copyright holder. For permission to reprint, reproduce, or transmit, contact Ms. Tin Tin Wisniewski (tintinyw@stanford.edu).

Hoover Institution Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

The preferred citation for this publication is
Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View (February 2011)," in *Future Challenges in National Security and Law*, edited by Peter Berkowitz, http://www.futurechallengesessays.com.

About the Author

Jack Goldsmith
Jack Goldsmith is the Henry L. Shattuck Professor of Law at Harvard University and the author of The Terror Presidency: Law and Judgment inside the Bush Administration *and co-author of* Who Controls the Internet?: Illusions of a Borderless World. *He served in 2003–4 as assistant attorney general, Office of Legal Counsel, and in 2002–3 as special counsel to the general counsel to the Department of Defense. Goldsmith is a member of the Hoover Institution's Koret-Taube Task Force on National Security and Law.*

Koret-Taube Task Force on National Security and Law

The National Security and Law Task Force examines the rule of law, the laws of war, and American constitutional law with a view to making proposals that strike an optimal balance between individual freedom and the vigorous defense of the nation against terrorists both abroad and at home. The task force's focus is the rule of law and its role in Western civilization, as well as the roles of international law and organizations, the laws of war, and U.S. criminal law. Those goals will be accomplished by systematically studying the constellation of issues—social, economic, and political—on which striking a balance depends.

The core membership of this task force includes Kenneth Anderson, Peter Berkowitz (chair), Philip Bobbitt, Jack Goldsmith, Stephen D. Krasner, Jessica Stern, Matthew Waxman, Ruth Wedgwood, and Benjamin Wittes.

For more information about this Hoover Institution Task Force please visit us online at http://www.hoover.org/taskforces/national-security.

HOOVER INSTITUTION
STANFORD UNIVERSITY