Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex

Dr. Mark Raymond

Security and intelligence practitioners are rapidly expanding their cyber capabilities to accomplish their core missions of warfighting, ensuring homeland security and advancing national security interests. However, their efforts also have significant implications for a large and expanding array of other actors, rules and institutions at both the domestic and global levels. This article discusses the emerging global regime complex for cyber issues, highlighting contemporary rule-making challenges and the potential for international conflict over the nature of the cyber regime complex. It then demonstrates the importance and the difficulty of engaging security and intelligence practitioners more closely with these processes of global rule-making, and argues that such efforts must begin at the cultural and attitudinal levels within the broader intelligence and defense communities. The article concludes by advancing modest recommendations for next steps in ensuring the engagement of security and intelligence practitioners with the global cyber regime complex. It recommends: (1) the augmentation and expansion of secondment, fellowship and exchange programs, to ensure as much dialogue and mutual learning as possible; (2) the institutionalization of capabilities for states to engage in good-faith troubleshooting when the activities of their security and intelligence practitioners have unintended negative effects on others; (3) the institutionalization of responsibility to actively consider the effects of policies, programs, and operations both on specific third parties and on the global public interest; and (4) the active promotion of all of the foregoing measures in all states that begin to develop significant cyber capabilities.

The Emerging Cyber Regime Complex

Contrary to media assertions that the Internet is an ungoverned Wild West, the Internet could not exist without a complex and robust array of rules. Internet protocols (TCP/IP, BGP, SSL, html, etc.) and hardware standards are only the tip of the iceberg.

Mark Raymond (@mraymondonir) is the Wick Cary Assistant Professor of International Security at the University of Oklahoma and a Fellow with the Center for Democracy and Technology. His work appears in International Theory, the Georgetown Journal of International Affairs and the Canadian Foreign Policy Journal. He is also the co-editor of Organized Chaos: Reimagining the Internet (Waterloo, Canada: CIGI, 2014). He has testified before the United Nations Commission on Science and Technology for Development, and participated in the Internet Governance Forum. His current research projects examine the politics of global rule-making, as well as Internet governance. He received his Ph.D. from the University of Toronto.

Many such examples have escaped notice as a result of high levels of private and non-profit governance that have caused citizens and policy-makers to take the Internet's continued existence for granted rather than treat it as the ongoing social accomplishment it truly is. Because the Internet is an ongoing social accomplishment in addition to a collection of physical infrastructure, governance issues are central to the ways in which cyber-conflict is evolving and will continue to evolve. Changes in these governance mechanisms will shape what is possible, what is likely, what is easy or difficult, and what is expensive or inexpensive. Further, there are increasing indications that a key subset of cyber conflict will revolve precisely around contesting the nature and form of these governance mechanisms. That is, cyber conflict is not merely about offensive and defensive cyber operations by state and non-state actors. It also includes attempts to shape how the administration and use of the Internet is governed. This latter dimension of (potential) cyber conflict is fundamentally a problem of rule-making. While much of this rule-making happens at the global level, the interconnected nature of the Internet at the physical and logical layers means that domestic policy and the actions of domestic firms and non-state actors can have significant negative externalities. [1] Accordingly, there are critical pressures for global coordination and cooperation on many dimensions of Internet governance even beyond the technical requirements for globally unique Internet Protocol (IP) addresses and Internet domain names (DNS).

Scholars of International Relations (IR) have understood these attempts to create policy coordination above the level of the state through the concept of an international regime. A regime in this sense is a

set of implicit and explicit principles, norms, rules and decision-making procedures that set rules of the game and shapes expectations among actors. Regimes have typically been delineated by substantive issue-areas.[2] While interconnections between different issue-specific regimes have been noted, both practitioners and scholars have (until recently) usually treated them as analytically separate entities. As a result of globalization and the increasing density of global governance mechanisms, this analytic choice may be unsustainable. For instance, Joseph S. Nye, Jr. has argued that the narrow Internet governance regime is more usefully seen as embedded in a broader cyber regime complex.[3]

A regime complex refers to a connected set of regimes that have common subject matter, at least partially overlapping membership and (as a result) generate problematic interactions.[4] For example, attempts to deal with intellectual property rights enforcement are proceeding simultaneously through the international trade regime as well as through the Internet governance regime and through domestic courts and legislatures. Similarly, attempts to create rules of the road for state conduct online are evident in the United Nations, through the Group of Governmental Experts (GGE), as well as in particular bilateral relationships (e.g. the US and China) and in NATO. There is no guarantee that the outcomes of these distinct processes will be complementary or even compatible. As a result, there is a greater need than in the past to 'deconflict' formerly distinct regimes that are now creating or that could create negative externalities for each other. Because many of these rule-sets will pertain to the work of security and intelligence practitioners, it is vital that these communities be involved in such deconflicting efforts.

While Nye is right to suggest the need to focus on the broader cyber regime complex in addition to the narrower Internet governance regime, it is important to recognize that the cyber regime complex is still in the early stages of formation. These processes of figuring out how to manage new (or at least newly salient) interactions between established rules and institutions in distinct issue-areas are evident in a large number of international processes, including: (1) the IANA function transition process and the broader review of ICANN accountability issues; (2) the World Internet Conference sponsored by China; (3) the NETmundial meeting and subsequent (controversial) "NETmundial Initiative"; (4) the decennial review of the World Summit on the Information Society (WSIS+10); (5) the UN GGE; (6) the Trans-Pacific Partnership (TPP) and Transatlantic Trade and Investment Partnership (TTIP); and (7) the UN Human Rights Council, Freedom Online Coalition and other attempts to protect rights online. These processes are characterized by increasing levels of contention. This contention has multiple causes, including path dependence, complexity and uncertainty, increasing distributional concerns and (in some cases) concerns about defection from cooperative agreements, and disagreement over legitimate procedural rules.[5] Disagreements over legitimate procedural rules for knitting formerly disparate regimes into a regime complex are especially noteworthy given the prevalence of debate over the nature and appropriateness of 'multistakeholder

governance' as a mechanism for dealing with Internet issues. Advanced industrial democracies, members of the Shanghai Cooperation Organization and members of the G-77 have distinct views about how to legitimately engage in such processes. Internet issues are further complicated by the distinctive procedural expectations of the large firms that own most Internet infrastructure and of the Internet's technical community, composed primarily of engineers and computer scientists. [6]

Meeting these challenges entails accomplishing rule-making among scores of actors with diverse views of how to do it, with different conceptions of justice and different interests, amid complexity and uncertainty, and constrained by past choices. Under these conditions, it is virtually certain that actors will experience repeated, spectacular failures in their efforts to create and operate a cyber regime complex. However, humans are relatively resilient against failures of this kind; otherwise, maintaining large-scale, complex social systems would not be possible. We routinely get all kinds of things terribly wrong, and yet life goes on. But that does not mean failure is inconsequential. We can, and should, try to minimize failures and correct them quickly. To do so, governments and other relevant actors should do three things. [7] First, they should invest heavily in thinking and learning about desirable rules and procedures for managing cyber issues. In particular, efforts should be made in any policy development process to consider possible negative externalities of decisions for other related policy and governance areas. Such efforts need to be at least on the scale of learning processes created in the early nuclear period, which was the last time governments sought to deal with the implications of a fundamentally disruptive technological advance. Second, actors should seek to create a procedural *modus vivendi.* Here, the emphasis needs to be on explicit discussion of procedural, rather than merely substantive, issues. One example would be a mechanism for determining which forum should deal with a particular issue, as well as for deciding whether a new process or institution is required. Another example would be consideration of a dispute-settlement process explicitly concerned with reconciling conflicting requirements generated by different parts of the broader regime complex. Ensuring these procedural needs are met in a manner regarded as legitimate by various actors will be difficult, but cannot be neglected if the regime complex is to operate successfully. Third, and finally, it is vital that actors remain patient and inculcate an expectation of repeated failure and iteration.

> Governance issues are central to the ways in which cyber-conflict is evolving and will continue to evolve.

Given its global, multistakeholder and highly-privatized nature, it would be unrealistic to propose the creation of a single new organization or process to address these and other

challenges in the global cyber regime complex. It would be similarly unrealistic and also inappropriate to recommend militarizing or securitizing [8] the cyber regime complex in order to ensure the proper engagement of security and intelligence practitioners. Nevertheless, involving these parties is vital to ensuring the effectiveness and legitimacy of this regime complex. The next section of this article outlines the high stakes and some considerable difficulties in involving the military and intelligence communities in the cyber regime complex. It then argues that such efforts must begin at the cultural and attitudinal levels within the security and intelligence communities, and identifies four such attitudes. The section concludes by acknowledging some promising (though incomplete) efforts on the part of security and intelligence practitioners to engage with the broader cyber regime complex.

Engaging Security and Intelligence Practitioners in the Cyber Regime Complex

The primary reason to include the military and intelligence communities in the operation of the cyber regime complex is that they affect its viability and effectiveness. Security and intelligence practitioners have had, and will continue to have, both positive and negative effects on the broader global cyber regime complex. Security and intelligence practitioners are vital to ensuring a safe online environment for critical infrastructure, e-government and e-commerce. Despite high rates of private ownership of critical Internet infrastructure, governments play important roles in incident response and in ongoing cybersecurity education through the work of Computer Security Incident Response Teams (CSIRTs) such as the United States Computer Emergency Readiness Team (US-CERT). [9] The Cybersecurity Act of 2015 enhanced the US government's role in facilitating information-sharing about the existence and nature of cyber threats. [10] Government incentivizes improvements to hardware and software standards by exercising its buying power as a large procurer of information technology products and services. [11] Further, government officials continue to engage directly with key technical standard-setting bodies and with multistakeholder policy development processes concerning Internet issues, as well as with their counterparts in other governments. In this latter respect, they can make especially important contributions to stabilizing the rules of the road for state conduct in the cyber domain. [12] Insofar as security and intelligence practitioners succeed in these various tasks, they bolster the stability and interoperability of the global Internet and thereby facilitate the operation of the global cyber regime complex.

Security and intelligence practitioners have had, and will continue to have, both positive and negative effects on the broader global cyber regime complex.

However, security and intelligence practitioners may also negatively impact the operation of the global cyber regime complex. Two such effects are particularly noteworthy. First, in the process of conducting intelligence, law enforcement or military operations they may deliberately or inadvertently (a) destroy Internet infrastructure and IT assets,[13] or (b) temporarily disrupt the normal operation of the Internet.[14] Second, they may also cause an erosion in trust by compromising (or attempting to compromise) Internet standards and technology, and by engaging in bulk data collection that is of dubious value in achieving national security objectives. Henry Farrell and Martha Finnemore have argued that the most significant damage caused by the Snowden revelations and similar leaks is a decrease in the ability of the US government to act hypocritically by simultaneously championing Internet freedom and maintaining extensive Internet monitoring.[15] Compounding the diplomatic damage from hypocrisy, former National Security Agency (NSA) official William Binneyhas suggested that these data collection programs are ineffective because they have inundated analysts with data.[16] This claim is supported, at least in the case of telephone metadata, by a White House review of NSA programs.[17]

It's likely impossible to entirely mitigate the negative effects of security and intelligence practitioners' activities on the global cyber regime complex.

James Comey, Director of the Federal Bureau of Investigation, has repeatedly advocated for a 'back door' into any encrypted communication.[18] This position has been publicly criticized by a group of leading technical experts, who suggest that it will undermine cybersecurity because of the difficulty in preventing unauthorized actors from using the same kind of access and because it has the potential to allow governments to violate human rights.[19] Comey's position has recently been disavowed by the Attorney General, Loretta Lynch,[20] but given the secrecy surrounding intelligence practices it is unlikely that such reassurances will convince skeptics. To the extent that public officials with security and intelligence portfolioscontinue to discount privacy concerns, it is likely that the that the overall legitimacy of the global cyber regime complex and public trust in the cyber domain as a whole will continue to erode.

To minimize the damage caused by their activities, and to maximize the benefits they can provide, it is important that security and intelligence practitioners become more engaged in the global cyber regime complex. However, given the confidential nature of their activities, there will clearly be challenges in ensuring appropriate levels of communication between security and intelligence practitioners on the one hand, and the remainder of the emerging global cyber regime complex on the other hand. It is

likely impossible to entirely mitigate the negative effects of security and intelligence practitioners' activities on the global cyber regime complex, just as it will be impossible to entirely avoid adverse effects on the global cyber regime complex arising from the activities of its other participants (economic regulatory agencies, firms, international organizations, etc.). However, some steps can be taken to make partial improvements. Some such steps can be taken unilaterally by security and intelligence practitioners, while others require coordination with the technology community and other members of the global cyber regime complex.

Efforts to involve security and intelligence practitioners more effectively in the global cyber regime complex must begin at the cultural and attitudinal levels since organizational cultures and attitudes have broad and enduring effects on organizational behavior.[21] While cultural and attitudinal change may also be required in the private and voluntary sectors, I focus here on such changes within the security and intelligence communities. At its most basic, involvement in the global cyber regime complex need not entail official membership in organizations, speaking publicly on cyber issues or even attending meetings. The military and intelligence communities of advanced industrial democracies and emerging powers are undoubtedly watching these processes with more interest then they did even five years ago. Yet attention may not translate into positive outcomes. Ensuring that security and intelligence practitioners' activities have the most positive effects possible on the global cyber regime complex depends on substantial part on the attitudes adopted by such communities toward these governance processes. I focus on four attitudes that can be influenced by leaders within the military and intelligence communities, and that can help to minimize the chance of problematic interactions between security agencies and other parts of the global cyber regime complex.

It is especially incumbent on security and intelligence practitioners to internalize the importance of carefully weighing the potential costs of their activities on other specific actors, and on the broader public interest.

It is especially incumbent on security and intelligence practitioners to internalize the importance of carefully weighing the potential costs of their activities on other specific actors, and on the broader public interest. The secrecy of their operations reduces (and often eliminates) opportunities for external review of the cost-benefit calculations made on such issues. For example, it is virtually impossible for such agencies to consult broadly with independent human rights experts and even with independent technical experts on the possible effects of a particular kind of cyber tool. More effectively

internalizing effects on other parties requires being acutely aware that when different communities speak of cybersecurity; they often mean different things. Referent objects of the term 'cybersecurity' include the security of the physical network and of computer protocols, the security of critical national infrastructure, the security of intellectual property, and the security of users' private information and other human rights. All of these perspectives need to be considered before reaching the conclusion that a particular kind of operation provides a net benefit.

Second, it is necessary for security and intelligence practitioners to resist the tendency to think of cyber operations as cheap or even costless. What may appear easy and cheap in the short-term may be costly in the long-term. This kind of concern is especially salient for early adopters of cyber technologies for military and intelligence purposes. Military use of such tools, as in the Stuxnet case, may encourage proliferation of such capabilities, as well as permissive international norms regarding their use. While recent work by the United Nations (UN) Group of Governmental Experts (GGE) indicates the possible emergence of basic norms for state conduct in the cyber domain,[22] contrary state practice could undermine such efforts. The other side of this coin is that if strong international norms do emerge in this area, militaries that invest heavily in such capabilities may be stuck holding devalued investments. Initially attractive intelligence programs may also turn out to be more costly in the long-run; this kind of dynamic is central to Farrell and Finnemore's argument about the costs of hypocrisy. The corrosive effects of the Snowden revelations on the cyber regime complex, and on American diplomacy more broadly, are evident.[23] While this point is related to the previous point about ensuring that costs borne by other actors are internalized in calculations of costs and benefits undertook by security and intelligence practitioners, it bears mentioning to highlight the real possibility those other actors may attempt to reimpose the costs of negative externalities on those that generate them.

Military use of such tools, as in the Stuxnet case, may encourage proliferation of such capabilities, as well as permissive international norms regarding their use.

Third, it is important to resist the tendency to think of the Internet solely as a source of threat; such over-securitization carries real costs in terms of diminished openness and interoperability, and potentially also regarding stability. The risks of framing issues in concerning security has been recognized in diverse areas of IR scholarship since very shortly after the end of the Cold War prompted a rethinking of what we mean when we invoke the phrase 'international security.' Daniel Deudney argued that reframing environmental issues in terms of security might have problematic consequences.[24]

More recently, Stefan Elbe has pointed out that securitizing the challenge of HIV/AIDS likewise poses important ethical dilemmas.[25] Lene Hansen and Helen Nissenbaum have raised these issues directly in the context of cybersecurity. They argue that "the most significant lesson" of applying securitization theory to the cyber domain is that it highlights "the political and normative implications" of employing the cybersecurity frame. They conclude that "cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized and from the political to the technified".[26] If cyber issues are prone to securitization, there is good reason to avoid further securitization at least until the issues are less novel and better understood. Securitization makes extraordinary steps (such as bulk Internet data collection) possible and diminishes opportunities for dissent or even policy review. It also contributes to a sense of urgency that may prompt rapid policy adoption that is inappropriate given the level of uncertainty about interactions between technologies and particular rule-sets.[27]

Finally, while each of these attitudes pertains to the way that security and intelligence practitioners make cost-benefit calculations in the course of fulfilling their missions, it is also important for these communities to take seriously the notion of appropriate limits on the means by which they accomplish their ends. In this regard, important current initiatives include those undertaken by various human rights bodies at the United Nations and by the GGE. The United Nations has affirmed that human rights are technologically neutral and that human rights apply online.[28] Accordingly, security and intelligence agencies are legally required to comply with their states' respective human rights obligations. The GGE has concluded that the UN Charter applies online in its entirety, and also that the law of armed conflict applies in the digital domain.[29] This suggests that states have international obligations to respect the sovereignty of other states, as well as to refrain from intentional targeting of (and disproportionate damage to) civilian facilities and infrastructure. In the last three years, the rules of the road for state conduct in the cyber domain have become far clearer. Security and intelligence professionals can, therefore, engage productively with the global cyber regime complex by carefully considering the implications of these developments for their work and determining how best to accomplish their missions within these limits.

Despite the sensitive nature of their work, security and intelligence community members have found ways to engage more closely with parts of the global cyber regime complex. Much of this engagement is with private actors and is segmented primarily on national lines. Speculation exists regarding close ties between such agencies and various proxies in China, Russia, and other states.[30] Connections between US intelligence agencies and Silicon Valley firms have also been documented.[31] Governments have also engaged more closely with the Internet Corporation for Assigned Names and Numbers (ICANN), especially through its Governmental Advisory Committee (GAC), and with other technical bodies

engaged in various aspects of Internet governance. However, such relationships typically involve government employees drawn from areas other than the military and intelligence communities.

The UN GGE remains a valuable mechanism allowing major governments to clarify their understandings of how international law applies in the cyber domain. While this work has addressed important questions of direct relevance to security and intelligence practitioners, the GGE cannot provide a sufficient venue for resolving problematic interactions between the military and intelligence communities and other parts of the cyber regime complex. First, the GGE is multilateral rather than multistakeholder in nature and thus does not provide effective means to coordinate with non-state actors. Second, it includes only a small number of governments, and enlarging it substantially risks undermining its ability to reach consensus. Third, it is an ad hoc body intended to foster dialogue on cyber norms, not to provide an ongoing facility for conflict resolution between elements in the broader global cyber regime complex.

Such mechanisms may be necessary for the long-run, but are unlikely to be created in the near future due to the complexity of creating such mechanisms among an array of heterogeneous actors with low levels of trust and high levels of uncertainty.[32] However, more modest outreach efforts to increase communication between security and intelligence practitioners and other parts of the cyber regime complex are both possible and desirable. As much as possible, these efforts should avoid strict segmentation on national lines, since coping with the potential for unintended transnational consequences is an important objective. Accordingly, states might pursue such outreach and engagement initiatives among preexisting regional and other groupings, to minimize trust problems. It is also advisable to begin by focusing on relations with academic experts. Such experts do not have the same profit motives and other incentives as private firms and even technical bodies, while they offer many of the same technical skills. The academics also include skill sets in law, policy, governance, and ethics that may be underrepresented in the private sector yet critical to improving the engagement of security and intelligence practitioners with the global cyber regime complex. Finally, military establishments often have substantial past experience in consulting with academics, for example on issues of nuclear strategy.[33] In managing such relationships, it is important for both sides to guard against outside experts being co-opted by security agencies, as such outcomes diminish the quality of the advice provided.

The United Nations has affirmed that human rights are technogically neutral, and that human rights apply online.

This article concludes by advancing modest next steps for engaging security and intelligence practitioners with the global cyber regime complex, with the goal of minimizing the problematic interactions created by their work for other components of this vital part of contemporary global governance. These proposals are by no means exhaustive. They also, cannot be expected to eliminate problems for the effectiveness and legitimacy of the cyber regime complex arising from the work of military and intelligence agencies. Rather, they are intended to assist in minimizing such effects and in responding to them productively.

CONCLUSION

Security and intelligence agencies should continue (and, where possible, expand) their outreach efforts. Personnel from military cyber units and intelligence agencies could benefit from secondment not only to allied counterparts and technology firms, but also to think tanks, digital rights advocacy groups, and universities. Similarly, there are potential gains from fellowship programs that allow experts from academia and industry to spend time in security agencies. Initiatives such as the Army Cyber Institute at West Point indicate that the US government has begun to create such mechanisms, but it is important to ensure that such programs are broad in scope, adequately resourced, and coordinated across the many different service branches and civilian agencies with cyber capabilities. Deepening whole-of-government coordination on Internet governance files will also ensure the inclusion of views from the security and intelligence community in national positions and better inform security professionals on developments in the cyber regime complex.[34] The two-way nature of these efforts is vital to their utility. Security and intelligence practitioners must remain open to learning not only about efficiency improvements in their work but also about limits on their tools and their organizational cultures intended to safeguard Internet stability and interoperability.

Second, militaries and intelligence agencies should ensure that they institutionalize the capability to engage in good-faith troubleshooting when their activities cause unintended negative consequences for third parties. This recommendation is consistent with the suggestion for the development of an 'e-SOS' function for the cyber domain and an international legal duty to assist or responsibility to troubleshoot.[35] Given security sensitivities, this may require working with affected parties at arm's length, likely through a national CSIRT. Absent some coordinating mechanism, CSIRTs and security agencies may find themselves working at cross-purposes. Coordination may not be feasible with especially sensitive programs and operations, but such conflicting efforts should be avoided where possible. Since such cases are likely to be among the most serious cyber disruptions given state capabilities, improving response quality will likely also improve the effectiveness and thus the legitimacy of the global cyber regime complex.

Third, security and intelligence agencies should institutionalize the responsibility

to actively consider the effects of their policies, programs, and operations both on specific third parties and on the global public interest. This should be done by mandating the formation and genuine empowerment of teams of individuals trained to evaluate such impacts. These teams should consist of individuals with expertise in relevant technological fields as well as in law, ethics, politics, economics and international affairs. Their operation would closely parallel the role of so-called "Red Teams" in military planning.[36] For this reason, I suggest referring to them as "Green Teams" to emphasize their non-adversarial purpose, and to distinguish them from teams focused on strategically anticipating adversaries' reactions. While at least some portions of the US security and intelligence communities already attempt to consider such issues in their decision-making processes, it is important that such teams be empowered so that they can operate independently and make themselves effectively heard. Such considerations will become even more important over time given that the maturation of cyber technologies and cyber doctrines are likely to result in cyber capabilities being diffused throughout military force structures (rather than concentrated in the hands of special purpose elements) and perhaps even automated such that certain capabilities may be triggered without human action.

Finally, states that are early adopters of cyber capabilities in the security and intelligence communities should strive to ensure that all of the foregoing recommendations are adopted by any subsequent state that develops significant cyber capacity. This is especially important with respect to the formation and empowerment of Green Teams. The use of Green Teams should be regarded as analogous to the robust control systems created to safeguard against the accidental use of nuclear weapons. Just as states recognize a continuing interest in ensuring that any new nuclear powers adopt the best available safeguards,[37] there should be a recognition that all states share a similar interest in the development of restraint on the use of many cyber tools.

The increasing density and complexity of institutions for global governance are likely to generate further connections between efforts to govern different policy issues. Given the centrality of modern information and communications technologies to various areas of social, political and economic life, the cyber regime complex is certain to occupy a position of network centrality in this system, with connections to many other kinds of institutions. As a result, problematic interactions can be expected to be both relatively frequent and consequential. Mechanisms to manage these problematic interactions should, therefore, be a major priority, in the interest of minimizing damage to the effectiveness and legitimacy of the global cyber regime complex on which the stability and interoperability of the Internet depends. Security and intelligence practitioners have an important role to play in supporting the development of such mechanisms. They can, and should, take steps along the lines recommended in this article in order to minimize the chance that their work negatively affects the operation of the global cyber regime complex and of the global communications facilities that it supports.

NOTES

1. Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs* International Engagement on Cyber III (2013a).

2. The classic definition of a regime is found in Stephen D. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," *International Organization* 36.2 (1982), 185.

3. Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series,* Paper No. 1 (2014). Available at https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

4. Amandine Orsini, Jean-Frédéric Morin and Oran Young, "Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance," *Global Governance* 19.1 (2013).

5. Timothy Simcoe, "Standard Setting Committees: Consensus Governance for Shared Technology Platforms," *American Economic Review* 102.1 (2010); Mark Raymond and Gordon Smith, "Reimagining the Internet: The Need for a High-Level Strategic Vision for Internet Governance," in Raymond and Smith (eds.), *Organized Chaos: Reimagining the Internet* (Waterloo: Centre for International Governance Innovation, 2014); Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond, "The Emergence of Contention in Global Internet Governance," Global Commission on Internet Governance Paper Series, No. 17 (Waterloo: Centre for International Governance Innovation, 2015). Available at https://www.cigionline.org/publications/emergence-of-contention-global-internet-governance.

6. Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7.3 (2015).

7. Mark Raymond, "Meeting Global Demand for Institutional Innovation in Internet Governance," in Roland Paris and Taylor Owen (eds.), *The World Won't Wait: Why Canada Needs to Rethink its International Policies* (Toronto: University of Toronto Press, 2016).

8. Securitization refers to a process of socially constructing a particular issue as an existential threat to a valued referent object, in order to motivate action that may not be politically possible absent this framing. See Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner, 1998).

9. See https://www.us-cert.gov/.

10. See https://www.congress.gov/bill/114th-congress/senate-bill/754.

11. Jeffrey Hunker, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away," *Journal of National Security Law and Policy* 4.1 (2010), 210.

12. United Nations General Assembly A/70/174 (2015).*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement (accessed January 17, 2016).

13. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53.1 (2011).

14. Anita R. Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict," Journal of Peace Research 52.3 (2015); Philip N. Howard, Sheetal D. Agarwal and Muzammil M. Hussain, "When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media," *The Communication Review* 14.3 (2011).

15. Henry Farrell and Martha Finnemore, "End of Hypocrisy: American Foreign Policy in the Age of Leaks," *Foreign Affairs* 92.6 (2013).

16. Zack Whittaker, "NSA is So Overwhelmed with Data, it's No Longer Effective, Says Whistleblower," *ZDNet* (April 30, 2015). http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/ (accessed January 22, 2016).

17. John Terbush, "Is the NSA's Data Snooping Actually Effective? *The Week* (December 19, 2013). http://theweek.com/articles/453981/nsas-data-snooping-actually-effective (accessed January 22, 2016).

18. Nicole Perlroth and David E. Sanger, "F.B.I. Director Repeats Call That Ability to Read Encrypted Messages is Crucial," *New York Times* November 18, 2015. http://www.nytimes.com/2015/11/19/us/politics/fbi-director-repeats-call-that-ability-to-read-encrypted-messages-is-crucial.html (accessed January 22, 2016).

NOTES

19. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Computer Science and Artificial Intelligence Laboratory Technical Report (Cambridge MA: Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, (July 6, 2015). http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8 (accessed January 22, 2016).

20. Jeff Stone, "Loretta Lynch: US is Not Seeking Backdoor Access to Encrypted Communication but Wants Silicon Valley's Help," *International Business Times* (January 22, 2016). http://www.ibtimes.com/loretta-lynch-us-not-seeking-backdoor-access-encrypted-communication-wants-silicon-2276297 (accessed January 22, 2016).

21. See, for example, Peter J. Katzenstein (ed.), *The Culture of National Security* (New York: Columbia University Press, 1996). For an exploration of the ways in which organizational culture can become pathological, see Michael N. Barnett and Martha Finnemore, "The Politics, Power, and Pathologies of International Organizations," *International Organization* 53.4 (1999): 699-732. For a cautiously optimistic approach to employing such culture in explaining behavior, see Alistair Iain Johnston, "Thinking About Strategic Culture," International Security 19.4 (1995), 32-64.

22. UNGA (2015).

23. See also Bradshaw et al. (2015).

24. Daniel Deudney, "The Case Against Linking Environmental Degradation and National Security," *Millennium* 19.3 (1990).

25. Stefan Elbe, "Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security," *International Studies Quarterly* 50.1 (2006).

26. Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53.4 (2009), 1172.

27. On the desirability of flexible, soft law rule-sets in situations of high uncertainty, see Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54.3 (2000), 441-444.

28. United Nations General Assembly A/Res/68/167 (2013). *The Right to Privacy in the Digital Age.* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed January 25, 2016).

29. UNGA (2015).

30. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (2013). http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed January 29, 2016). See also: Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* eds. Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (Cambridge: MIT Press, 2010).

31. James Risen and Nick Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders," *New York Times* (June 19, 2013). http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=0 (accessed January 29, 2016).

32. Barbara Koremenos, Charles Lipson and Duncan Snidal, "The Rational Design of International Institutions," *International Organization* 55.4 (2001); Mark Raymond, "Renovating the Procedural Architecture of International Law," *Canadian Foreign Policy Journal* 19.3 (2013b); Raymond and DeNardis (2015).

33. Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5.4 (2011).

34. Alexander Klimburg has called for the adoption of a 'whole of nation' approach, including firms and civil society, consistent with the more inclusive approach I call for in this article. See Alexander Klimburg, "Mobilising Cyber Power," *Survival: Global Politics and Strategy* 53.1 (2011).

35. See: Duncan Hollis, "An 'e-SOS' for Cyberspace," *Harvard International Law Journal* 52.2 (2011); Mark Raymond, "Managing Decentralized Cyber Governance: the Responsibility to Troubleshoot," Strategic Studies Quarterly 10.4 (forthcoming December 2016).

36. Gregory Fontenot, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review* 85.5 (2005).

37. Adam M. Scheinman, "Calling for Action: The Next Generation Safeguards Initiative," *The Nonproliferation Review* 16.2 (2009).