



# ESSENTIAL QUESTIONS FOR CYBER POLICY

**Strategically Using Global Norms to Resolve  
the Cyber Attribution Challenge**

**DR. PANAYOTIS A. YANNAKOGEORGOS**

Cyber Defense Analyst  
Air Force Research Institute

**MR. LYNN MATTICE**

President and Founder  
National Economic Security Grid

Air University Press  
Air Force Research Institute  
Maxwell Air Force Base, Alabama

October 2011

### Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the official policy or position of the organizations with which they are associated or the views of Air University, the Air Force Research Institute, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.



Air University Press  
Air Force Research Institute  
155 North Twining Street  
Maxwell AFB, AL 36112-6026  
<http://aupress.au.af.mil>

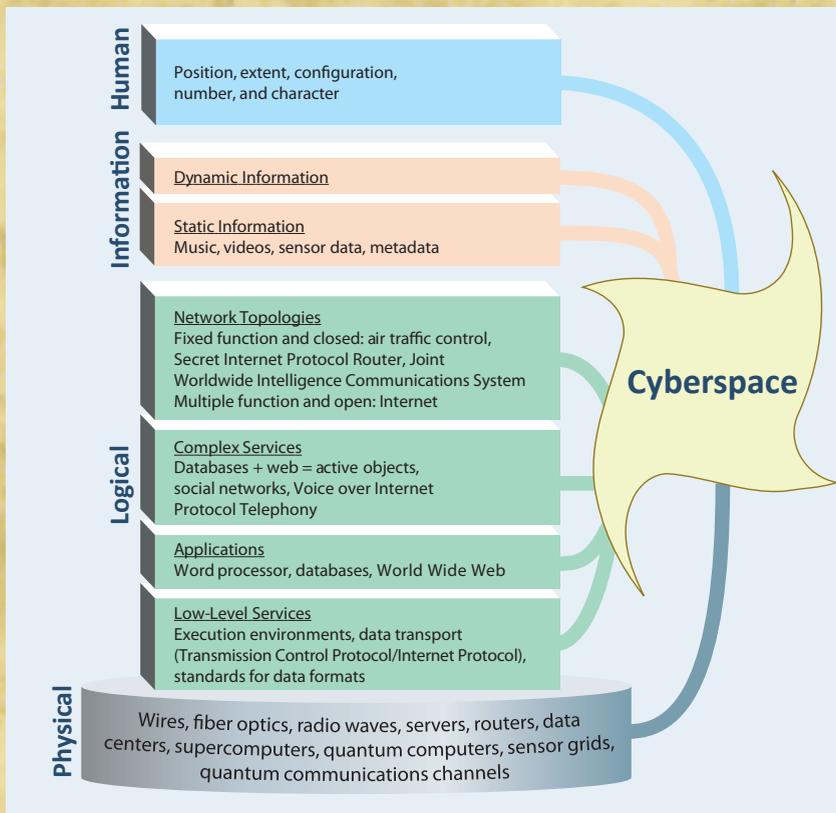
## What Is Cyberspace?\*

According to US Air Force doctrine for cyberspace operations, “cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, and maritime.”<sup>1</sup> This description creates an aura of cyberspace as a solely virtual domain, separated from the real world. Such a conceptualization has implications for the attribution problem. Cyberspace has the sole purpose of serving human operators and creating effects in the physical world. Focusing on technology rather than the characteristics that wholly compose the cyber environment (fig. 1) creates the impression that this domain is not connected with the real world. Refining the conceptualization of cyberspace will allow for its demystification and a closer alignment within the physical world. Doing so requires looking at cyberspace as a complex ecosystem composed of human operators, ranging from casual Internet users to information warriors; the actual information that is stored, transmitted, and transformed; the computer code and protocols; and the physical elements on which the logical elements reside.<sup>2</sup>

The current concentration on the importance of technical attribution stems in part from an emphasis on the logical rather than the physical and human layers that compose cyberspace. Although doctrine and policy note the physical elements of cyberspace, these remain largely secondary to the protocols and computer language through which digital communications occur. Data and information are not transported in a virtual ether divorced from the laws of physics, space, and time. Rather, they travel through physical infrastructures, such as undersea cables, and reside on devices operated by people located within the boundaries of a nation-state’s sovereign territory. Therefore, people and computer systems may be held responsible for cyber attacks under laws of a nation-state (if those laws exist). Thus, refocusing on the holistic characteristics of cyberspace allows for a conceptualization that policy makers may use to hold nation-states responsible for actions in the domain. Hence, an approach that does not treat cyber as a virtual domain but recognizes the physical and social attributes brings clarity to discussions of global norms of responsibility for a nation-state’s behavior in cyberspace.

---

\*A monograph by Panayotis A. Yannakogeorgos, *Beyond Anonymous: Resolving the Cyber Attribution Challenge with Global Norms for State Responsibility* (Maxwell AFB, AL: Air University Press, forthcoming [winter 2012]), will include an extended discussion of the issues raised in this policy brief.



**Figure 1. Characteristics-based model of cyberspace.** (Adapted from David Clark, “Characterizing Cyberspace: Past, Present and Future,” working paper, version 1.2, 12 March 2010, <http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf>.)

## Why Is the Interconnected Cyber Environment Unsecure?

Several factors account for the generally unsecure nature of our interconnected environment:

- For over 40 years, professors have taught courses on designing and writing computer coding. When universities first established such courses, we lived in a world in which no one ever imagined the inter-

connectivity that would evolve and become so central to our lives today. No stand-alone computer systems network-connected to third parties that performed various services or support. As the interconnectivity of the Internet developed, few people realized the inherent flaws and lack of sound security measures in legacy systems or new systems that utilized legacy-style programming methodologies.

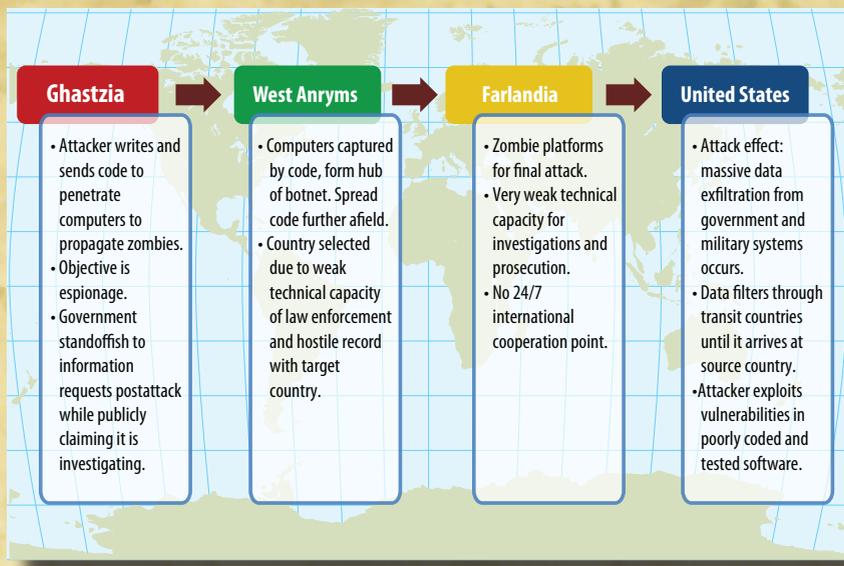
- Legacy computer hardware, middleware, and network designers also overlooked or outright ignored the idea of building in security measures, viewing them as adversely affecting performance, output, or throughput and generally deeming them unnecessary.
- From the beginning, both software developers and hardware manufacturers established an environment in which they accepted neither liability nor responsibility for any loss, delay, disruption, or other action that could affect the purchaser/user community, whether caused directly or indirectly by the systems, hardware, or software supplied. This “use at your own risk” disclaimer to liability has manifested itself into a patch-management nightmare. The periodic issuance of security patches regularly follows every new release of software or hardware. These patches deal with flaws that the “rush-to-market” mentality of the manufacturers and producers created by failing to take a duty-of-care philosophy in product design and delivery. Early on in the evolution of software, hardware, and networks, people became accustomed to “computer bugs” and other design flaws that they simply accepted as the norm. Rarely has a single industry benefited from such a desensitized consumer population, which has allowed producers and manufacturers to skirt responsibility and liability for the flawed products and systems they produce.

### **With International Cooperation, Is Technical Cyber Attribution a Daunting Challenge?**

Malicious cyber actors exploit gaps in international cybersecurity cooperation to launch multistage, multijurisdictional attacks. Rather than consider technical attribution the challenge, the more accurate argument holds

that the attribution challenge resides in international cooperation. Although strengthening network protocols is desirable, respected cyber experts David Clark and Susan Landau have suggested that “better attribution techniques will neither solve nor prevent” the complex, multistage, multijurisdictional nature of computer exploitations that occur today.<sup>3</sup> Although this piece does not delve into the intricacies of methods one may use to technically attribute an attack, one should note that the multistage and cross-jurisdictional characteristics of a cyber attack (fig. 2) determine the complexity of attributing the source of the attack and highlight the fact that gaps in international cooperation are the real problem in attribution.

By having appropriate global policies in place, one can surmount the challenge of attribution. The root of the problem lies in so-called spoofing attacks—that is, the masking of one’s personal or machine identity on a network. Machines identify each other on the Internet through Internet protocol (IP) and media access control (MAC) addresses. Engineers never intended IP to function as the backbone of the global project that became the Internet.



**Figure 2. Outline of a hypothetical multistage, cross-jurisdictional attack launched for the purpose of data exfiltration**

Communications protocols designed and deployed for military and research purposes in the late 1960s lacked the ability to track and trace user behavior in a highly untrustworthy computing environment. Thus, today an individual can manipulate various layers of the transmission-control protocol (TCP)/IP suite to create an ambiguous identity of a user, device, or website, allowing a malicious actor to exploit protocol vulnerabilities in such a way that networked digital devices appear located elsewhere in the world. Dorothy Denning of the Naval Postgraduate School aptly points out that to “trace an intruder, the investigator must get the cooperation of every system administrator and network service provider on the path.”<sup>4</sup>

Although attribution of malicious cyber incidents to individuals is a complicated law enforcement task, military and diplomatic contexts overstate the challenge. Observers can identify the source of every action in cyberspace. Experts have noted that “the very fact that one attempts to conduct cyberwarfare means that some bit in some data stream is changed to reflect one’s presence and actions.”<sup>5</sup> Putting in place a worldwide effort to monitor malicious traffic and enforce behaviors that fall outside a spectrum of international norms of behavior renders all people and machines transmitting bits and bytes in cyberspace visible.<sup>6</sup>

However, much of the discussion in doctrine and policy remains uninformed by these technical realities. Instead, one finds a preoccupation with the mythical issue of how, with current network topologies, no physical identifiers exist for a cyber attack as they do for a missile flash observable from space or a radiological signature to determine the origin of a nuclear attack. Thus, the common view is that ambiguity is the norm on the Internet, and attribution remains an unsolvable technical problem because of current network protocols. However, it is really the gaps in international cooperation that prevent the investigator from following the path of an intruder back to the malicious machine.

Recall that the ecosystem within which cyber attacks occur is not isolated from the real world. Real people program computers located on a country’s sovereign soil to send signals to other computers to cause effects. These signals may transit through multiple countries to reach their target. A cyber attack occurs because attackers, facilitators, and defenders exist within the chain of that attack. All operate within the territory of a nation-state (with the odd exceptional case of actors on oil platforms in

international waters). Nation-state governments therefore have an important role to play in mitigating attacks and should be held responsible for instigating or facilitating an attack. A nation-state may facilitate a cyber attack either by lacking the technical capability of preventing the attack or by not practicing due diligence in enforcing laws to prosecute the perpetrators of an attack. Given the multijurisdictional nature of most cyber attacks, nation-states need to cooperate in the development of common laws and policies to prohibit the use of their territory as safe havens for digital strikes.

Technical challenges do not hinder global cybersecurity cooperation; rather, the latter suffers from a lack of national-level cybersecurity action plans that implement the technology, management procedures, organizational structures, law, and human competencies into national security strategies.<sup>7</sup> Criminals, privateer-hacker networks, and information warriors exploit countries without these structures to launch cyber attacks of national and global significance. Indeed, the vitality of our social, economic, and governmental institutions is at great risk from cyber vulnerabilities existing in less-developed parts of the world.<sup>8</sup> Reducing vulnerabilities and threats from cyber attack hinges on the US policy community's support of norms of behavior among nation-states, enforceable at the national level, to secure the cyber commons.<sup>9</sup>

### **What Existing, Institutionalized Global Norms of Behavior for Cyberspace Could the United States Sponsor?**

Currently, the behavioral baseline for cybersecurity enjoys broad international consensus, as articulated within the United Nations (UN), its specialized agencies, and regional organizations. For example, at the UN General Assembly, member nation-states declared their awareness that “effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society.”<sup>10</sup> By identifying the provisioning of cyber crime as an activity separate from government or law enforcement, they essentially created a broader cybersecurity framework that tasked governments and private actors with preventing cyber crime. The UN General Assembly stated that “technology alone

cannot ensure cybersecurity,” specifically “in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies.”<sup>11</sup> Such recognized needs formed the basis for a global culture of cybersecurity (table 1).

**Table 1. Foundations of the global culture of cybersecurity**

<i>Element</i>	<i>Intended Outcome</i>
Awareness	All information society stakeholders, including individuals, should sustain a level of awareness regarding the importance of having secure information systems.
Responsibility	Stakeholders are responsible for securing their own information systems and for reviewing the policies, practices, measures, and procedures pertaining to their own cyberspace.
Response	Stakeholders assure timely and cooperative response by sharing information (possibly including cross-border sharing) about threats, vulnerabilities, and security incidents in order to facilitate the detection of and response to the misuse of information systems.
Ethics	The ethical basis of the global culture of cybersecurity is founded on utilitarian grounds in that each participant is expected to respect the interests of others and to act or avoid inaction that will harm others.
Democracy	Cybersecurity regimes are guided by democratic principles, identified as the freedom of thoughts and ideas, free flow of information, confidentiality of information and communication, protection of personal information, openness, and transparency.
Risk assessment	One should conduct periodic broad-based risk assessments of the security implications of technological, physical, and human factors, policies, and services in order to determine the appropriate level of risk and the best way of managing the risk of potential harm to information systems according to a scale based on the importance of information to the information system under assessment.
Security design and implementation	The planning, design, development, operation, and use of an information system should incorporate security measures.
Security management	Security management occurs on the basis of dynamic risk assessment.
Reassessment	Given the dynamic nature of information insecurity, only a periodic reassessment of security protocols and procedures will assure that all the above elements remain relevant.

*Adapted from* UN General Assembly, “Creation of a Global Culture of Cybersecurity,” Resolution A/RES/57/239, 31 January 2003, 2–3, [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_57\\_239.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf).

## What Is the US Government Position on Global Norms for Cyberspace?

Recent official statements and events indicate the need for US policy supporting global norms of behavior in cyberspace. Some suggestions call for holding nation-states accountable for the actions of agents within their borders. Formal shifts in policy began in 2011 when the US *National Military Strategy* described the cyber threat as “expanded and exacerbated by lack of international norms, difficulties of attribution, low barriers to entry, and the relative ease of developing potent capabilities.”<sup>12</sup> Similar views emerged in May 2011 when the president’s *International Strategy for Cyberspace* formally articulated what various senior leaders and policy makers had been stating for the past two years: “The United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships.”<sup>13</sup> Later in the year, the Department of Defense’s *Strategy for Operating in Cyberspace* stated that “the Department will work with interagency and international partners to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate.”<sup>14</sup> Both policy documents indicate the readiness of the US government to adopt embryonic international norms of behavior.

However, the US government appears to be playing a game of forum picking with “like-minded states” rather than shaping international initiatives already under way at the International Telecommunications Union (ITU). Indeed, one finds implicit mentioning of the ITU in a broader listing of international forums within which the United States will collaborate.<sup>15</sup> The World Summit on the Information Society’s Tunis Agreement and Geneva Action Plans, the work of the High-Level Experts Group of the Global Cybersecurity Agenda, and the ITU’s International Multilateral Partnership against Cyber Threats (IMPACT) program are all global initiatives related to cybersecurity. By not offering strong support to such initiatives instead of tackling the challenges existing in global cybersecurity forums, the United States attempts to lead a world that fails to follow. Inventing the Internet and effectively supporting governance mechanisms are two different things. Despite the difficulty of doing so, the United States should develop

strategy to surmount existing challenges within the ITU. Reinventing what the rest of the world sees as a legitimate forum may suggest hegemonic intentions and result in a negative outcome for US interests.

### **Why Is American Sponsorship of Embryonic Global Norms Important?**

The concept of US sponsorship of global norms has emerged within the global affairs community as one way to address complex transnational policy issues. Global affairs expert Simon Reich articulates it as a way to merge “hard” and “soft” power to effect change in certain transnational policy issues. This concept entails a US “willingness to enforce or underwrite the costs of enforcing a policy without necessarily taking the lead in placing it on the agenda. . . . Sponsorship entails the selective enforcement, by the United States, of policy initiatives promoted by nongovernmental organizations and codified by global organizations. Where such conditions exist, global norms take root and influence behavior.”<sup>16</sup> The effectiveness of US sponsorship depends upon the development and articulation of the norm by private entities and upon its codification and institutionalization. Failure to meet these conditions makes that sponsorship seem unilateral, imperialistic, or suggestive of conducting ineffective multilateralism. It does not affect the desired outcome of behavioral management in accordance with the norm. This is the path down which current cyber strategy has begun to tread.

According to Reich, creation of a global norm requires meeting three conditions: broad-based support of private entities, global institutional codification, and US sponsorship through enforcement.<sup>17</sup> The first sequence—that is, the articulation of norms and their institutionalization—has been met. Now the United States must accept and sponsor these global efforts through soft- and hard-power mechanisms.

### **What Are Some Options for a Range of US Response Mechanisms?**

Policy makers need to guide the US response by sponsoring global norms of behavior already articulated in multilateral institutions of diplomacy. US enforcement of these norms via soft and hard measures could result in an

overall cleaner cyber ecosystem in which nation-states can no longer walk away from the crime scene, claiming ignorance of how it occurred.

Cyber specialist Jason Healey developed a taxonomy of a range of actions for a nation-state’s responsibility that serves as a useful starting point for developing a broader response framework to actions, or inactions, a nation-state may take in responding to a range of cyber incidents. Table 2 depicts the taxonomy combined with a framework for US response along a range of development, diplomacy, and defense. The range of nation-state activity describes a level of responsibility for which a nation-state could be held accountable and seeks to guide the possible framework for US policy described in the next section.

**Table 2. Range of nation-state activity**

		US Response Framework		
		Development	Diplomacy	Defense
Range of State Activity	<b>State prohibited</b>	X		
	<b>State prohibited but inadequate</b>	X		
	<b>State ignored</b>	X	X	
	<b>State encouraged</b>		X	
	<b>State shaped</b>		X	
	<b>State coordinated</b>		X	
	<b>State ordered</b>			X
	<b>State-rogue conducted</b>			X
	<b>State executed</b>			X
	<b>State integrated</b>			X

*Source:* This taxonomy for nation-state actions is adapted from categories of nation-states in Jason Healey, “Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks” (Vienna, VA: Cyber Conflict Studies Association, 2010), 4. The range of US response framework is Dr. Yannakogeorgos’s addition.

“State prohibited” cyber attacks are those against which a nation-state has enacted laws and has established sufficient enforcement mechanisms—but that occur anyway. A nation-state would not be held responsible in such a scenario since one assumes that it would make a vigorous effort to investigate and prosecute those responsible for an attack. However, a nation-state that

has updated legal codes but cannot investigate or prosecute an attack due to gaps in technical or managerial elements necessary to combat cyber crime could be held responsible since it does not meet minimum standards to combat cyber criminal activity. Nevertheless, it would be eligible for US aid in combating cyber crime should it choose to implement aid. Refusing aid would place the nation-state in a subsequent category of reprisal. In this second range, sanctions are either authorized bilaterally or pursued in multilateral institutions of diplomacy. A finding of some nation-state involvement could justify a US response short of war (e.g., sanctions, blocking, throttling of traffic, and limited acknowledged strikes) as well. Open conflict in cyberspace that escalates into kinetic attacks could occur if the effect of a cyber attack is consequential enough to warrant a kinetic or cyber response. Such is the case today in the physical world and could have parallels in cyberspace. In open conflict, a nation-state may not even care to mask its involvement in the attack, thereby negating the attribution challenge altogether.

### **Is There a Model of Effective US Sponsorship of Global Norms That Could Apply to Cyberspace?**

The United States generally uses diplomatic pressure to engender domestic reforms and stimulate enforcement of minimum standards for the elimination of trafficking in persons by governments in individual countries. Analyzing US success at leading the world in stemming the scourge of human trafficking offers one approach to a way forward for international engagement in cyberspace. Hence, the antitrafficking agenda has many parallels to a global cybersecurity agenda in terms of holding nation-states responsible for actions occurring within their borders. However, the United States would have to accept the institutionalization of global norms within the ITU despite the challenges that are manifest within the organization.

US sponsorship of the antitrafficking global norm through the Trafficking Victims Protection Act of 2000 has created a framework guiding US efforts to name and shame origin, transit, and destination countries for the modern-day slave trade via a tier-based system. Tier-one countries are model countries. Tier-two countries are those that are making an effort but still require further enhancement of domestic practices. Tier-three countries, which are doing nothing to reform, may have sanctions placed against them. A similar

initiative could establish minimum standards, based on existing cyber norms for the elimination of cyber crime, applicable to the government of a country of origin, transit, or destination of a malicious code used to execute severe cyber attacks. Adapted and refined from the trafficking-in-persons model, along with input from relevant global policies such as the Council of Europe Convention on Cybercrime, the following elements should become minimum standards indicative of a government's making serious and sustained efforts to eliminate cyber crime:

- Review and update old or obsolete legal authorities and develop necessary legislation for investigation and prosecution of cyber crime, including extradition measures.
- Determine key stakeholders from national and local governments, industry, civil society, and academia with a role in cybersecurity to develop networks and processes of international cooperation for enhancing incident response and contingency planning.
- Ensure that prosecutors, judges, and legislators have an adequate level of understanding of cyber issues.
- Create a government agency that monitors data patterns for evidence of malicious cyber activities.
- Create an around-the-clock point of contact for international cyber crime to cooperate with international counterparts during the investigation of transnational cyber crime. This applies to those instances in which infrastructure is situated in or perpetrators reside in one national territory but victims reside elsewhere.
- Require that, for the knowing commission of any cyber attack involving a country's government officials, said country prescribe punishment commensurate with that for grave crimes, such as criminal behavior or armed attacks.
- Require that, for the knowing commission of any cyber attack, the government of the country prescribe punishment sufficiently stringent to deter such an attack and adequately reflective of the reality of the offense.

The following factors are further indicia of a country's serious and sustained efforts to rid itself of cyber crime and prevent cyber attacks (see fig. 3), all of which could be used to identify countries to model as tier-one archetypes:

Whether the government of the country vigorously investigates and prosecutes acts of [cyber crime] . . . that take place wholly or partly within the territory of the country [including required incarceration for individuals convicted of such attacks as appropriate]. . . . A government, which does not provide . . . data [regarding investigations, prosecutions, convictions, and sentences after requests from the US government for such data], consistent with the capacity of such government to obtain such data, shall be presumed not to have vigorously investigated, prosecuted, . . . or sentenced such acts. . . .

Whether the government of the country has adopted measures to prevent [cyber crime], such as measures to inform and educate the public, including potential victims, about the causes and consequences of [cyber crime].

Whether the government of the country cooperates with other governments in the investigation and prosecution of [cyber crime].

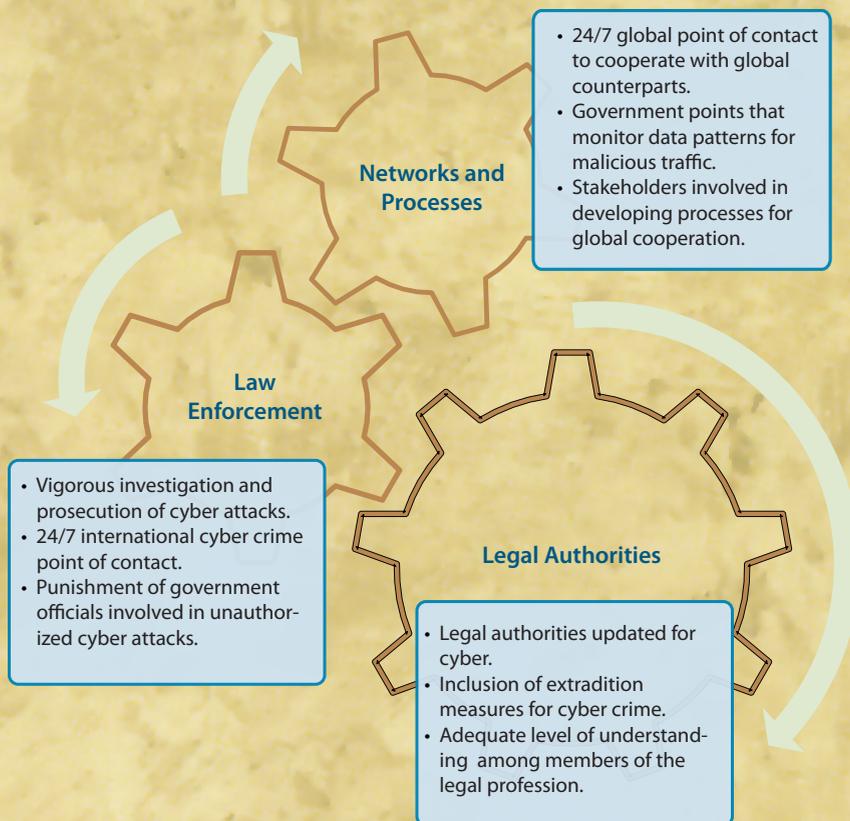
Whether the government of the country extradites persons charged with [malicious cyber acts] on substantially the same terms and . . . extent as persons charged with other serious crimes (. . . to the extent such extradition would be inconsistent with the laws of such country or with international agreements to which the country is a party, whether the government is taking all appropriate measures to modify or replace such laws and treaties so as to permit such extradition).

Whether the government of the country monitors [data] patterns for evidence of [malicious cyber activities] and whether law enforcement agencies of the country respond to any such evidence in a manner that is consistent with . . . vigorous investigation and prosecution.

Whether the government of the country vigorously investigates, prosecutes, convicts, and sentences public officials who participate in or facilitate [cyber attacks,] (including nationals of the country who are deployed abroad). . . . After reasonable requests from the Department of State for data regarding such investigations, prosecutions, convictions, and sentences, a government which does not provide such data consistent with its resources shall be presumed not to have vigorously investigated, prosecuted, convicted, or sentenced such acts.

Whether the percentage of victims of [malicious cyber incidents] in the country that are non-citizens of such countries is insignificant.<sup>18</sup>

The unprecedented gravity of the cyber problem relies on passing through Congress a framework that allows the United States to bring its elements of power as mechanisms for global enforcement of global norms. As reported in the *Quadrennial Defense Review Report of 2010, Department of Defense Strategy*



**Figure 3. Model of a tier-one country**

for *Operating in Cyberspace* and *International Strategy for Cyberspace* of 2011, and *National Security Strategy* of 2010, strengthening international partnerships to secure the cyber domain requires an understanding of what gaps exist in the capabilities of our international partners within the technical, legal, and organizational domains.<sup>19</sup> Identifying these gaps and their root causes will give the US policy community the knowledge it needs to help our partners strengthen their national cybersecurity. International cooperation is a necessity for resolving the attribution challenge. Stopping a trace at a nation-state's borders rather than trying to track down individuals may create an impetus for international cooperation with the right formula of develop-

ment, diplomacy, and—potentially—defensive measures articulated by the United States. We now need policy makers to establish the legal and policy framework to allow for US sponsorship of global norms that make nation-states responsible for wrongful acts in cyberspace.

### Notes

1. Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010, 2, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>.

2. David Clark, “Characterizing Cyberspace: Past, Present and Future,” working paper, version 1.2, 12 March 2010, <http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf>.

3. David D. Clark and Susan Landau, “The Problem Isn’t Attribution: It’s Multi-Stage Attacks,” in *ReArch 2010: Proceedings of the Re-Architecting the Internet Workshop* (New York: Association for Computing Machinery, 2010), 1, [http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch\\_papers/11-Clark.pdf](http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf).

4. Dorothy E. Denning, “Cyberspace Attacks and Countermeasures,” in *Internet Besieged: Countering Cyberspace Scofflaws*, ed. Dorothy E. Denning and Peter J. Denning (New York: ACM Press, 1998), 35.

5. Raymond C. Parks and David P. Duggan, “Principles of Cyber-warfare,” in *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security* (West Point, NY: US Military Academy, 5–6 June 2001), 122–25 (see p. 123 for the quotation).

6. One might argue that it is difficult to assess whether or not an activity is malicious until it is too late. However, for the purpose of holding nation-states responsible, the model assumes the existence of preventive efforts in place that would reduce the noise, thereby mitigating the risk of someone’s using legitimate network activity to disguise an attack.

7. Solange Ghernouti-Hélie, “A National Strategy for an Effective Cybersecurity Approach and Culture” (presentation at the International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010), <http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2010.119>.

8. Franz-Stefan Gady, “Africa’s Cyber WMD,” *Foreign Policy*, 24 March 2010, [http://www.foreignpolicy.com/articles/2010/03/24/africas\\_cyber\\_wmd](http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd).

9. In a speech on Internet freedom, Secretary of State Hillary Clinton stated that

the spread of information networks is forming a new nervous system for our planet. . . .

States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. 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.

Hillary Rodham Clinton, "Remarks on Internet Freedom," 21 January 2010, US Department of State, <http://www.state.gov/secretary/rm/2010/01/135519.htm>.

10. UN General Assembly, "Creation of a Global Culture of Cybersecurity," Resolution A/RES/57/239, 31 January 2003, [1], [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_57\\_239.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf).

11. Ibid.

12. Department of Defense, *The National Military Strategy of the United States of America* (Washington, DC: Department of Defense, 2011), 3–4, <http://www.au.af.mil/au/awc/awcgate/nms/nms.pdf>.

13. White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), 9, [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

14. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 10, <http://www.defense.gov/news/d20110714cyber.pdf>.

15. These forums include the Organization of American States, Association of Southeast Asian Nations Regional Forum, Asia-Pacific Economic Cooperation Organization, Organization for Security and Cooperation in Europe, African Union, Organization for Economic Cooperation and Development, Group of Eight, European Union, United Nations, and Council of Europe. Although the ITU may be contained within the United Nations, the customary "UN and its specialized agencies" would have been a more appropriate labeling.

16. Simon Reich (with Panayotis A. Yannakogeorgos), *Global Norms, American Sponsorship and the Emerging Patterns of World Politics* (New York: Palgrave Macmillan, 2010), 3.

17. Ibid., 4.

18. "Minimum Standards for the Elimination of Trafficking in Persons," Trafficking Victims Protection Act of 2000, US Department of State, <http://www.state.gov/g/tip/rls/tiprpt/2008/105392.htm>.

19. See "Operate Effectively in Cyberspace," in Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2010), 37–39; Department of Defense, *Strategy for Operating in Cyberspace*, 9–10; White House, *International Strategy for Cyberspace*, 17–23; and White House, *National Security Strategy* (Washington, DC: White House, May 2010), 28, [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf).



