Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms

Author(s): Jan Neutze and J. Paul Nicholas

Source: *Georgetown Journal of International Affairs*, International Engagement on Cyber III: State Building on a New Frontier (2013-14), pp. 3-15
Published by: Georgetown University Press
Stable URL: https://www.jstor.org/stable/43134318
Accessed: 06-05-2020 02:58 UTC

Cyber Insecurity

Competition, Conflict, and Innovation Demand Effective Cyber Security Norms

Jan Neutze and J. Paul Nicholas

Many states around the world are entering into a period of perceived or real "cyber insecurity." What is cyber insecurity, and how is it manifested in states? Cyber insecurity refers to growing state concerns about the reliance on information and communication technologies (ICT) and the ability of the state to defend itself and mitigate risks in cyberspace.

What happens when a nation-state feels insecure? States act to reduce insecurity with domestic as well as international policies and programs. Specifically, states shift investments in defense and intelligence to manage the political perception of insecurity and build tangible capabilities to help deter adversaries. Domestically, states promulgate regulations intended to ensure domestic capabilities. Internationally, states leverage diplomacy to gain international support for policies that contain risks and establish stability. What has been missing, however, is a credible international diplomatic effort to establish cyber security norms or 'rules of the road' for nation state behavior in cyberspace.

The modern state is highly dependent on ICT for the core functions of its economy, defense, public health, and safety—even political stability. This dependency will only grow. The World Economic Forum estimates that 70 percent of the

Jan Neutze is Director of Cybersecurity Policy for Europe, Middle East, and Africa (EMEA) for Microsoft and formerly worked in the Executive Office of the Secretary-General of the United Nations.

J. Paul Nicholas is the Senior Director and head of Microsoft's Global Security Strategy and Diplomacy Team and previously served as a White House director of cyber security and critical infrastructure protection.

The views expressed in the article are the authors' alone and do not necessarily reflect the position of any affiliated organization

world's population lives in countries that are still in the process "digitizing," or coming online[1]. The connectivity and possibility of increased ICT usage portends to offer great benefits for states and citizens alike. It offers greater efficiency and transparency in governments, enables improvements in civil society, and supports economic growth.

However, ICT dependency is not only about innovation and economic development. While ICT can provide many benefits, it can also be exploited to cause significant harm at a national level, including but not limited to exploitation of government systems (civil or military); damage to critical infrastructures (i.e., energy, communications, banking, transportation); theft of intellectual property; or criminal exploitation of citizens. In response, states are under significant pressure to develop and maintain capabilities for (1) defending the nation in cyberspace; (2) ensuring appropriate intelligence capabilities; (3) enforcing criminal law at scale; (4) reducing risk in its critical infrastructures and its broader economy.

Left unchecked, cyber insecurity has the potential to drive military competition.

Addressing cyber insecurity within states and also in the international system is an imperative. The development of cyber security norms—namely 'rules of the road' to guide nation-state behavior in cyberspace—is emerging as a primary international security challenge. Left unchecked, cyber insecurity has the potential to drive military competition; fuel distrust over increasing cyber espionage; increase chances for conflict; and curb technical innovation.

Attributing cyber attacks is difficult. Differentiating between state-sponsored and non-state threats can hinder traditional response and diplomatic strategies. For example, the employment of non-state proxies in cyberspace allows states to mask their involvement. Traditional deterrence strategies and defensive concepts need to be adapted to the unique character and functions of this increasingly important operational domain. Yet, adapting these concepts must not negatively impact the vital global connectivity, commerce, and free flow of information that cyberspace provides[2]. States are left to find the right mix of policies, and this balancing act can lead to insecurity. State insecurity can erode ICT innovation either by continued exploitation of ICT products in the name of national security, or through over-regulation in an effort to reduce risk.

The current trend of cyber insecurity can be reduced by sustained public and private sector engagements to identify and develop cyber security norms. Different from traditional state-to-state efforts, the development of cyber security norms will need to involve the private sector, which builds the global ICT products, and services that underpin cyberspace. Their insight can help inform the development of practicable

norms. Perhaps, more importantly, private sector ICT communities possess the technical understanding to recognize the tradecraft of state exploitation efforts and, increasingly, are concerned about the ability to recover rapidly from attacks.

This paper examines the consequences of cyber insecurity by looking at where states are investing resources, looking at the spectrum of cyber conflict, the urgent need for norms, and the challenges in building them. We will also place this discussion in a new risk context—global private sector ICT innovation. Finally, we make recommendations for jump-starting cyber security norms development.

An Age of Digital Peril? President Dwight D. Eisenhower was concerned that many Americans did not understand they were living in the "Age of Peril" brought on by the Soviet Union's desire for a nuclear race. Do Americans currently live in an age of digital peril? Are they facing a different kind of threat, namely one that is harder to recognize, assess, and defend against? When listening to the increasing rhetoric of policymakers, and looking at the investments that countries are making in cyber security—specifically in military, espionage and civilian capabilities—it certainly seems plausible. The Age of Digital Peril is upon the United States. The recent testimony from General Keith Alexander, Commander of U.S. Cyber Command certainly supports these concerns: "Offensive cyber programs and capabilities are growing, evolving, and spreading before our eyes; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individuals."[3] Yet, this concern is just one among many. The attack in August 2012 against the Saudi Aramco Oil Company, in which malicious actors rendered more than 30,000 computers on Aramco's business network unusable, raised concerns in many states about the implications of such an attack on their key businesses and infrastructure services.

Governments are acting to bolster the range of their national security capabilities in cyberspace. More than thirty countries have a stated policy on the use of cyberspace or the Internet for conflict. Moreover, many countries are taking steps to centralize, organize, and employ a wide range of cyber offense and defense capabilities. These capabilities could include, but are not limited to, the establishment of doctrine; cyber centers; coordination capabilities; force projection in cyberspace; and the development of offensive cyber capabilities. The list of countries currently includes Argentina, Brazil, Canada, China, France, Germany, India, Iran, Israel, Japan, Russia, the United States, the United Kingdom, and many others[4].

The United States has made significant investments in reducing its cyber insecurity, some of which have arguably increased the cyber insecurity of other states. It is important to understand U.S. efforts, as they provide a model that other countries may follow, either to simply maintain relevance or to vigorously compete militarily with the United States. One must understand such competition from both a military perspective as well as from a technical

innovation viewpoint.

In 2008, the United States began its Comprehensive National Cyber Security Initiative. It has already invested more than $10 billion into cyber defense, and has also announced other cyber programs with multibillion-dollar budgets[5]. The Department of Defense (DOD) established the U.S. Cyber Command in 2010, joining together facilities at the National Security Agency (NSA) in Fort Meade. Cyber Command is authorized to possess over 900 active duty military and civilians (plus contractors). Along with the cyber components of the military services, it projects a combined force of over 11,000 people. The FY2014 Budget request asked for $ 4.7 billion for Cyber Command, including specific funds to increase offensive operations. To put these figures in perspective, Cyber Command's budget for offensive cyber operations is bigger than the entire IT-budget of the German government. The funds also help the Command build a series of teams to (1) defend against national-level cyber threats; (2) support the objectives of individual Combatant Commanders; and (3) help operate and defend the DoD's information environment[6].

While governments are occasionally transparent about their organizations and resources for cyber defense, they are often opaque about details around their cyber offense capabilities, such as the acquisition and develowpment of cyber weapons. However, governments have begun to buy vulnerability data about private sector products from security researchers[7]. This data enables them to exploit such products, in order to target an entity and advance a national objective. There are no international prohibitions against the trade of cyber security vulnerabilities, and a rather robust market has thus grown up to support their trade, funded in part by governments. According to the *Economist*, "A Massachusetts firm called Netragard last year sold more than 50 exploits to businesses and government agencies in America for prices ranging from $20,000 to more than $250,000."[8] Vupen, a French company, claims to provide "...extremely sophisticated and government-grade exploits specifically designed for the Intelligence and [Law Enforcement Agency] community to help them achieve their offensive missions using tailored and unique codes created in-house by VUPEN for exclusive and undisclosed vulnerabilities discovered by VUPEN researchers."[9]

As governments continue to enter into vulnerability markets, it will grow harder for private sector firms to work

There are no international prohibitions against the trade of cyber security vulnerabilities, and a rather robust market has thus grown up to support their trade, funded in part by the governments.

with researchers to collaboratively fix products. "Most companies, including Microsoft, Apple Inc. and Adobe Systems Inc., on principle won't pay researchers who report flaws, saying they don't want to encourage hackers. Those that do offer "bounties", including Google Inc. and Facebook Inc., say they are hard-pressed to compete financially with defense-industry spending."[10]

The increased government interest in buying vulnerabilities of ICT products and their subsequent exploitation of them in operations can have swift and unintended consequences for the broader cyber ecosystem, and potentially even for the nation executing offensive operations. Specifically, attacking nations may miscalculate their ability to contain an attack. For example, other nation-states or technically talented non-state actors may choose to seize upon the same exploit and repurpose it for a much broader impact on global users or on the original attacking country. A broader attack could overwhelm private sector ICT firms' ability to rapidly marshal engineering teams to fix or mitigate one or more "zero-day" vulnerabilities. Not all ICT firms have developed comparable incident response teams and scalable sustained engineering teams to rapidly fix state sponsored exploits. In some instances, the required engineering fixes could take months to complete, until which time these exploits could dramatically erode stability and confidence in cyberspace.

The Unintended Consequences of Cyber Insecurity. Cyber insecurity will undoubtedly drive states to focus more on military espionage and state espionage in cyberspace. In addition, states will feel increased pressure to formulate effective deterrence regimes, clear signaling, and more rapid state-level responses to cyber events. Various components of government, including those actors engaged in diplomacy, intelligence, the military, and law enforcement, will need to coordinate and create a unified response to challenges. Depending on the nature or consequence of the cyber attack, states may have to act in the absence of perfect attribution, thus raising further concerns of misunderstanding and conflict.

States will invest in more than militaries to reduce the risks of cyber insecurity. They are also examining how to assess and manage cyber security risks in both critical infrastructures as well as their respective national economies. Specifically, states will enhance security through regulation.

In February 2013, the European Union released an ambitious cyber security strategy and a draft of the Network Information Security Directive that aimed to create baseline requirements for security; require reporting of cyber security incidents; and create new audit and compliance requirements for "market operators."[11] A few days later, the White House released Executive Order 13636, which intended to improve the cyber security and resiliency of critical infrastructures by first identifying what was critical, and then creating a cyber security framework, tailored regulations, and voluntary incentives designed to encourage greater investments in security.[12]

Both of these approaches have posi-

tive elements. However, the lack of alignment in cyber security regulatory approaches within nation states can create barriers for global ICT providers. Barriers such as unique product requirements or service compliance could cause ICT providers to not participate in certain markets, or stop future developments of certain products because of shrinking markets. While not immediate, over time these incremental changes can begin to erode innovations in certain types of products or services.

In other instances, state concerns over ICT supply chain security, such as fears of hidden malicious code or unwanted components, could taint key products or services upon which governments and infrastructure rely. This in turn is driving renewed interest in indigenous innovation. The European Union cyber strategy calls for more EU-made cyber products. The United States has created a series of supply chain-related legal provisions designed to ensure that the products are legitimate and function as intended, namely that they maintain code integrity. India and China have long aimed to increase indigenous ICT innovation. At the same time, China and the United States are engaging in tit-for-tat accusations over ICT protectionism, fueled by U.S. concerns over the supply chain integrity in companies such as Huawei and ZTE.[13]

The combined effect of militaries buying exploits of private sector ICT products, and their civilian regulators creating unrelated security requirements, should concern policy makers globally. This is a short-sighted approach with potentially dangerous consequences, both militarily and economically. Moreover, this political atmosphere creates a number of challenges for the ICT industry as well as an opportunity for government miscalculation. First, governments could exploit something that the private sector may not be able to fix rapidly, and the exploit could consequently spread beyond intended targets. Second, regulators may try to push the private sector to increase its defenses for a set of risks that they cannot fully anticipate or manage. Third, the government can place additional requirements on ICT providers to increase confidence in their products to withstand military grade attacks. The result is that the government is forcing the private sector (enterprises, critical infrastructures, and ICT vendors) to carry the cost of national security. Over time these increased costs will reduce functionality and innovation and result in less agile systems.

State cyber insecurity is not limited to external threats. Many states harbor significant concerns about the internal threats that come from cyber through social media and other types of applications that promote rapid exchange of ideas and transparency. The rise of social media is happening in parallel with the rise of the global middle class. According to the National Intelligence Council's *Global Trends 2030*, for the first time a majority of the world's population will not live in poverty, and the middle class will emerge as the most important social and economic sector in the vast majority of countries around the world.[14] The individual empowerment that comes with the rise of the middle class and its access to technology

creates phenomenal positive opportunities for social progress, problem solving, and increased economic growth. Yet, "in a tectonic shift, individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence—a capability formerly the monopoly of states."[15] Some states fear the rise of a wealthier, more educated people empowered by technology within their borders and their ability to govern such populations. Some of these states are leveraging botnets and other malware to monitor or limit the ability of its citizenry and thereby contain possibly powerful non-state actors that could present a nation state level threat.

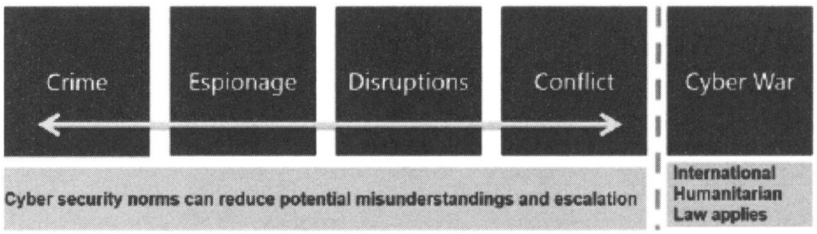

Figure 1: The Spectrum of Cyber Conflict (Source: Neutze and Nicholas)

Potential Cyber-conflict Spectrum. What does conflict in cyberspace look like? First of all, it will likely not resemble Hollywood blockbusters. Cyber conflict is perhaps best thought of as part of a spectrum from crime to war.

Figure 1 illustrates a spectrum with five broad categories. At the far end of the spectrum is war. The middle categories include organized conflict that does not result in a WMD-like kinetic effect, but may involve disruptions of key services including critical infrastructures, as well as espionage, surveillance, and theft of intellectual property. At the other end of the spectrum are more traditional cybercrime challenges.

Defining cyber conflict and its related terms is a complicated international endeavor. *The Tallinn Manual on the International Law Applicable to Cyber Warfare* resulted from an extensive three-year collaboration by international legal experts.[16] The authors of the manual have clarified that its contents and views do not reflect the North Atlantic Treaty Organization (NATO) or its doctrine, nor is it a reflection of the member states and their doctrines. It is simply a powerful consensus-based document that attempts to fill the gaps from failed attempts to come to agreement on key terms and definitions. The challenge is that states with military-grade cyber capabilities often do not want to define precise terminology and/or rules of engagement for fear that this might limit them or their cyber offense options. Yet, states with limited capabilities or who feel a higher degree of cyber insecurity and want to define conflict as a means of containing their potential adversaries.

Cyber Security Norms Dilemma.

The *Tallinn Manual* strikes at the heart of the problems of cyber security norms. Three rules from the manual illustrate a small portion of the complexity related to cyber security norms. One rule pertains to states knowingly allowing cyber attacks from their territories to harm other states. Another rule addresses state legal responsibility for attacks attributable to the state or its proxies. A third rule relates to what actually constitutes the use of force in cyber attacks. Each of these normative rules create challenges for governments and private sector ICT firms.

• *"Rule 5: A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used in acts that adversely or unlawfully impact other States."*[17]

- The experts could not reach consensus on whether this rule would apply if a state had knowledge of a situation where this was the case, and what constituted such knowledge. If a widely available report from ICT and antivirus firms were to name malware hosting operations in specific locations in specific countries, would that suffice as knowledge? If so, would that knowledge subsequently make the state responsible for operations executed on its soil? However, the experts generally agreed that if a state failed to act, the victim state could respond in a proportionate manner, where the use of counter measures or the right to self-defense was warranted.
- From a private sector perspective, rule 5 is somewhat puzzling. Perpetrators can launch cyber attacks from anywhere at any time, and the hosted malware that they use in an attack could exist in multiple countries or move between countries in minutes via cloud computing services. No state could realistically know ahead of time if a perpetrator planned to launch an attack on another state from within its borders without previous knowledge and surveillance of a suspected individual or organization. However, once an attack is underway, states and the private sector can work to stop the attacks.

• *"Rule 6: A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."*[18]

- Here, experts agreed on several key items. First, if the act in question was attributable to any state or organ of the state, then it was the responsibility of the state. Second, the act in question had to violate an international obligation such as a treaty or customary international law. Legal responsibility for actions would also apply to contractors acting on behalf of the state or persons who act or volunteer at the urging of the state.

• *"Rule 11: A cyber operation constitutes a use of force when its scale and effect are comparable to non-cyber operations rising to the level of a use of force."*[19]

- The lack of definitions for "threat" and "use of force" complicate establishing norms around this rule. However, the experts agreed that political and economic coercion do not constitute the use of force, and funding a hacking group does not constitute part of an insurgency. However,

> training and equipping a guerilla group with malware was deemed to constitute the use of force. The experts recognized that with no standard definition, the international community would likely judge such acts based on a certain set of criteria, including but not limited to severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[20]

The building of acceptable cyber security norms—including those which address the three issues above—will likely take years of dialogue or a serious, significant, and/or controversial incident in cyberspace.

To date, there have been two primary state-led efforts on cyber security norms, both of which have stalled on far simpler issues:

United Nations Government Group of Experts (UN-GGE). The United Nations Group of Government Experts (GGE) is attempting to build consensus around a limited set of cyber security norms focused on the cyberwar end of the threat spectrum. The GGE is a government-only group that is not required to solicit input from other non-government stakeholders. Most of the GGE effort has focused on getting the fifteen member states' representatives to agree that international law, including the Law of Armed Conflict (LOAC), should apply to conflicts in cyberspace. During much of the negotiating period, some countries, such as China, did not agree that the LOAC applies to cyberspace conflicts, officially for fear that this could lead to the militarization of cyberspace.

While GGE progress and agreement around the applicability of the LOAC to conflicts in cyberspace is important, it is by no means sufficient, as the establishment of cyber security norms is significantly broader than just the LOAC (see figure 2). Even if they do not rise to the level of armed conflict, more prevalent threats, including low intensity conflict in cyberspace, cyber-espionage, and large scale intellectual property theft exacerbate insecurity among states. This problem is due in part to the lack of a common understanding around doctrine, definitions and accepted norms of behavior in cyberspace.

Organization for Security Cooperation in Europe (OSCE) Informal Working Group on Building Confidence in Cyberspace. The OSCE has attempted to coordinate a states-only effort to build support in the international community for the development of a discrete set of confidence building measures (CBMs), aimed at increasing transparency, cooperation, and stability in the cyber ecosystem. While this effort has merit in principle, one of the organization's principle challenges has nearly doomed it from the start: the seemingly unrelated diplomatic and security disputes between member states that subsequently undermine specific, collaborative measures. In the case of cyber-CBMs, various disputes between the United States and Russia nearly derailed an agreement on basic confidence-building measures. After two years of debate, it now seems as though key OSCE players have agreed on a first

set of regional cyber CBMs. It remains unclear whether other regional fora (such as the ASEAN Regional Forum) will follow suit.

Unfortunately, delaying the development of cyber security norms not only furthers global cyber insecurity, but also hurts the global economy, which

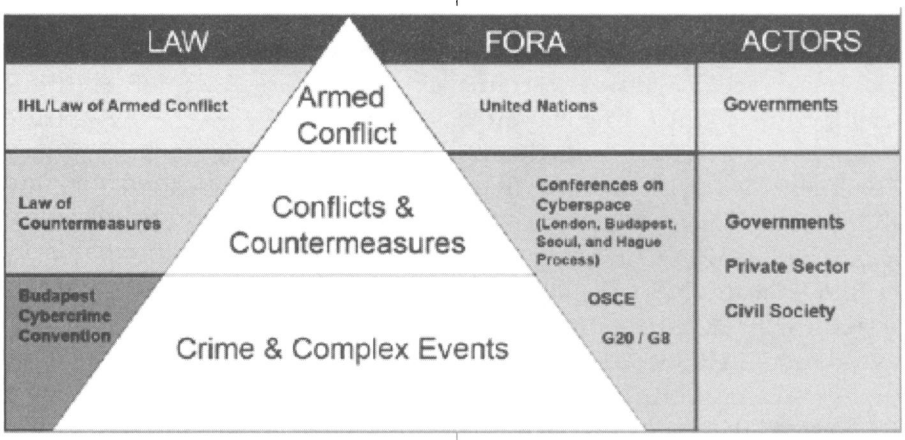

Figure 2: The Cyber security Norms Framework (Source: Neutze and Nicholas)

Beyond these limited steps, developing effective, broadly adopted cyber security norms and confidence-building measures are of critical importance not just to states, but also to the global economy and the continued development and innovation of global ICT. To date, states appear to view cyber security norms as agreements between and among states on what is acceptable behavior by military or intelligence actors. However, several states seem content with the status quo of broad cyber insecurity, because it enables them to continue growing and experimenting with cyber capabilities across a range of state powers including military, intelligence, and law enforcement.

increasingly depends on cyberspace. Moreover, states are playing a dangerous and short-sighted game. On the one hand, governments fuel cyber insecurity by ramping up offensive capabilities and buying up vulnerabilities in ICT products to create sophisticated cyber attacks. On the other hand, governments then begin to regulate the very industries whose products they attempt to exploit.

Establishing meaningful principles for cyber security norms enhances security among states and fosters confidence.

Narrowing international cyber security discussions to focus only on mil-to-mil or intel-to-intel collaboration—without addressing the broader spectrum of cyber conflict—could come at the expense of innovation, trust in digital services, and an erosion of the diverse global supply chain of ideas and creativity. This, in turn, could hurt

long-term innovation and economic growth.

A principle-based approach could help preserve innovation and competition. Focusing on key principles such as transparency, harmonization, collaboration, risk reduction, and proportionality can create a meaningful public-private dialogue.[21] Establishing meaningful principles for cyber security norms enhances security among states and fosters confidence. This confidence helps support greater private sector innovation, competition, and greater global economic opportunity. Without a set of organizing principles and fora for building norms, insecurity will grow and begin to erode the very foundations of the Internet.

Insecurity should not—and need not—function as the defining norm of cyberspace.

Conclusion. While the development of cyber security norms is both dominated and hampered by states, ensuring the stability of an ICT-dependent global economy is critical. Global ICT companies, technical, and academic experts have long established technical best practices around cyber defense, often across competitive boundaries. It is time for governments to agree to a global, multi-stakeholder norms-development process, or they may get left behind. The U.S. National Intelligence *Council's Global Trends 2030: Alternative Worlds* offers some sobering advice for governments in this regard:

> By 2030, no country—whether the US, China, or any other large country—will be a hegemonic power. The empowerment of individuals and diffusion of power among states and from states to informal networks will have a dramatic impact, largely reversing the historic rise of the West since 1750, restoring Asia's weight in the global economy, and ushering in a new era of "democratization" at the international and domestic level.[22]

Reducing cyber insecurity through norms requires a recognition that the stakeholders in norms development exist beyond simply governments. It also will require long-term stakeholder investments. First, we need to develop cyber literacy among international policymakers and diplomats. We similarly need to educate industry leaders on matters of statecraft and diplomacy. Both communities need to build a fundamental understanding of the range of cyber-conflict, including the actors and threats involved as well as national and international implications. Second, we need to broaden the range of stakeholders involved to benefit from existing technical expertise, namely in the private sector, which builds, owns, and operates the majority of today's cyberspace. Third, we need to build a global coalition that brings together the G20 countries and the twenty largest global ICT firms, whose products and services underpin cyberspace to jump-start a process of containing cyber-insecurity along the lines of "global zero" for

nuclear disarmament.

If public private dialogues stall, then the private sector should act. Private sector actors should establish a meaningful forum and agree to make it harder for governments to attack. Eight private sector companies responded strongly to National Security Agency spying and launched a global effort to reform government surveillance.[23] Yet, surveillance is only one element among the cybersecurity norms that stakeholders need to address, and it will take the active participation of many more stakeholders to make meaningful progress on cybersecurity norms.

Insecurity should not—and need not—function as the defining norm of cyberspace. Governments and the private sector should increase the speed and substance of the dialogue and begin to move forward. States can and should reduce cyber insecurity by building effective cyber security norms, and by working with the private sector to develop them. In his recent testimony, Admiral James G. Stavridis, NATO's Supreme Allied Commander for Europe and Commander of U.S. European Command, told the Senate Armed Services Committee that "Our economies are entangled in this Internet sea, and it's an outlaw sea. Nothing exists in the norms of behavior. There is a military aspect to it, but it's all of society. At some point, there needs to be a very global conversation on this challenge."[24] ■

NOTES

1 Soumitra Dutta and Beñat Bilbao-Osorio, ed., "The Global Information Technology Report 2012: Living in a Hyperconnected World," *INSEAD* and the *World Economic Forum*, Geneva: SRO-Kundig (2012); available online at http://www3.weforum.org/docs/Global_IT_Report_2012.pdf.

2 James Stavridis, "Statement of Admiral Keith B. Stavridis, United States Navy Commander, United States European Command, Before the Senate Armed Services Committee," (United States Senate, Washington, D.C., 19 March 2013) 28-29; available online at http://www.armed-services.senate.gov/download/2013/03/19/james-stavridis-testimony-031913 (date accessed: 8 December 2013).

3 Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Armed Services Committee," (United States Senate, Washington, D.C., 12 March 2013); available online at http://www.armed-services.senate.gov/statemnt/2013/03%20March/Alexander%2003-12-13.pdf (date accessed: 8 December 2013).

4 "Brazilian Army prepares its CDCiber, the 'Cyber Defense Center," Internet, http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/ (date accessed: 8 Decembwer 2013); "Japan to establish cyber defense force in 2013," Internet, http://defensesystems.com/articles/2012/09/12/agg-japan-cyber-defense-force.aspx (date accessed: 8 December 2013); For a list of countries identified by the UN as developing military cyber doctrines, see James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization," *Center for Strategic and International Studies* (2011); available online at http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (date accessed: 8 December 2013).

5 Alistair MacDonald and Paul Vieira, "Canada to Beef Up Its Cyber Defenses," *Wall Street Journal*, 17 October 2013, Internet, http://online.wsj.com/article/SB10000872396390444592704578062744030325244.html (date accessed: 11 December 2013).

6 Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Armed Services Committee," (United States Senate, Washington, D.C., 12 March 2013); available online at http://www.armed-services.senate.gov/statemnt/2013/03%20March/Alexander%2003-12-13.pdf (date accessed: 8 December 2013).

7 "The digital arms trade," *The Economist*, 30 March 2013, Internet, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade (date accessed: 8 December 2013).

8 Ibid.

9 "Security Overview for Governments," Vupen Security, Internet, http://www.vupen.com/english/services/solutions-gov.php (accessed 8 December 2013).

10 Joseph Menn, "Special Report - U.S. cyberwar strategy stokes fear of blowback," Reuters, 10 May 2013, Internet, http://uk.reuters.com/article/2013/05/10/uk-usa-cyberweapons-specialreport-idUKBRE9490EN20130510 (date accessed: 8 December 2013).

11 European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," 7 February 2013, Internet, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 (date accessed: 8 December 2013); European Commission, "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union," 7 February 2013, http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=1666 (date accessed: 8 December 2013).

12 President Barack Obama, Executive Order Executive Order 13636: Improving Critical Infrastructure Cybersecurity, 12 February 2013, Internet, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (date accessed: 17 December 2013).

13 Andrew B. Kennedy, "India must innovate in global ICT game," *The Hindu*, 26 February 2013, Internet, http://www.thehindubusinessline.com/todays-paper/tp-oncampus/india-must-innovate-in-global-ict-game/article4452979.ece.

14 National Intelligence Council, "Global Trends 2030: Alternative Worlds," Internet, http://www.dni.gov/index.php/about/organization/global-trends-2030.

15 Ibid.

16 Michael N Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2003).

17 Ibid., 26.

18 Ibid., 29-30.

19 Ibid., 45-47.

20 Ibid. 29-30.

21 *Five Principles for Shaping Cybersecurity Norms.* Microsoft Corporation. October, 2013. http:/download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8- 0063DAB88F72/Five_Principles_Norms.pdf Website not found; please recheck link. SEE COMMENT

22 National Intelligence Council, "Global Trends 2030: Alternative Worlds," Internet, http://www.dni.gov/index.php/about/organization/global-trends-2030.

23 For more information, please visit the Global Government Surveillance Reform Website: http://reformgovernmentsurveillance.com/ (date accessed: 18 December 2013).

24 James Stavridis, "Statement of Admiral Keith B. Stavridis, United States Navy Commander, United States European Command, Before the Senate Armed Services Committee," (United States Senate, Washington, D.C., 19 March 2013), 28-29; available online at http://www.armed-services.senate.gov/download/2013/03/19/james-stavridis-testimony-031913 (date accessed: 18 December 2013).