Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain

Geoff Van Epps [*]

Introduction

Significant changes in the global strategic landscape over the past two decades include the fall of the Iron Curtain and the dissolution of the Soviet Union, accelerated globalization, increasing reliance on digital information technologies in all aspects of life, the rise of China and India, global financial crises, the political revolutions of the Arab Spring, and the emergence of violent Islamist extremism as a key feature of the geopolitical landscape. Yet at the same time, many of the key dynamics of the international arena remain unchanged from twenty years ago, including the volatility and instability of the Middle East, the lack of development in most of Africa, the ever-increasing integration of the global economy, and the preeminence of the United States as an actor in global affairs, with other states, such as the United Kingdom, Germany, and Russia also playing key roles.

Among all that has changed and all that remains the same, new issues have emerged, few of which merit consideration in isolation. Rather, the complex and interconnected nature of today's international system demands analysis that accounts for the relationships between actors and issues and considers the multiplicity of effects that their interaction unavoidably creates. Two key features of the current strategic environment—the two that are the focus of this article—are the indispensability of information technology in all aspects of modern life and the continued significance of Russia as an actor on the global stage.

Driven by the growing dependence of modern society on digital technology and the vulnerability of digital systems to cyber threats, cybersecurity has emerged as a critical national security issue, spawning a growth industry that researches solutions to the technical, legal, and policy challenges of the day. At the same time, the United States and its allies in the North Atlantic Treaty Organization (NATO) contend with a Russian Federation that no longer poses the existential threat of the Soviet superpower era but still wields enough power to demand attention and to play the role of spoiler on many important global issues. The U.S. and NATO have repeatedly and publicly declared improved relations and increased cooperation with Russia to be top priorities, but that rhetoric has seldom translated to concrete improvement in their relationships or broad advancement across the agenda of critical topics. However, cybersecurity is an area of strategic importance where real progress is possible. The June 2013 announcement of a new U.S.–Russia bilateral agreement to work together on cybersecurity is an important

[*] Geoff Van Epps is a lieutenant colonel in the US Army. This article is based on research he conducted while serving as a Senior Fellow at the George C. Marshall European Center for Security Studies in Garmisch, Germany, from 2012-2013.

symbolic first step in that direction, but the accord is modest, and should merely serve as a starting point for a longer-term and more extensive program of cooperation. More tangible improvement of U.S. and NATO relations with Russia is vital, given the interconnectedness of all three actors and their status as the three most important actors in modern European—and to some extent global—security affairs. Given Russia's robust cyber capability (and demonstrated willingness to employ it), its longstanding quest for recognition as a leader in world affairs, and the public call to develop international norms for cyberspace, cybersecurity is a prime topic for U.S. and NATO engagement with Russia.

Complex Interdependence and Cyberspace

United States engagement with Russia is inevitable as both countries rank among the few states with both global interests and the ability to advance those interests. NATO, too, is inextricably bound to the U.S., with whom it shares many common values and objectives, while its geographic proximity to Russia and its intertwined (and occasionally competing) security interests make constant interaction with the Russian Federation unavoidable and highly important.

The growing entanglement between the U.S. and NATO, on one side, and Russia on the other is therefore not surprising. As globalization has accelerated and technology has advanced over the past quarter-century, the expenses associated with transportation and communication have plummeted, greatly reducing the effects of distance on economic, military, social, and other aspects of interaction between states, organizations, and even individuals.[1] Declining costs have generated a rise in the volume of interactions between these actors, conveying additional costs and benefits to all parties involved and creating a situation where each player in the web of relationships maintains a degree of interdependence on the others.[2] This interdependence—defined as the mutual dependence between parties or the ability of those parties to reciprocally affect one another—is the hallmark of globalization and the defining feature of the modern international system.[3]

The idea that actors in the international system interrelate in ways that make them reliant on one another, that this reliance extends across nearly all dimensions of their relationships, and that the behavior of those actors is affected as a consequence is both simple and powerful. The theory gained credibility and widespread acceptance over the past three decades, moving it rapidly into the mainstream of international political thought and influencing the development of foreign policy for the United States and many other countries, particularly the advanced industrial and post-industrial democracies. Applying the notion of complex interdependence to world affairs has had a recur-

---

1 Joseph S. Nye, *Understanding International Conflicts*, 4th ed. (New York: Longman, 2003), 185–92.

2 Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 3rd ed. (New York: Longman, 2001), 7–9.

3 Joseph S. Nye, "Independence and Interdependence" (1976), in Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 154; Keohane and Nye, *Power and Interdependence*, 7.

sive effect on the international system, simultaneously shaping how international actors view their relationships, craft their policies, and choose to behave while also offering plausible explanations for how and why those behaviors cause events to unfold on the world stage as they do. At the same time, an idealistic view of interdependence has fed the expectation that interdependence—especially complex interdependence, with its deepened relationships along multiple dimensions—would lead to an inexorable decline in international conflict by increasing constraints on belligerent behavior, building a sense of community among global actors, and reducing incentives for conflict.[4] Yet while complex interdependence has grown in importance and acceptance, it has not fulfilled hopes for increased global peace and cooperation.[5] Largely, this is because interdependent relationships deepen and strengthen ties between actors, but such interdependencies still can result in competition and even conflict. Most significantly, even in non-zero sum situations, where all parties benefit from a relationship, asymmetries exist, and the distribution of gains is uneven among the actors involved. As a result, interdependence does not mean uniform cooperation and an end to conflict. Rather, it creates conditions that simultaneously encourage greater cooperation in some areas while fostering conflict in others.[6]

Cyberspace provides a clear illustration of an arena where actors engage in both collaboration and fierce competition, often among the same actors and frequently at the same time. The rapid development and spread of advanced information technologies over the past few decades has generated a cyber dimension to complex interdependence that has its own unique characteristics. This information revolution has powered radical changes in politics, business, culture, and other aspects of society, spawning new types of community, encouraging the growth of organizations as networks, creating demands for new roles for government, and generally challenging hierarchical bureaucracies while fostering a trend toward decentralization.[7] The consequences of this shift are hard to overstate. Bureaucracies, whether corporate or governmental, are undercut by formal and informal organizations that more rapidly and efficiently share and process information to influence larger groups of people more quickly than traditional institutions. Individuals and private organizations have joined states as direct players in world politics. As this has occurred, the façade of the inviolable and immutable sovereignty of states has showed signs of change, with transnational communications granting the masses the

---

4 The tradition of belief that interdependence will mark the end of war can be traced to before World War I in works such as Norman Angell, *The Great Illusion: A Study of the Relation of Military Power in Nations to Their Economic and Social Advantage* (New York: Putnam, 1910). A post-Cold War analysis of the effect of interdependence on interstate conflict is Susan M. McMillan, "Interdependence and Conflict," *Mershon International Studies Review* 41 (1997): 35–36.

5 Nye, *Understanding International Conflicts*, 195.

6 Nye, "Independence and Interdependence," 154.

7 Nye, "The Information Revolution and American Soft Power" (2001), in Nye, *Power in the Global Information Age* (New York: Routledge, 2004), 81–82.

ability to engage on issues that were formerly the sole preserve of governments.[8] Such changes have not been uniform across the globe—their emergence has been much faster in the "zone of democratic peace," while virtually nonexistent in underdeveloped regions—but they nonetheless represent an order of magnitude shift in the contact among societies and demonstrate the potential for even broader alteration of the status quo.[9]

At the same time that they have instigated such drastic societal change, many of these developments have served only to reinforce the characteristics of complex interdependence: the emergence of powerful non-state global actors; the importance of non-security issues like the economy and the environment; and the effects on the ease of use of military force in an age of mass media, whistleblowers, and social networking. The computer networks that enable many of these changes—cyberspace—allow international actors to "embrace" one another by digital connection with speed, ease, and frequency.[10] Indeed, the essence of cyberspace is its connectivity, and as the volume of international digital transactions continues to grow for the foreseeable future, the ties that bind connected actors in the international system will strengthen further, and their interdependence will increase.[11] At the same time, cyberspace's unique nature, its relative immaturity as a medium, and the lack of widely accepted norms for operating within it will pose new challenges that will affect these relationships and potentially change the dynamics of complex interdependence in new and unpredictable ways.

Cyberspace and Cybersecurity

Digital interconnectedness has become a ubiquitous feature of modern life, both a cause and an effect of the growing interdependence that defines the international system. Information technology penetrates and enables every facet of society. Explosive growth in the connection of computers and computer-enabled equipment over networks that permit the rapid communication of vast amounts of information at steadily declining costs has driven changes so profound that the development and diffusion of these technologies is widely seen as comparable in scope and impact to the Industrial Revolution.[12] Digital technology now underpins the function of our world, providing the means to communicate globally, buy and sell goods and services, execute financial transactions, manage air traffic, track and predict weather, operate critical infrastructure, control industrial systems, direct the operations of military units, and perform thousands of other vital functions with unprecedented speed and precision. These developments have conveyed tremendous benefits globally, but they have not come without accompanying challenges.

---

[8] Ibid., 83–88.

[9] Keohane and Nye, *Power and Interdependence*, 217–18.

[10] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4:3 (Fall 2010): 102-35, quote on p. 121.

[11] International Telecommunications Union, *Measuring the Information Society 2012* (Geneva: International Telecommunications Union, 2012) is the annual report by the UN specialized agency that attempts to quantify the breadth and depth of the spread of information and communications technology globally.

[12] Nye, *Understanding International Conflicts,* 215,

The most prominent of these concerns is cybersecurity, which encompasses a set of related technical, policy, and legal issues that could collectively threaten the positive-sum outcomes achieved by the current webs of global interdependence and thereby alter the basis of many current, key relationships in the international system.[13]

Collectively, the information technology networks—and the hardware, software, connective lines, and data that constitute them—that facilitate our digital interconnectedness have become known as cyberspace, a complex and ever-changing manmade environment that is partly physical and partly virtual.[14] Its unique nature makes merely conceptualizing cyberspace a challenge, and achieving consensus on the exact definition of cyberspace has been elusive.[15] Most definitions, however, are consistent with the U.S. military's description of cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[16] However, the lack of agreement on what cyberspace *is* remains problematic because it affects how actors view the medium and subsequently develop capabilities, craft policies, and ultimately decide to act on cyber issues.[17]

Difficulty defining cyberspace leads inevitably to key conceptual debates whose eventual resolution will strongly influence subsequent thinking about cyber topics. As an important example, embedded in the U.S. military's definition is the idea of cyberspace as the fifth domain for military operations (along with land, sea, air, and space), which has policy and doctrine implications that can complicate discussions with allies, adversaries, and even other U.S. government stakeholders in discussions of cybersecurity issues. The U.S. Department of Defense made the conceptual leap to define cyberspace as an operational domain as "an organizing concept for DOD's national security missions" in order to "take full advantage of cyberspace's potential."[18] This declaration does not resolve the theoretical debate within DoD entirely; on the contrary, it merely provides a common conceptual framework for discussing cyber-related issues and serves more as a new starting point for discussion than a definitive end point for thinking about cyber-

---

[13] James C. Mulvenon and Gregory J. Rattray, "Addressing Cyber Instability: Executive Summary," *Cyber Conflict Studies Association Web Site* (9 July 2012), 1; available at www.thecre.com/fnews/wp-content/uploads/2012/07/CCSA-Addressing-Cyber-Instability.pdf.

[14] Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), 4.

[15] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 24. A summary of definitions of U.S., U.K., Canadian, and Australian terms can be found in David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, 2011), 36.

[16] United States Department of Defense, *Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, D.C.: Government Printing Office, 2011), 77.

[17] Betz and Stevens, *Cyberspace and the State*, 36-37.

[18] United States Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC: Government Printing Office, 2011), 5.

space.[19] At the same time, theory or policy developed from this point of view is less valuable when trying to harmonize actions with other actors who do not view cyberspace in the same terms.

Perhaps the best model for visualizing the networks of information systems themselves is offered by RAND scientist Martin Libicki, who describes cyberspace as consisting of three layers. The first layer, which undergirds the other two, is the physical components consisting of "boxes and (sometimes) wires" that forms the hardware of the information system. The middle layer is syntactic, containing the software with instructions and protocols that allow the hardware devices to function and communicate with one another. The uppermost layer is the semantic layer, containing the system's information – and therefore the reason the system exists.[20] Libicki's model helps structure discussions of cyberspace by adding shape, scope, and tangibility to the concept, but like all models it has limitations and may not withstand the test of time as the complexity of information systems continues to grow and new technologies change the design and function of these systems.

Another important ongoing debate deals with whether or not cyberspace constitutes an international commons. Those who argue that cyberspace is a commons do so because it shares characteristics with the other global commons of air, sea, and space, and because the idea of a global commons is widely understood and accepted. The most significant contribution of the idea of cyberspace as a commons is that, by definition, the global commons do not fall under the jurisdiction of a single country and their joint use is governed by international norms – much as many authorities argue is the case with cyberspace today.[21] Those experts who reject the idea of cyberspace as a commons find fault with the idea that the Internet is borderless and that nation-states have no ability to exercise sovereignty within cyberspace. In their view, nearly all of the infrastructure comprising cyberspace—the physical layer, to use Libicki's construct—resides within the borders of a sovereign state and is, therefore, subject to the laws of that state.[22] Re-

---

[19] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 12. See also Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security,* for a more extensive analysis.

[20] Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), 12–13.

[21] Leon E. Panetta, "America's Pacific Rebalance," *Project Syndicate* (31 December 2012); available at http://www.project-syndicate.org/commentary/renewing-the-us-commitment-to-the-asia-pacific-region-by-leon-e--panetta. See also James C. Stavridis and Elton C. Parker, III, "Sailing the Cyber Sea," *Joint Forces Quarterly* 65 (2012): 62; and Mark Barrett, Dick Bedford, Elizabeth Skinner, and Eva Vergles, *Assured Access to the Global Commons* (Norfolk, VA: Supreme Allied Command Transformation, North Atlantic Treaty Organization, 2011), xii–xiii.

[22] James Lewis, "Rethinking Cyber Security—A Comprehensive Approach," speech to the Sasakawa Peace Foundation, Tokyo, Japan (12 September 2011); available at http://csis.org/files/publication/110920_Japan_speech_2011.pdf. See also Nye, *Cyber Power*, 15.

solving this debate will affect the further development of cyberspace, its architecture, governance and the values that shape it.[23] Meanwhile, disagreement on this fundamental notion impedes progress toward international consensus on rules for operating in cyberspace and on who bears responsibility for enforcing those norms.

Deficient Security

However one conceives of cyberspace, the rapid spread of and increased reliance on information technology has in many cases outstripped the ability of governments to regulate its use or even to understand the problems new technologies create. The debates on how to define cyberspace, whether or not to think of it as an operational domain, and whether or not it constitutes a global commons are important but abstract. On the other hand, the fact that most of the infrastructure of what has evolved into modern-day cyberspace is built with technology that was developed with no consideration of a need for security features is a concrete problem that has made securing cyberspace an almost Sisyphean task. The original designers of the Internet were researchers at four universities in the western United States who used federal government funding in the 1960s to create a network allowing computers at their schools to communicate directly with one another. The connection was designed in a decentralized manner in order to promote scalability, privacy, and ease of communication rather than security. Its inventors envisioned linking thousands of well-intentioned academics and scientists to exchange research – not the billions of machines and users executing the vital and occasionally sinister functions of today.[24]

As the Internet matured, grew in size, and spread from academia to government to broad civilian use, the underlying fact that the technological building blocks of the Internet were designed without security in mind emerged as its core technical problem. Today, in the words of one expert, "connectivity is currently well ahead of security."[25] Openness and ease of use have inevitably attracted malicious actors, whose sophistication and ambition grew along with the Internet, evolving from mild web page defacement in the 1990s to highly organized cyber crime syndicates and state-directed espionage and cyber attack programs today.[26] The U.S. recognizes this vulnerability, with President Barack Obama describing in a 2009 speech "the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy."[27] Consequently, early in his presidency, the Obama Administration completed a Cyberspace Policy Review and expanded the Comprehen-

---

[23] Lewis, "Rethinking Cyber Security."

[24] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 81-83.

[25] Kenneth Geers, *Strategic Cyber Security* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2011), 10.

[26] Mulvenon and Rattray, "Addressing Cyber Instability," 1–2.

[27] Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," 29 May 2009; available at www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

sive National Cybersecurity Initiative to confront "one of the most serious economic and national security challenges we face as a nation."[28]

U.S. partners and allies also acknowledge the gravity of cyber threats and are working to address the issue. In its 2010 *Strategic Concept*, NATO's description of the security environment noted, "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[29]

Similarly, Russia and China have also expressed concern about the threat posed by inadequate cybersecurity, most publicly in a letter they submitted, along with the governments of Tajikistan and Uzbekistan, to the United Nations General Assembly in 2011, calling for an international code of conduct for information security. Their proposal described the "need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security."[30] This theme is also echoed in Russia's 2013 Foreign Policy Concept, which calls for an international code of conduct for information security under UN auspices and commits to countering actions with "purposes that run counter to international law, including actions aimed at interference in the internal affairs and constituting a threat to international peace, security, and stability."[31]

All Threats Are Not Created Equal

Recognizing the fundamental lack of security in cyberspace is a necessary first step toward addressing the problem, but it is not sufficient to achieve a solution. The vulnerability opens a window to several threats, each of which targets different portions of cyberspace, has different objectives, poses a different risk to national security, and requires different solutions to mitigate. As with other cybersecurity issues, no clear consensus on classifying these threats has emerged. The U.S. Department of Defense, focused primarily on defending U.S. government computer networks, recognizes two principal categories of threat: computer network attack (CNA) and computer network exploitation

---

[28] Office of the President of the United States, *Comprehensive National Cybersecurity Initiative* (Washington, D.C.: The White House, 2009), 1; available at http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[29] North Atlantic Treaty Organization, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO, 20 November 2010), 11; available at www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[30] "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General," Sixty-sixth Session of the United Nations General Assembly, 14 September 2011.

[31] Ministry of Foreign Affairs of the Russian Federation, "Concept of the Foreign Policy of the Russian Federation," 12 February 2013; available at http://www.mid.ru/brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D.

(CNE).[32] Political scientist Joseph Nye, in a broader and more useful view of the hazards in cyberspace, sees four activities that threaten national security: espionage, crime, war, and terrorism.[33]

War and terrorism are potentially the most immediately destructive threats in cyberspace, and they correlate closely to the U.S. DoD category of computer network attack. The recently constituted U.S. Cyber Command (USCYBERCOM) is the DoD organization working to defend against these threats along with protecting defense networks against espionage. However, the USCYBERCOM mandate only extends to defending some portions of the U.S. government network; it has no responsibility for most of the civilian federal government systems, state or local government networks, or any of the private-sector digital infrastructure or the transportation, energy, finance, or communications systems they control.[34] The U.S. Department of Homeland Security bears the burden of securing the non-defense portion of the federal government network, but there is no federal agency responsible for securing the country's most critical privately-owned infrastructure from cyber attack.[35] For the NATO Alliance as a whole, responsibility is similarly fragmented, with member states taking ownership of the security of their own networks and NATO assuming responsibility from the point where NATO and national networks connect inward to shared Alliance networks.[36]

Espionage and crime may pose less immediately destructive threats than cyber war or terror attacks, but they are the most costly security threats the U.S. currently faces.[37] Cyber crime has become a highly organized and phenomenally profitable illicit activity, where modern international business practices merge with cutting-edge technology to

---

[32] Jayson M. Spade, *China's Cyber Power and America's National Security* (Carlisle, PA: U.S. Army War College, 2012), 7.

[33] Nye, *Cyber Power*, 16.

[34] Richard A. Clarke, "War from Cyberspace," *The National Interest* (November/December 2009): 33–34.

[35] Ibid., 34–35. A recent executive order expanded programs to share information on cyber threats between the federal government and the private sector, established voluntary cybersecurity best practices for critical infrastructure providers, and called for incentives to encourage compliance with the standards. See Office of the President of the United States, "Executive Order—Improving Critical Infrastructure Cybersecurity," 12 February 2013; available at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. However, with the U.S. Congress unwilling or unable to pass laws like the Cybersecurity Intelligence Sharing and Protection Act (CISPA) or the Cyber Security Act of 2012 to legislate information sharing programs and technical security standards, many of the most obvious and significant vulnerabilities in the U.S. remain unaddressed.

[36] North Atlantic Treaty Organization, "Defending the Networks: The NATO Policy on Cyber Defence," 4 October 2011; available at http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

[37] Nye, *Cyber Power*, 16.

outpace corporate and law enforcement attempts to combat the threat.[38] Internet security firm McAfee estimated in a widely quoted report that cybercriminals stole a staggering USD 1 trillion in data and intellectual property in 2008.[39] A competing firm, Symantec, issued its own annual report for 2012 and calculated more narrowly and conservatively that consumer cybercrime accounted for USD 110 billion in losses.[40] The lack of agreement on what constitutes a cybercrime combined with uneven reporting protocols makes pinpointing the exact scope of the problem difficult, but the rough order of magnitude is clear – and it is huge.[41] Notwithstanding its scope, cybercrime is, for most countries, including the U.S., not viewed as a direct threat to national security, and therefore is not an issue that the defense establishment addresses. Largely left to the law enforcement community, international cooperation to deal with cybercrime is uneven, in spite of the first international convention on cybercrime having been signed a dozen years ago. Troublingly, many of the countries where cybercrime activity is highest, most notably Russia, have not accepted international norms on cybercrime and lack either the ability or the will to curb the online criminal activity occurring within their borders.

Cyber espionage, on the other hand, is closely related to cyber crime, and has the full attention of defense ministries around the world. However, the distinction between commercial espionage, which is often considered a form of cybercrime, and defense-related espionage is not always apparent. Cyber espionage, taken as a whole, is a significant threat, but dealing with it is problematic because, at the most basic level, espionage is widely practiced and not illegal under international law.[42] Nations have conducted espionage since ancient times, and there are few incentives for them to curb activities that provide intelligence that contributes to national security and international stability.

---

[38] Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 415.

[39] McAfee and SAIC, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency* (28 March 2011), 5; available at www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf. This estimate has proven controversial in cybersecurity circles, because the number is shockingly large and because the figure has subsequently been repeated in speeches by President Obama, General Alexander from CYBERCOM, and members of Congress. Analysis of the USD 1 trillion loss estimate can be found, among other sources, at Misha Glenny, "Why You Can't Trust the Cybercrime Stats," *Wired UK* (6 November 2011); available at www.wired.co.uk/magazine/archive/2011/12/ideas-bank/cybercrime-stats. See also Andy Greenberg, "McAfee Explains the Dubious Math behind Its 'Unscientific' $1 Trillion Data Loss Claim," *Forbes* (3 August 2012); available at www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim; and Peter Maass and Megha Rajagopalan, "Does Cybercrime Really Cost $1 Trillion?" *Pro Publica* (1 August 2012); available at www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

[40] Symantec, *2012 Norton Cybercrime Report* (5 September 2012), 3; available at www.norton.com/ 2012cybercrimereport.

[41] Wilson, "Cyber Crime," 428–29.

[42] James Lewis, "Five Myths about Chinese Hackers," *Washington Post* (22 March 2013).

However, cyber espionage has some unique features that distinguish it from traditional espionage. Because it is "in many ways easier, cheaper, more successful and has few consequences,"[43] more countries are likely to participate in cyber espionage and do so more often.[44] Even now, losses to espionage annually are enormous. More important than the financial loss, however, is the transfer of invaluable intellectual property to potential adversaries, especially technologically advanced potential peer competitors like China and Russia. The head of U.S. Cyber Command, General Keith Alexander, labeled the losses "the greatest transfer of wealth in history" in a 2012 speech at the American Enterprise Institute,[45] and former White House official Richard Clarke wrote of his concern that they "might swing the balance of power in the world away from America."[46]

Just as the distinction between cyber espionage and cyber crime is a slight one, the differences between espionage and attack in the cyber realm are equally subtle.[47] In fact, intrusion into a network to commit an attack appears virtually identical to an act of espionage in the initial phases,[48] and code left behind by intruders to enable further spying could be virtually indistinguishable from a program planted to damage the system in a later attack.[49] Every act of trying to gain access to a system without authorization—whether erroneously, out of curiosity, or for malicious purposes—is almost indistinguishable to the system administrators charged with defending a network, and large numbers of attempts make it difficult to identify the serious threats from all the white noise of ongoing network activity. In a 2010 speech, General Alexander claimed that "DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day."[50] While each probe does not necessarily constitute an attack, let alone a serious one, the sheer volume of potentially harmful activity demands attention and has driven the search for solutions.

As a final complication, simply recognizing—and classifying— a threat in cyberspace is challenging, but identifying the source of the threat is often an even greater problem. Attribution of any activity in cyberspace is incredibly difficult. Every actor in cyberspace can hide behind a veil of anonymity because of weak standards for creden-

---

43 Clarke and Knake, *Cyber War*, 232.

44 Ibid., 228–37.

45 Gen. Keith Alexander, "Cybersecurity and American Power," Keynote Address to the American Enterprise Institute, 9 July 2012; available at http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

46 Clarke and Knake, *Cyber War*, 237; Greg Masters, "Global Cybercrime Treaty Rejected at U.N.," *SCMagazine* (23 April 2010); available at www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/.

47 Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 69.

48 Libicki, *Cyberdeterrence and Cyberwarfare,* 16.

49 Libicki, *Cyberdeterrence and Cyberwarfare,* 24–25; Clarke, "War from Cyberspace," 33–34.

50 Gen. Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," CSIS Cybersecurity Policy Debate Series (3 June 2010), 6; available at http://csis.org/files/attachments/100603csis-alexander.pdf.

tialing and verifying user identity, and this anonymity is reinforced by the technical ease of masking an actor's identity, location, or the routing of his online activities.[51] In practical terms, this renders malicious actors in cyberspace virtually immune from discovery, as current digital forensic techniques are often inadequate for providing irrefutable proof of their identities. It also makes determining state responsibility for activities in cyberspace a laborious undertaking, as governments claim plausible deniability for actions that appear to emanate from their territory but cannot be proven to do so.[52]

No Simple Solutions

In spite of the seriousness of the vulnerabilities in cyberspace, finding solutions is not simple. The problems resemble webs of Gordian knots, often requiring cross-disciplinary approaches that combine complicated solutions with technical, legal, and policy components and often have unintended consequences in the *terra incognita* of cyberspace.[53] The complexity, overlap between problem areas, and difficulty in coordinating and standardizing responsibility for addressing issues has resulted in slow progress both nationally and at the international level.

Perhaps the most significant challenge has been the lack of an international legal regime or of any emergence of broadly accepted norms for cyberspace, either as an expanded application of existing rules or through the creation of new frameworks specific to the issue.[54] This gap is a function of the lack of a clear body of law that immediately translates to the new challenges arising in cyberspace, coupled with cyberspace's growing importance outrunning the glacial pace of developing international legal standards.[55] Without such a framework, discussion between nation-states about what constitutes acceptable behavior remains more theoretical than practical, and the consequent list of unsolved problems is eye-opening. For example, issues of state responsibility for malicious acts in cyberspace emanating from or passing through a country's borders remain an un-

---

[51] Geers, *Strategic Cyber Security*, 95.

[52] Determining state responsibility for a cyber incident has two components: degree of involvement and degree of certainty. Each of those dimensions exists along a scale from low to high, meaning that an outside observer can determine varying extents of state involvement in the activity behind the incident, and can do so with different levels of certainty. The more certain of the state's role and the higher the state's level of involvement, the greater responsibility that state bears for the incident.

[53] Maeve Dion, "Different Legal Constructs for State Responsibility," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Eneken Tikk and Anna-Maria Talihärm (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 69.

[54] The *Tallinn Manual* is a peer-reviewed but unofficial attempt to remedy this serious deficiency by an international group of experts to interpret existing international law in a cyber context. Less than a year old, the eventual influence of this document has yet to be determined. See Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[55] Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86:2 (2010): 533.

resolved and contentious issue.[56] Cybercrime remains essentially unchecked, and responsibility for responding to cross-border criminal activities is not automatically assigned or consistently acknowledged. The absence of a universal definition of beyond-the-pale behavior that constitutes a legitimate *casus belli* between states leaves unclear the lines that, if crossed, could lead to international conflict. And without a regime to provide consequences for bad behavior, it is nearly impossible to prevent disruptive or provocative actions that could forestall the emergence of standards of conduct or even serve as an outright threat to peace.[57]

Furthermore, the national frameworks for dealing with cyber-related issues, from crime to espionage to military doctrine, are often incomplete, out of date, or inadequate. Some national legal codes fail to provide even the most basic tools for combating digital fraud and theft, let alone more sophisticated or emerging criminal threats. Even the most advanced national strategies and frameworks have gaps or create tradeoffs, seeking different ways to balance, for example, responsibility for cybersecurity between government and the private sector, or the relative importance of security compared to civil liberties.[58] These national policies, in turn, are poorly harmonized internationally, even among close partners, due to the lack of global norms and differing national priorities.

Differences in prioritizing the agenda for international cybersecurity stem from fundamentally divergent understandings of the nature of cyberspace and acceptable behavior in the cyber domain. Some states, like China and Russia, consider existing international law inadequate, advocate a new international treaty to deal specifically with operations in cyberspace, value sovereignty over international cooperation, and view Internet content as a potential threat to their political stability that demands tight controls. On the other side of the debate, most advanced democracies share a view that international law can be effectively applied to cyber issues, consider a new cyber law treaty unnecessary, welcome international cooperation even at the expense of some sovereignty, and view access to the Internet and the free flow of information as fundamental rights. These incompatible perspectives complicate the development of international law on cyber issues and pose an obstacle in nearly all discussions on these matters, as the key players struggle to find common ground for cooperation on even the most fundamental issues.[59]

---

[56] Goodman, "Cyber Deterrence," 112–13.

[57] Lewis, "Rethinking Cyber Security."

[58] A repository of national cyber strategies and policies is on the NATO Cooperative Cyber Defence Centre of Excellence web page at http://ccdcoe.org/328.html.

[59] Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), 34–35. For a representative example, see Masters, "Global Cybercrime Treaty Rejected at U.N." The East-West Institute and Moscow State University's Information Security Institute have partnered in a Track 2 effort to develop consensus terminology for cybersecurity. Their first round of work produced agreement on twenty basic terms in April 2011; see Karl Frederick Rauscher and Valery Yashchenko, "Russia-US Bilateral on Cyber Security: Critical Terminology Foundations," April 2011; available at www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf. A follow-on program is underway to expand the agreed-upon lexicon even further.

As a consequence of the lack of international norms and the inconsistency of national frameworks for addressing cyber issues, "bad actors" in cyberspace—whether states, groups, or individuals—often operate beyond the reach of the victims who seek to retaliate or obtain redress for the harm that has been done to them. Shortcomings of this nature create gaps that may be exploited and lead to friction between parties. In some cases, security breaks down to the point that conflict erupts.

When Security Fails

In spite of the relative newness of cyberspace, the wide range of newsworthy cybersecurity incidents is eye-catching. The full spectrum of potential threats to national security in cyberspace may not yet be apparent, but a brief survey of the major incidents demonstrates both the evolving seriousness and variety of threats with national security implications, many of which are historically unique and have established new precedents or pose new challenges for the international community.

Early and comparatively low-impact cybersecurity incidents extend back in time to the Cold War, when the United States reportedly corrupted a Soviet spying operation by allowing oil pipeline control system components to be stolen with malicious programming that resulted in the pipeline's eventual and spectacular malfunction, producing a tremendous explosion that was the largest non-nuclear explosion ever recorded.[60] During the Second Intifada in the Palestinian Territory in 2000, Israeli government hackers disabled the public web pages of the Palestinian National Authority and Hezbollah in an attempt to disrupt command and control of the uprising. Palestinian operatives responded with cyber attacks against Israeli banks and government computer systems, sparking a sort of "cyber holy war."[61] Israel also used offensive cyber techniques to fool Syrian air defense radar as part of the Israeli Air Force bombing of a suspected Syrian nuclear site in September 2007.[62]

A long-running, shadowy espionage operation known as Titan Rain occurred from roughly 2003 to 2005, involving the systematic infiltration of U.S. and Western European government computer networks.[63] Widely judged to be a Chinese government program, the spying effort netted ten to twenty terabytes of data from U.S. military networks alone.[64] Attempts to block penetrations while they were ongoing were often futile, and the stealthy nature of the intrusions made even identifying when the networks were

---

[60] Clarke and Knake, *Cyber War*, 92–93. Other sources dispute that report, like, for example, Jeffrey Carr, "The Myth of the CIA and the Trans-Siberian Pipeline Explosion," *Digital Dao* (7 June 2012); available at http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html.

[61] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SC Magazine* (27 August 2008); available at www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.

[62] Clarke and Knake, *Cyber War*, 1–11.

[63] Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* (Spring 2009); available at www.securityaffairs.org/issues/2009/16/mazanec.php.

[64] Carr, *Inside Cyber Warfare*, 4.

compromised, for how long, and what data was stolen a matter of educated guesswork.[65] Titan Rain appears to be part of broader, long-term Chinese cyber espionage efforts sometimes referred to as an Advanced Persistent Threat (APT), and subsequent similar operations attributed to China include hacking of computer systems belonging to members of the U.S. Congress and a massive exfiltration of highly sensitive designs for U.S. defense contractor Lockheed Martin's cutting-edge F-35 Joint Strike Fighter program.[66] Although Titan Rain and related espionage programs are almost certainly of Chinese origin, China's steadfast denials are neither surprising nor unusual given the difficulty of ironclad attribution in cyberspace. Likewise, the vulnerability of even the most sensitive data to theft or corruption and the high payoff of cyber espionage programs at relatively low risk make operations of this kind increasingly likely to occur without the civilizing influence of the implicit rules of the road that have evolved to govern traditional spying.[67]

The first major interstate cyber conflict began in April 2007 when the Estonian government moved a Soviet-era Second World War memorial from its prominent location in the middle of the capital, Tallinn, to a military cemetery outside the city center. The decision sparked a vociferous reaction from Russia and from the ethnic Russian minority within Estonia, escalating to violent clashes among partisans on both sides of the issue and quickly devolving into riots and looting in the Tallinn city center. The clashes spilled over into cyberspace, where highly-wired Estonia was extremely vulnerable to disruptions of its government, financial, law enforcement, and media web sites during three weeks of increasingly intense and highly coordinated attacks.[68] Although the cyber assaults ultimately caused more inconvenience than actual damage, the incident was seminal in several important ways.[69] It was the first major, broadly aimed cyber attack on a country's government and industry as part of an international conflict and was serious enough to warrant an Estonian request for consultation with its NATO Allies under the provisions of the Atlantic Charter.[70] It also raised important questions about the

---

65 Clarke and Knake, *Cyber War*, 124–26.

66 Spade, *China's Cyber Power*, 5.

67 Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 31.

68 Geers, *Strategic Cyber Security*, 84–86.

69 Rain Ottis, "Case Studies on Cyber Conflict – Estonia 2007 and Stuxnet 2010," Presentation at the George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, 22 October 2012.

70 Ulf Häußler clarifies that the only formal consultation of a NATO member with the North Atlantic Council (NAC) under the provisions of the North Atlantic Treaty was when Turkey made the request in February 2003, just prior to the resumption of hostilities against Iraq. Although discussions at the NAC did occur in the context of the 2007 Estonia cyber attacks, neither the Council nor Estonia explicitly mentioned Article 4 in conjunction with the talks. See Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," in *International Cyber Security Legal & Policy Proceedings 2010*, ed. Christian Czosseck and Karlis Podins (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 104–5.

thresholds for the use of force and armed attacks under international law.[71] Although Russia denied responsibility, and digital forensics were unable to prove conclusively that the Russian government was behind the attacks, the totality of the evidence strongly suggests Russian state encouragement, and perhaps direction, of the attacks.[72] The Russian government's deniability in this case arose from the involvement of "patriotic hackers," who the Russian government claimed were merely incensed, Internet-savvy citizen activists, mobilized and self-organized to execute highly-coordinated attacks against specific Internet targets using tens of thousands of hijacked computers from 177 countries with no state support or assistance.[73] The disavowal of responsibility, now exceedingly common in subsequent cases, underscores the challenges of attribution and state responsibility in cyberspace. It also highlights challenges that would emerge again in later cyber incidents.

During the August 2008 Russia–Georgia War, cyber attacks synchronized with Russian ground and air operations paralyzed the Georgian ".ge" internet domain by flooding the system's servers with an unmanageable torrent of Web traffic. Government, banking, and media Web sites were overwhelmed, and even the national mobile phone network was eventually incapacitated.[74] The most significant effects were the Georgian government's inability to communicate effectively—particularly in telling its side of the story during hostilities with Russia—and the disruption of public services, especially banking, electricity, and telecommunications.[75] As with the Estonian incident, Russia strongly denied state responsibility for the cyber component of the war, although it unquestionably enjoyed strategic benefits brought about by the cyber attacks on Georgia,[76] and the organizers of the attacks clearly had foreknowledge of the ground war and assistance (if not direction) in planning, organizing, reconnoitering, and synchronizing their activities with Russian military actions.[77]

A more narrowly directed cyber operation uncovered in 2010 shed light on a newer and less public form of cyber conflict. A covert U.S.-Israeli operation named Olympic Games targeted the Iranian nuclear program.[78] One of the Olympic Games computer viruses called Stuxnet contained code that searched for specific software and hardware

---

[71] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 196–97.

[72] Kara Flook, "Russia and the Cyber Threat," American Enterprise Institute Critical Threats (13 May 2009); available at www.criticalthreats.org/russia/russia-and-cyber-threat. See also Carr, *Inside Cyber Warfare,* 3; and Goodman, "Cyber Deterrence," 111.

[73] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010), 18–25.

[74] Clarke and Knake, *Cyber War*, 17–21.

[75] Tikk, Kaska and Vihul, *International Cyber Incidents*, 77–79; Goodman, "Cyber Deterrence," 115.

[76] Carr, *Inside Cyber Warfare*, 15–19.

[77] Flook, "Russia and the Cyber Threat."

[78] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times* (1 June 2012).

configurations unique to Iranian uranium enrichment centrifuge facilities. Once it found the right combinations, it took control of the machinery and forced it to operate outside its normal parameters, interfering with the enrichment process, damaging the equipment, and causing confusion among the scientists and administrators leading the program.[79] Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction," according to former CIA director and retired Air Force General Michael V. Hayden. "Somebody crossed the Rubicon."[80] Indeed, Stuxnet was technically innovative and a watershed in terms of causing physical damage, which arguably exceeded the legal threshold for a use of force, if not an armed attack, under international law. However, since the U.S. and Israel have never formally acknowledged their roles, it also raised again the standard problems with attribution and state responsibility and further reinforced the need for concerted collective action to address the continuing challenges of cybersecurity.

Russia's Role

Russia, for all its problems, still plays a highly significant role in the international system. For a variety of reasons, it maintains sufficient power in its post-Soviet incarnation to be decisive on issues of vital importance to the international community. Though its relations with the U.S., Europe and its neighbors in the post-Soviet space are sometimes rocky, the Russian Federation's combination of physical size, geostrategic position, military brawn, economic might, natural resources, and other factors demand that Russia be considered, if not consulted, in addressing nearly every important topic on the international agenda.[81] In many cases, Russia wields sufficient influence to determine when and how key problems are resolved – or whether they will continue to fester. In spite of this critical role, or perhaps because of it, the United States and its NATO Allies struggle to maintain consistently favorable, productive, and cooperative ties with Moscow, and find it virtually impossible to transform their relationships into stable and meaningful partnerships that take advantage of their deep interdependencies and the many issues where their interests overlap.

Winston Churchill famously commented in a 1939 BBC radio address, "I cannot forecast to you the action of Russia. It is a riddle wrapped in a mystery inside an enigma, but perhaps there is a key. That key is the Russian national interest."[82] Churchill's apt observation is no less true today than it was almost three-quarters of a century ago. Russia, like most countries, will act in its own interest – or in the best interests of its national leadership. Nonetheless, understanding Russia's interests and divining how Russia will

---

[79] Ottis, "Case Studies on Cyber Conflict"; Sanger, "Obama Order."

[80] Sanger, "Obama Order."

[81] Stephen J. Blank, "Introduction," in *Prospects for U.S.-Russian Security Cooperation*, ed. Stephen J. Blank (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009), 1.

[82] Winston Churchill, "The War Memoirs of Winston Churchill," *Life Magazine* (10 May 1948): 63.

behave to further them is no easy matter.[83] The inscrutable Russian psyche affects foreign policy decisions, as Russian leaders seek to restore national prestige and earn anew the respect of the international community by demonstrating strength, assertiveness, and decisiveness in their external relations. Outside of Russia, this approach often translates to perceived arrogance or even aggressiveness in Russian behavior, leading to tempestuous relationships and borderline-erratic patterns of interaction with other countries.[84]

In spite of the lack of apparent existential threats to the Russian Federation, Russian politicians often display an attitude of insecurity against external threats and a view of the international environment as an incubator for potential menaces.[85] This outlook—and its incongruence with the broader world's view of Russia's security situation—explains much of the friction resulting from Russia's foreign policy. Viewed through this lens, Russia's consistent efforts to maintain influence in the "near abroad" of former Soviet republics and to ward off what it views as unhelpful meddling by outside powers such as the U.S., China, and Europe is designed to stabilize its periphery, buffer against outside threats, and permit the country to concentrate on domestic matters.[86] Similarly, NATO's expansion into Eastern Europe and the former Soviet Union has been vigorously opposed by Russia, with discussions of membership for Ukraine and Georgia around NATO's 2008 Bucharest Summit provoking particularly strident objections. While an impartial analysis would view NATO as a model security institution that provides regional stability that benefits the Russian Federation, Russia's opinion of NATO is quite different, seeing the Alliance as a historic rival and potential threat as it encroaches on strategically vital territory on the Russian border and threatens Russia with encirclement.[87] The European Union's Eastern Partnership has likewise been met with Russian skepticism, with Moscow holding the view that the initiative is an attempt to lure several former Soviet republics out of the Russian orbit.[88]

These long-standing difficulties have been accompanied over the years by friction over a rotating agenda of issues, recently including U.S. plans for missile defense, efforts at democracy promotion,[89] public shaming over Russia's poor human rights re-

---

[83] Samuel A. Greene and Dmitri Trenin, (*Re) Engaging Russia in an Era of Uncertainty*, Policy Brief 86 (Washington, D.C.: Carnegie Endowment for International Peace, December 2009), 4; Andrei Shleifer and Daniel Treisman, "Why Moscow Says No," *Foreign Affairs* (January/February 2011): 122–38.

[84] David J. Kramer, *The Russia Challenge: Prospects for US-Russian Relations*, Policy Brief (Washington, D.C.: The German Marshall Fund, 2009), 2.

[85] Olga Oliker, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov, *Russian Foreign Policy: Sources and Implications* (Santa Monica, CA: RAND Project Air Force, 2009), 2 and 83–84.

[86] R. Craig Nation, *Results of the "Reset" in US-Russian Relations*, Russie.Nei.Visions No. 53 (Paris: IFRI, 2010), 9; Oliker, et al., *Russian Foreign Policy*, 93–95.

[87] Linas Linkevicius, "Reset with Russia, but with Reassurance," *International Herald Tribune* (9 September 2010); Nation, *Results of the "Reset*," 13-14; Shleifer and Treisman, "Why Moscow Says No."

[88] Kramer, *The Russia Challenge*, 4.

[89] Oliker, et al., *Russian Foreign Policy*, xvi.

cord,[90] and disagreement over Libya, Syria, and Iran.[91] Relations with the West reached their nadir during Russia's August 2008 war against Georgia, when Russia's reputation suffered serious damage and Western cooperation with Russia ground to a halt.[92] After several months of deadlock, in February 2009 U.S. Vice President Joseph Biden announced the Obama Administration's desire to "press the reset button" on its relations with Russia, reversing a "dangerous drift" and emphasizing a list of common interests, including nuclear proliferation, international terrorism, and stability in Afghanistan.[93]

The results of the reset have been inconclusive. Some experts view it as having accomplished what was intended by thawing relations between the U.S. and Russia and reigniting cooperation on Afghanistan, sanctions against Iran, Russian entry into the WTO, and a new strategic arms reduction treaty.[94] Other observers are less sanguine, pointing to a slow erosion of the reset's initial promise through disagreement over Iran and Syria, questions over the legitimacy of Putin's 2012 presidential election victory, passage in the U.S. of the Magnitsky Act to sanction Russian officials who violate human rights, Russian war games simulating an invasion of Poland, and other aggravations.[95] The ultimate value of the reset may never be clear, but the need for the U.S. and NATO to continue a policy of engagement with Russia remains unchanged.

With relationships that are increasingly interdependent and interests that converge on many issues, the U.S. and NATO clearly recognize that cooperation with Russia is a necessity, and that the absence of cooperation comes at a cost.[96] Following a bilateral meeting with then-President of the Russian Federation Dmitry Medvedev in 2012, U.S. President Barack Obama affirmed this view, saying that "as two of the world's leading powers, it's absolutely critical that we communicate effectively and coordinate effectively in responding to a wide range of situations that threaten world peace and security…. [A]t a time of great challenges around the world, cooperation between the United

---

[90] Commission on U.S. Policy toward Russia, *The Right Direction for U.S. Policy toward Russia* (Washington, D.C.: The Nixon Center, March 2009), 13–14; Dmitri Trenin, et al., *The Russian Awakening* (Moscow: Carnegie Moscow Center, 2012), 8.

[91] Nation, *Results of the "Reset*," 23; David M. Herszenhorn and Nick Cumming-Bruce, "Putin Defends Stand on Syria and Chastises U.S. on Libya Outcome," *The New York Times* (21 December 2012).

[92] Robert Coalson, "Former U.S. State Dep't Official Pifer Asks, 'Are the Russians Ready to Reengage?'" *Radio Free Europe/Radio Liberty* (19 November 2012).

[93] Craig Whitlock, "'Reset' Sought on Relations with Russia, Biden Says," *Washington Post* (8 February 2009).

[94] Stephen Sestanovich, interview by Bernard Gwertzman, "Reassessing the U.S.-Russia 'Reset'," Council on Foreign Relations Web Site (13 December 2012); available at www.cfr.org/russian-federation/reassessing-us-russia-reset/p29659.

[95] Anne Gearan, "Sour U.S.-Russia Relations Threaten Obama's Foreign Policy Agenda," *Washington Post* (14 January 2013); Thomas E. Graham and Dmitri Trenin, "Why the Reset Should Be Reset," *New York Times* (12 December 2012); and Shleifer and Treisman, "Why Moscow Says No."

[96] Blank, "Introduction," 16.

States and Russia is absolutely critical to world peace and stability."[97] Similarly, the 2010 NATO Strategic Concept affirmed that "NATO–Russia cooperation is of strategic importance as it contributes to creating a common space of peace, stability and security…. [W]e remain convinced that the security of NATO and Russia is intertwined and that a strong and constructive partnership based on mutual confidence, transparency and predictability can best serve our security."[98] Russia, for its part, has taken a more cautious view, calling in its national security strategy for "an equitable and valuable strategic partnership with the United States of America, on the basis of shared interests and taking into account the key influence of Russian-American relations on the international situation as a whole" and indicating its willingness to "develop relations with NATO on the basis of equality and in the interests of strengthening the general security of the Euro-Atlantic region."[99]

Unfortunately, the current strategic dialogue is limited, both with respect to what issues are being discussed and in terms of concrete progress anywhere on the agenda. The U.S., Russia, and NATO all suffer from myopia in their views of engagement, tackling only a narrow range of issues, declining to take risks to achieve success, and thereby missing opportunities to score even minor victories.[100] This failure is disappointing, because cooperation for its own sake is fruitful as it breaks the inertia of intractability and breeds further cooperation, whether on related issues or elsewhere on the docket.[101] Tangible progress is elusive, and finding a way to achieve it must be the goal, starting with small wins, building confidence, making cooperation a habit, and ultimately taking on the most demanding tasks as trusted partners. For this reason, in an open letter published earlier this year, four former U.S. Ambassadors to Moscow and four former Soviet or Russian Ambassadors to Washington chided their current governments to work harder in this regard because "a more active search for joint projects in areas of mutual self-interest will add an important element to the structure of Russian-American stability."[102] Cybersecurity represents one key area where U.S., NATO, and Russian interests

---

[97] Barack Obama and Dmitry Medvedev, "Remarks by President Obama and President Medvedev of Russia After Bilateral Meeting," 26 March 2012.; available at www.whitehouse.gov/the-press-office/2012/03/26/remarks-president-obama-and-president-medvedev-russia-after-bilateral-me.

[98] North Atlantic Treaty Organization, *Active Engagement, Modern Defence* (Strategic Concept), 29–30.

[99] National Security Council of the Russian Federation. "Russia's National Security Strategy to 2020," 12 May 2009; available at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (English translation).

[100] Blank, "Introduction," 17; Oliker, et al., *Russian Foreign Policy*, 137; Sestanovich, "Reassessing the U.S.-Russia 'Reset'."

[101] Blank, "Introduction," 6.

[102] John Beyrle, et al. "Priorities for Russia-U.S. Relations: A Statement by Former Ambassadors to Washington and Moscow," Carnegie Endowment for International Peace Web Site (12 April 2013); available at http://carnegieendowment.org/2013/04/12/priorities-for-russia-u.s.-relations-statement-by-former-ambassadors-to-washington-and-moscow/fza1.

coincide and rapid progress is eminently achievable, providing a foundation for further collaboration and improving the broader relationships among all parties in the process.

Russia and Cybersecurity

Russia is a highly capable power in the cyber realm, described by the head of U.S. Cyber Command as a "near peer" to the U.S.,[103] with more sophistication than other advanced competitors like China and Israel.[104] This aptitude is a consequence of Russia's wealth of highly educated workers with strong technical backgrounds, who make up a large pool of skilled human capital well suited for employment on information technology endeavors.[105] Lacking outlets for this talent in the underdeveloped Russian tech industry, Russian government and organized crime networks—which appear to have a great deal of overlap in the cyber realm[106]—provide the largest markets for gainful employment.[107]

Although Russia possesses an advanced capability that ranks among the best in the world, its fundamental understanding of cybersecurity diverges widely from that of the U.S. and NATO,[108] which creates philosophical and conceptual differences that pose real—albeit surmountable—obstacles to constructive dialogue on cyber issues. At present, a lack of common understanding makes any discussion between Russia and the West on cyber topics, in the words of one expert, an act of "mutual incomprehension and apparent intransigence."[109] These differences must be understood and resolved for cooperation to bear fruit, which can only be achieved through regular dialogue and consistent interaction, a perspective reflected in the comment by the U.S. Secretary of State's Coordinator for Cyber Issues Christopher Painter that "We need to engage with countries around the world, even with those with whom we disagree."[110]

---

[103] Keir Giles, "'Information Troops' – A Russian Cyber Command?" in *3rd International Conference on Cyber Conflict*, ed. Christian Czosseck, Enn Tyugu, and Thomas Wingfield (Tallinn: CCD COE Publications, 2011), 50.

[104] James Fallows, "Cyber Warriors," *The Atlantic* (March 2010); available at www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/. See also David A. Fulghum, "China Cyber-skills Are Improving But Still Don't Top Russia and Israel," *Aviation Week* (28 March 2012).

[105] Flook, "Russia and the Cyber Threat"; Fulghum, "China Cyber-skills Are Improving."

[106] Carr, *Inside Cyber Warfare*, 124–25; Flook, "Russia and the Cyber Threat"; Joshua McGee, "US-Russia Diplomacy – The "Reset" of Relations in Cyberspace," Center for Strategic and International Studies Web Site (5 August 2011); available at http://csis.org/blog/us-russia-diplomacy-reset-relations-cyberspace.

[107] Flook, "Russia and the Cyber Threat"; "Interview with Joseph Menn, Author of Fatal System Error," *Cyveillance* (2 June 2010); available at https://blog.cyveillance.com/general-cyberintel/fatal-system-error-joseph-menn.

[108] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," *New Atlanticist* (20 June 2011); available at www.acus.org/new_atlanticist/comparing-norms-national-conduct-cyberspace.

[109] Giles, "Russia's Public Stance on Cyberspace Issues," 64.

[110] Benjamin Boudreaux, "Cyber Diplomats," *State Magazine* (April 2013): 32.

Russia does not see cybersecurity or any cyber activity as a distinct issue, standing alone and addressed in isolation, as is the tendency in the West. In fact, *cyber*—a ubiquitous term in the West—is not a word used in official Russian-language documents, except when referring to the activities of other countries. Rather, where Westerners discuss *cyber,* the Russian military community instead prefers to use the term *informationization*, viewing cyber as an embedded part of the broader concept of information operations.[111] Indeed, the foundational document for Russian information security does not contain either the words *cyber* or *Internet* anywhere in its text.[112] Rather, the Russians take a holistic, integrated approach to information operations (or information warfare) that blends a technical dimension consisting of hardware, software, and other technological components with a psychological aspect that affects information processing, perceptions, attitudes, and decisions to provide Russia an information advantage over competitors or adversaries.[113] In the Russian view, the technical dimension of cyber—protecting data and computer systems from hackers, spies, and criminals—cannot be divorced from the cognitive aspects of employing information, such as public affairs, psychological operations, deception, and so on.[114]

This point of view leads Russia to focus its national information security efforts on protecting society from "harmful" information. The notion that information might be considered dangerous highlights another important distinction between Russian and Western perspectives. The West sees information as a public good, which governments should subject to minimal controls and allow to flow as freely as possible, including over the Internet – what former U.S. Secretary of State Hillary Clinton called the "freedom to connect."[115] In contrast, the Russian Federation worries heavily about the unfettered exchange of information having a destabilizing effect on its societies, or at least on the rule of the current leadership.[116] "Internet sovereignty," or the ability of the government to monitor and, if necessary, control the information domain is an essential element of the Russian position on cybersecurity and a key component of Russia's international

[111] Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 476.

[112] "Information Security Doctrine of the Russian Federation" 9 September 2000; available at www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

[113] Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 137–52.

[114] Thomas, "Nation-State Cyber Strategies," 477–79.

[115] Hillary Clinton, "Remarks on Internet Freedom," 21 January 2010; available at www.state.gov/secretary/rm/2010/01/135519.htm

[116] Jason Healey, "Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms," *New Atlanticist* (21 September 2011); available at www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms.

efforts on cyber issues to date.[117] It also remains an important point of disagreement with the U.S. and other mature democracies.

In the international arena, the one important treaty on cybersecurity issues already in existence is the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, a major regional agreement with the potential for global acceptance. It has been adopted by thirty-nine mostly European countries—including the U.S. but not Russia—since its initiation in 2001.[118] The treaty provides a model for cooperation between different countries and with private industry in combating cybercrime, offering a template with potential for expansion to other cyber issues.[119] Russia, however, objects to ratification of the treaty as an infringement of its sovereignty, as it would invite demands for cooperation in identifying, for example, the perpetrators of the cyber attacks on Estonia in 2007 or Georgia in 2008, along with requests from foreign law enforcement agencies in shutting down the extensive cybercriminal activity that originates on Russia territory.[120]

Rather than support the Budapest Convention, Russia has emphasized the need for a new international regime that more closely corresponds to its views on cybersecurity. Russian officials and academics consistently espouse a position that existing international law is inadequate and that new accords are necessary to affirm national sovereignty and deter aggressive behavior in cyberspace.[121] Their proposals, including the 2011 letter to the UN Secretary-General it co-authored with China, Tajikistan, and Uzbekistan, generally seem to share three aims: to constrain or limit competing U.S. initiatives to develop norms in cyberspace, which they view as a means of consolidating the U.S. competitive advantage in cyberspace; to affirm the rights of countries to monitor and control the flow of information over the Internet, which they see as essential to ensuring domestic security; and to prevent the further development or proliferation of offensive cyber weapons. These tenets contrast sharply with the Western emphasis on commitment to the free flow of information, measures to combat cyber crime, and state responsibility for Internet activity occurring within a country's borders.[122] These differences might appear to be irreconcilable at first blush, limiting the odds of achieving consensus on an international framework for cyber operations.[123] However, there are many points of agreement that provide a starting point for cooperation – on securing supply

[117] Giles, "Russian Cyber Security," 2.
[118] Council of Europe, "Convention on Cybercrime, Chart of Signatures and Ratifications," 22 March 2013; available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM =&DF=&CL=ENG.
[119] Hughes, "A Treaty for Cyberspace," 534.
[120] Giles, "'Information Troops'," 51; Giles, "Russia's Public Stance on Cyberspace Issues," 67.
[121] Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views of China, the U.S., Russia, India and Norway*, ed. Andrew Nagorski (New York: EastWest Institute, 2010).
[122] Carr, *Inside Cyber Warfare*, 34–35; Healey, "Breakthrough or Just Broken?"
[123] Shane Harris, "The Cyberwar Plan," *National Journal* (14 November 2009).

chains, protecting critical infrastructure, sharing information on threats, and combating Internet use by drug traffickers and pedophiles.[124]

While Russia may view cybersecurity differently from the U.S. and its NATO partners, taking advantage of the commonalities that do exist is necessary in order to forge a broader agenda on cybersecurity, across the spectrum of security issues and, ultimately, beyond mere security to a fuller range of topics. Expanding the "envelope of cooperation" demands innovative partnering, breaking patterns of mistrust, and forging new means to identify and achieve common goals.[125] In the context of U.S.–Russia and NATO–Russia relations, this will involve reconciling the lack of U.S. and NATO trust in Russia, as well as ensuring that Russia feels like an equal partner, fully vested in the ownership and decision making of whatever venues are used for engagement. It will also require working through seemingly incompatible visions for European security, dissimilar strategic cultures, and a track record startlingly lacking in sustained tangible cooperation.[126] Both sides will have to be willing to take some risks, both in security terms and with domestic constituencies, to achieve appreciable results.[127] But such risks are a modest investment that offers the potential of substantial return on cybersecurity issues of great importance to all parties.[128]

Engaging Russia in the Cyber Domain

The U.S. and Russia have long acknowledged their mutual interest in cooperating on cybersecurity issues, stretching back to a 1998 declaration by U.S. President Bill Clinton and Russian President Boris Yeltsin that included a commitment to "mitigating the negative aspects of the information technology revolution," which they characterized as a "serious challenge" to the security of the two countries.[129] The same statement also emphasized collaboration in anticipation of Y2K,[130] which resulted in extensive joint preparations for and monitoring of potential information technology problems at the turn of the millennium.[131] Since then, the two countries have worked together primarily on is-

[124] Healey, "Breakthrough or Just Broken?"; "Russian Premier Chides USA over 'Unfair' Internet Policy, Urges 'Common Rules'," *Interfax* (30 October 2012); available at www.accessmylibrary.com/article-1G1-306951274/russian-premier-chides-usa.html.

[125] Martin E. Dempsey, "From the Chairman: Making Strategy Work," *Joint Forces Quarterly* 66 (2012): 2–3.

[126] James Sherr, "NATO and Russia: Doomed to Disappointment?" *NATO Review 2011*; available at www.nato.int/docu/review/2011/nato_russia/Disappointment/EN/index.htm.

[127] Oliker, et al., *Russian Foreign Policy*, 138.

[128] Dempsey, "From the Chairman: Making Strategy Work," 2–3.

[129] "Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century," 2 September 1998; available at http://www.gpo.gov/fdsys/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf.

[130] Ibid.

[131] Among many others, see for example Stephen Barr, "U.S., Russia Agree to Establish Y2K Center," *Washington Post* (11 September 1999); Elizabeth Becker, "U.S. and Russia Agree on Joint Defense Against Y2K Debacles," *New York Times* (28 October 1999); Tom Bowman,

sues tangentially related to cybersecurity, such as joint monitoring of electronic launch procedures for ballistic missiles and updated digital encryption standards for the White House–Kremlin hotline.[132] In December 2009, the U.S. and Russia affirmed their commitment to cooperation during a meeting of the UN Committee on Disarmament and International Security by agreeing to bolster Internet security and develop norms for military operations in cyberspace.[133] Shortly afterward, this led to a UN General Assembly Resolution calling for the "strengthening the security of global information and telecommunications systems" and "study [of] existing and potential threats in the sphere of information security and possible cooperative measures to address them."[134] U.S.–Russian concurrence on the resolution's wording—however vague and seemingly anodyne the content—represented a breakthrough in bilateral cyber diplomacy, ending ten previous years of wrangling over verbiage and leading to further official discussions on cybersecurity.[135]

Most subsequent official bilateral consultations have been held deliberately out of the public view, and have been described by U.S. Vice President Joseph Biden as designed to "build up cooperation and to set up lines of communication in the event of an alarming incident."[136] The latest series of talks, which began in February 2011, focused on cybersecurity areas of mutual concern such as exchanging technical information on threats, working toward common understanding on military operations in cyberspace, and establishing protocols for communicating between Moscow and Washington during cyber-related crises.[137] In an early gesture that suggested a symbolic effort to build trust, the U.S. complied with a proposal to exchange position papers on cyberspace by providing the Russians with the Pentagon's *Strategy for Operating in Cyberspace*[138] before

"U.S., Russian Military Ally Against Y2K Bug," *Baltimore Sun* (27 October 1999); and Elizabeth Shogren, "U.S., Russia Cooperate on Y2K Concerns," *Los Angeles Times* (2 December 1999).

[132] Franz-Stefan Gady and Greg Austin, *Russia, the United States, and Cyber Diplomacy* (New York City: EastWest Institute, 2010), i.

[133] Ibid.

[134] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/Res/64/25 (2 December 2009).

[135] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 3–4.

[136] Ellen Nakashima, "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity," *Washington Post* (26 April 2012).

[137] Howard Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace," The White House Blog (12 July 2011); available at http://www.whitehouse.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace. See also Barack Obama and Vladmir Putin, "Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building," 17 June 2013; available at www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0.

[138] United States Department of Defense, *Strategy for Operating in Cyberspace.*

the document was officially published in July 2011.[139] U.S. Cybersecurity Coordinator Howard Schmidt and Russian National Security Council Deputy Secretary Nikolay Klimashin issued a joint statement in June 2011 characterizing the discussions as "deepening mutual understanding on national security issues in cyberspace,"[140] and Schmidt later blogged that they are "a prime example of the 'Reset' in U.S.–Russia relations taking on a new and important dimension."[141]

More than two years of these talks culminated in a bilateral accord announced by U.S. President Obama and Russian President Putin in June 2013 on the sidelines of the G8 Summit in Northern Ireland. As expected, the joint statement issued by the White House described measures including information sharing between national computer emergency response teams (CERTs), expansion of the nuclear hotline to provide direct communications during cyber crises, and establishment of a cybersecurity working group within the framework of the U.S.–Russia Bilateral Presidential Commission. Although the announcement rightly calls U.S.–Russian cybersecurity cooperation "essential to safeguarding the security of our countries" and describes the agreement as "landmark steps" in helping "to meet our national and broader international interests," much work remains to be done. Mere willingness to cooperate signals the importance of cybersecurity to both parties—especially in light of the general contentiousness of U.S.–Russian relations—but the pact should be seen as a cautious but necessary first step in a deepening relationship rather than an end in itself.[142]

NATO and Russia have to date shared a relationship on cybersecurity issues that is even less auspicious. The transition from Cold War adversaries to modern partners has been halting and is still incomplete. Writ large, NATO–Russia relations are governed by the 1997 NATO–Russia Founding Act on Mutual Relations, Cooperation, and Security, which established relations on a "NATO+1" basis, meaning that NATO would act as a bloc in working bilaterally with Russia on any issue. In 2002, the Rome Declaration modified that relationship by establishing the NATO–Russia Council (NRC) as a forum for Russia to ostensibly meet as an equal partner of the NATO member states in addressing areas of common interest.[143] Since then, Russia has made repeated overtures in the NRC to cooperate on cybersecurity, but NATO has never demonstrated the willingness—i.e., the trust—to accept. During the 2012 NATO–Russia Council meeting of foreign ministers, the strongest endorsement that the parties could muster was "interest expressed in exchanging views on cybersecurity and in discussing opportunities for mili-

[139] Nakashima, "In U.S.-Russia Deal."

[140] "Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin: U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace," 23 June 2011; available at www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf.

[141] Schmidt, "U.S. and Russia: Expanding the "Reset" to Cyberspace."

[142] Obama and Putin, "Joint Statement by the Presidents of the United States and Russia."

[143] NATO–Russia Council, "About NRC," NATO-Russia Council Web Site (2013); available at www.nato-russia-council.info/en/about/.

tary-technical cooperation," hardly a clarion call for a true partnership.[144] Most recently, Russian Foreign Minister Sergey Lavrov called for Russia and NATO to work together to build up cybersecurity during the April 2013 NATO–Russia Council meeting of foreign ministers, and Lavrov later told the media that U.S. Secretary of State John Kerry had "immediately supported" the proposal, although no official U.S. or NATO statement on Lavrov's proposal followed the meetings.[145]

As with all Alliance decisions, achieving unanimity among the twenty-eight member nations is extremely difficult. Any interaction with Russia is a special challenge given the sensitivity of several current NATO countries that were either former Warsaw Pact members or Soviet republics and view their relations with Russia during the Soviet era through a lens of domination or even occupation. For them, discussions of general partnership with Russia verge on heresy, and cooperation on cybersecurity, particularly in the wake of the 2007 cyber attacks on Estonia and the 2008 Russia-Georgia War, is nearly unthinkable. Fortunately for the skittish NATO members—or, perhaps more appropriately, because without their consent, no change is possible—NATO policy essentially forbids cooperating on cybersecurity with any countries outside the Alliance except for a select group of its closest partners, requiring either a change to current policy or case-by-case exceptions to forge any real cyber partnership.[146]

An Agenda for NATO–Russian Cooperation

Absent any ongoing cooperation between NATO and Russia, a virtually blank slate exists for developing NATO's agenda to finally begin to engage Russia in the cyber domain – and NATO must acknowledge that such engagement is imperative going forward. While the NATO Policy on Cyber Defense acknowledges that NATO will "tailor its international engagement based on shared values and common approaches,"[147] and a recent NATO study called international partners "essential actors of NATO's cyber defense" with whom NATO should "develop bilateral arrangements … focusing on infor-

---

[144] North Atlantic Treaty Organization, Press Release (2012) 053, "Meeting of the NATO-Russia Council at the Level of Foreign Ministers Held in Brussels on 19 April 2012," 19 April 2012; available at www.nato.int/cps/en/natolive/official_texts_86211.htm?mode=pressrelease.

[145] Sergey Lavrov, "Speech of and Answers to Questions of Mass Media by Russian Foreign Minister Sergey Lavrov Summarizing the Results of the Session of NATO-Russia Council at the Foreign Minister Level, Brussels, 23 April 2013," Ministry of Foreign Affairs of the Russian Federation Official Site, 23 April 2013; available at www.mid.ru/BDOMP//brp_4.nsf/english/EFF6D7ADFD1A258B44257B58004CF50C.

[146] NATO's menu of partnership programs is complex and, in theory, each partner country has its own Individual Partnership and Cooperation Program with NATO, which may or may not include cybersecurity cooperation. In practice, seven non-NATO nations have comprehensive cooperation agreements for cybersecurity in place according to Gerhard Jandl, "The Challenges of Cyber Security – A Government's Perspective," *Human Security Perspectives* (2012): 26–37. See North Atlantic Treaty Organization, "Partnership Tools" for additional details on NATO partnership policy; available at www.nato.int/cps/en/natolive/topics_80925.htm.

[147] North Atlantic Treaty Organization, "Defending the Networks."

mation-sharing, exchange of best practices, and judicial agreements," Alliance gridlock has prevented NATO from even initiating a relationship with Russia on issues of mutual concern.[148] As a consequence, NATO members with favorable bilateral relations with the Russian Federation are bypassing NATO to work directly with Russia on cybersecurity and other topics, which neutralizes the collective influence of NATO and plays toward the Russian strategic goal of marginalizing NATO wherever possible.[149] Rather than sitting on the sidelines as the cyber domain is evolving around it, NATO has the opportunity and the need now to match its actions to its rhetoric by accepting Russian overtures to cooperate on cybersecurity. It should build internal consensus on engaging Russia with relatively low-cost, low-risk measures where both sides can easily find agreement as first steps toward an eventually more substantial partnership that tackles the thornier problems where the two sides have fundamental differences. Specifically, NATO should seek to cooperate with Russia to accomplish the following goals.

Add a Cybersecurity Working Group to the NATO-Russia Council. Ideally, this arrangement would establish a stand-alone working group on par with working groups covering topics like missile defense, logistics, or terrorism. If that were to provide too broad of a mandate for the Alliance partners to agree to, it could be formed as a subgroup underneath the Science for Peace and Security Committee with a much narrower and more technical purview. In any case, forming a working group at the NRC would signal the intention to work seriously with Russia on cybersecurity and would provide an organizational venue for doing so.[150]

Partner Computer Emergency Response Teams. Regardless of the level of trust between NATO and the Russian Federation, having contacts established between the technical experts who have the ability to respond in the event of a crisis is invaluable.[151] NATO should collectively adopt the pragmatic stance of some of its member states and begin a series of limited, technically-oriented exchanges between the NATO Computer Incident Response Capability Technical Center and the Russian CERT in order to exchange technical information and determine how best to communicate during a crisis.

---

[148] Vincent Joubert, *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO,* NATO Defense College Research Paper No. 76 (Rome: Imprimerie Deltamedia Group, 2012), 7.

[149] Haider Ali Hussein Mullick, "Catching the BUG (Belarus, Ukraine and Georgia) – Russia's Buffer or NATO's Annex? A New Framework for Euro-Atlantic-Russian Cooperation," *Georgetown Journal of International Affairs* (4 May 2013); available at http://journal.georgetown.edu/2013/05/04/catching-the-bug-belarus-ukraine-and-georgia-russias-buffer-or-natos-annex-a-new-framework-for-euro-atlantic-russian-cooperation-by-haider-ali-hussein-mullick/.

[150] NATO-Russia Council, "About NRC."

[151] "Joint Statement on Bilateral Discussions on Cooperation in Cybersecurity, China Institute of International Relations (CICIR)–Center for Strategic and International Studies (CSIS)," Center for Strategic and International Studies (June 2012); available at http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.

Share Cyber Intel. Because cyberspace is constantly evolving and the nefarious actors who operate within it are continually adapting, maintaining up-to-date information on cyber threats is an endless challenge. Likewise, sharing intelligence across NATO can be a sensitive and difficult process, so any proposal for trading secrets with Russia might on the surface seem dubious – except that during an April 2013 visit to Moscow, NATO Deputy Secretary-General Alexander Vershbow proposed the creation of two centers to allow Russia and NATO to share intelligence, conduct joint planning, and coordinate operations on missile defense.[152] While a final agreement on establishing these centers is nowhere near, missile defense has been as much of a source of friction between the U.S., NATO, and Russia as cybersecurity, so the proposed facilities provide a template for a cyber threat information clearinghouse as another space for NATO and Russia to cooperate. Such a clearinghouse could start small and work initially on shared analysis of excellent but unclassified data from commercial cybersecurity firms and, as trust is built, graduate to more sensitive and classified intelligence products.[153]

Develop Confidence-Building Measures. The Organization for Security and Cooperation in Europe (OSCE) is nearing completion of a set of confidence-building measures (CBMs) intended to prevent misunderstandings and avert international conflicts among its fifty-seven member countries.[154] Although the publicly available draft of the measures reveals them to be voluntary and not particularly robust,[155] the agreement, once finalized, will be important for having started a conversation on cybersecurity among over a quarter of the world's nation-states and in facilitating the exchange of cybersecurity terminology, doctrine, and contacts among the members. NATO should build on the OSCE agenda to pursue a more detailed and more ambitious set of CBMs with Russia, including joint early-warning mechanisms, exchanges of technical cybersecurity recommendations, and improvement of cyber crisis communication channels.[156] Given that all twenty-eight NATO countries and Russia are part of the OSCE, achieving

---

[152] Inna Soboleva, "NATO, Russia Consider Joint Missile-Defense System," *Russia Beyond the Headlines* (8 April 2013); available at http://rbth.ru/politics/2013/04/08/nato_russia_consider_joint_missile-defense_system_24761.html.

[153] Mandiant Intel Team, "No Clearance Required: Using Commercial Threat Intelligence in the Federal Space," Mandiant Web Site (2 May 2013); available at www.mandiant.com/blog/clearance-required-commercial-threat-intelligence-federal-space/.

[154] Aliya Sternstein, "U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact," *Nextgov* (5 December 2012); available at www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near-agreement-cyber-early-warning-pact/59977/.

[155] Jeffrey Carr, "OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous," *Digital Dao* (13 November 2012); available at http://jeffreycarr.blogspot.de/2012/11/osces-cyber-security-confidence.html#!/2012/11/osces-cyber-security-confidence.html. The hacker group Anonymous stole a confidential draft of the CBMs from the OSCE Internet server on 11 November 2012, and posted the documents online. Carr's blog provides a summary and analysis of the contents, along with a link to the stolen documents.

[156] Detlev Wolter, "Looking towards the Future of Cyber Security: What Does a Stable Cyber Environment Look Like?" Speech at the UNIDIR Cyber Security Conference 2012 (8 November 2012); available at www.unidir.ch/files/conferences/pdfs/pdf-conf1920.pdf.

consensus on confidence-building measures at the NRC should be attainable, and it would go a long way to addressing Russia's almost paralyzing fears of being blamed for a cyber incident in which it legitimately played no role.[157] And since NATO and Russia have a long track record of devising CBMs related to nuclear weapons, adapting those existing procedures and processes to cybersecurity would appear eminently achievable.

Conduct Combined Cyber Defense Exercises. Concerns about allowing Russian participation in cyber exercises abound—both objections to any Russian role and wariness over Russian intimidation of other exercise partners, especially those from the post-Soviet space—but NATO has been successfully dealing with Moscow in non-cyber contexts for years. NATO should adopt a similar approach with cybersecurity. Since 2010, U.S. European Command (EUCOM) has hosted a series of cyber defense exercises called Cyber Endeavor, nested in and simultaneous with its larger Combined Endeavor command-and-control exercise.[158] Because the EUCOM commander is dual-hatted as the NATO Supreme Allied Commander, this arrangement allows all of NATO to participate in the exercise, along with other nations that fall outside of NATO's cybersecurity cooperation policy, effectively sidestepping the NATO guidelines and expanding the circle of authorized participants. In 2012, the exercise included 175 participants from thirty-two countries, some members of NATO and some not, focused on network defense procedures and cyber incident response.[159] NATO should embrace this forum for engaging Russia by inviting it, through EUCOM, to future iterations of this exercise, initially as an observer and later as a full participant, as it has done on other, non-cyber exercises in recent years.[160]

NATO also has conducted an annual, more limited, technical cyber defense exercise series called Locked Shields through the Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn, Estonia. The 2013 exercise included CERTs from NATO headquarters, eight NATO member countries, and Finland (one of the countries NATO security policy allows the Alliance to partner with on cybersecurity issues) in a real-time network defense exercise focused on mitigating large-scale cyber attacks.[161] Although the current security policy proscribes Russian participation, the CCD COE Steering

[157] This situation, commonly referred to as a "false flag," is described in, among other sources, in Geers, *Strategic Cyber Security*, 118; and Nye, *Cyber Power,* 16–17. It was also a consistent theme of nearly every Russian speaker at the 7th International Forum for Partnership of State Authorities, Civil Society, and the Business Community in Ensuring International Information Security, held 22–25 April 2013, in Garmisch-Partenkirchen, Germany.

[158] "Exercise Combined Endeavor."

[159] James G. Stavridis, Testimony before the 113th Congress, House and Senate Armed Services Committee Testimony, 19 March 2013; available at www.armed-services.senate.gov/statemnt/2013/03%20March/Stavridis%2003-19-13.pdf, 13.

[160] James G. Stavridis, Testimony before the 112th Congress, House and Senate Armed Services Committee Testimony, 20 March 2011; available at www.armed-services.senate.gov/statemnt/2011/03%20March/ Stavridis%2003-29-11.pdf, 17.

[161] CCD COE, "NATO Team Wins the Locked Shields Cyber Defence Exercise," NATO Cooperative Cyber Defense Centre of Excellence Web Site (26 April 2013); available at www.ccdcoe.org/413.html.

Committee should ask its stakeholders for explicit permission to pursue Russian involvement in Locked Shields, first as an observer and then as a participant, perhaps partnered with another CERT.

Forge Consensus on International Cyber Law. The fundamental disagreement on the adequacy of existing international law—the U.S. and NATO want to apply current law to cyber issues, while Russia insists that a new international treaty is required—seriously inhibits progress on other cyber issues, because the law defines what is and is not permissible in cyberspace. As a first step toward resolving these differences, NATO should involve Russia in its efforts to interpret and elaborate international cyber law, which could help soften the divide that exists between the two camps.

An easy, low-risk first step is to invite Russian participants to the semi-annual International Law of Cyber Operations Course, organized by the CCD COE, the U.S. Naval War College, and the NATO School. The course is intended for legal advisors to cyber policymakers and provides a basic knowledge of international law as it applies to cyber operations. It could serve as a valuable forum for thoughtful interaction between legal experts from NATO and Russia.[162]

NATO also needs to recognize the opportunity it missed in sponsoring the development of the Tallinn Manual with virtually no representation or input provided by experts from Russia or virtually anywhere outside of Western Europe or North America, which resulted in a legal reference that essentially proselytizes to the already converted on international cyber law. As a consequence, Russia has adopted a position that either ignores or rejects (depending on the source) the interpretations of international law represented in the Tallinn Manual.[163] Future projects of this nature are important, but their impacts will be limited as long as the pool of contributors remains exclusive, as is the plan for a follow-up Tallinn 2.0 project to examine international law for cyber attacks that stay below the threshold of armed attack.[164] Admittedly, finding a Russian legal expert with the appropriate credentials who would be a constructive participant and not an obstacle to progress could prove difficult. However, when the alternative is to create another reference work that "[l]arge parts of the world will not consider … legitimate,"[165] NATO should underwrite more inclusive projects that are likelier to find widespread acceptance and narrow the differences between the opposing viewpoints on key issues of international cyber law.

---

[162] CCD COE, "International Law of Cyber Operations," NATO Cooperative Cyber Defense Centre of Excellence Web Site; available at www.ccdcoe.org/352.html.

[163] "The Applicability of International Law in Cyberspace – From If to How?" Panel Three at the Georgetown University Conference on the International Law on Cyber (10 April 2013); available at http://lsgs.georgetown.edu/events/InternationalEngagementonCyber2013/PanelThreeApplicabilityofInternationalLawinCyberspace041013.pdf. The comments of Dr. Anatoly Streltsov from Lomonosov Moscow State University in this transcript are representative.

[164] CCD COE, "Four Legal Experts Appointed as Centre's Senior Fellows," NATO Cooperative Cyber Defense Centre of Excellence Web Site (9 May 2013); available at www.ccdcoe.org/422.html.

[165] "Apply International Law to Cyber-Warfare? Good Luck," *The Economist* (23 March 2013).

U.S.–Russia Cybersecurity Engagement

Whereas NATO–Russian cyber cooperation is essentially nonexistent, U.S.–Russian bilateral cyber cooperation can best be characterized as nascent and low-key, even if the June 2013 breakthrough agreement on cybersecurity cooperation is viewed in an optimistic light. Although the 2011 U.S. *International Strategy for Cyberspace* calls for a "wide range of bilateral dialogues" to "advance common action on cyberspace's emerging challenges,"[166] publicly very little information is available about work with Russia on any cybersecurity issues beyond occasional media reports of law enforcement assistance in bringing down an Internet fraud ring.[167] New cooperation between the U.S. and Russia on cyber issues may result from the June 2013 accord, but the modest measures it contained are more token steps that indicate a desire to work together than they are deeply substantive solutions to the most pressing cybersecurity challenges the two countries face. The establishment of a cyber working group under the auspices of the U.S.–Russia Presidential Commission provides a forum for the two sides to maintain momentum toward further cooperation. Indeed, the U.S. and Russia should build on their recent achievement to solidify their relationship in cyberspace by pursuing the following steps.

Deepening CERT Partnerships. Whatever increase in interaction has taken place between U.S. and Russian CERTs that has occurred since the Obama-Putin announcement on cybersecurity cooperation has happened behind closed doors – and it has almost certainly not been enough. As with NATO–Russian CERT partnerships, the value of knowing who to call in the event of a crisis is immeasurable, and increasing the frequency of interaction between U.S. and Russian CERTs has virtually zero downside. Over time, the two sides should strive for increased real-time collaboration between technical experts and analysts, joint technical training and exchanges, sharing of information on threats and trends, and development of standardized incident response management procedures to build trust and confidence between the two teams and to increase their interoperability during crises.

Conducting Combined Cyber Defense Exercises. The U.S. should invite Russia to begin participating in its European Command-sponsored exercise Cyber Endeavor, which would be important for both direct engagement with Russia and to boost NATO's involvement with Russia on cyber defense cooperation. At the same time, U.S. Pacific Command also hosts its own annual Cyber Endeavor exercise, which in 2012 involved

[166] Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: Government Printing Office, 2011), 12.

[167] Nikola Krastev, "In U.S. Cybercrime Case, Track Record Indicates Russia Willing to Cooperate," *Radio Free Europe/Radio Liberty* (9 October 2010); available at www.rferl.org/content/In_US_Cybercrime_Case_Track_Record_Indicates_Russia_Willing_To_Cooperate/2185564.html.

twenty-two countries from the Asia-Pacific region.[168] Because none of the PACOM exercise participants are former Soviet republics or Warsaw Pact countries, Russian involvement would likely produce less controversy than it would in the European theater. The U.S. should extend invitations to the Russian Federation to both Cyber Endeavor exercises, starting as an observer and with the intent to bring it up to full participation as soon as possible. It should also work to include cyber defense dimensions to ongoing U.S.–Russian exercises like Northern Eagle, Atlas Vision, and Vigilant Eagle to improve cyber defense interoperability between the two militaries at all levels.[169]

Cooperating on Cybercrime. U.S.–Russian cooperation on cybercrime has been sporadic, while the growth of organized Russian cybercriminal networks has continued unabated in recent years, accounting for 36 percent of global cybercrime in 2011 in spite of reported Russian government efforts to crack down.[170] The ideal outcome for the U.S. would be to convince Russia to adopt the Budapest Convention, which appears unlikely given Russia's clamorous opposition on grounds of sovereignty. The U.S. should continue to press Russia to adopt the Budapest Convention, but it should not abandon its efforts to improve cooperation with Russia on combating cybercrime through the G8's Roma-Lyon High Tech Crime Sub-Group, which has produced a small but substantive program of law enforcement cooperation.[171] The U.S. should also encourage Russia's inclusion in programs that combat types of online crime where Russia has publicly advocated for increased cooperation and whose subject makes controversy unlikely, such as fighting child pornography or drug trafficking.[172] More directly, the U.S. should work to strengthen its bilateral law enforcement cooperation on cyber issues, capitalizing on the recent progress in the wake of the Boston Marathon bombings,[173] to cement its relation-

[168] Carl Hudson, "Pacific Endeavor 2012 Begins," United States Pacific Command Web Site (8 August 2012); available at www.pacom.mil/media/news/2012/08/08-pacific-endeavor-2012-begins.shtml.

[169] Gerald O'Dwyer, "Norway Hails Northern Eagle as Bridge-Builder," *DefenseNews* (24 August 2012); available at www.defensenews.com/article/20120824/DEFREG01/308240002/Norway-Hails-Northern-Eagle-Bridge-builder. See also "Military Cooperation: Past Events," U.S. Department of State Web Site; available at http://m.state.gov/mc38712.htm.

[170] Loek Essers, "Russian Cybercriminals Earned $4.5 Billion in 2011," *ComputerWorld* (24 April 2012); available at http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011.

[171] "The G8 24/7 Network of Contact Points Protocol Statement," December 2007; available at www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

[172] TASS, "Russia Calls for Cooperation in Combating Child Pornography," *Voice of Russia Radio* (1 June 2012); available at http://english.ruvr.ru/2012_06_01/76693555/. For example, in spite of its public statements, Russia is not one of the forty-nine countries that formed the Global Alliance Against Child Sexual Abuse Online in December 2012. See also United States Department of Justice. "Attorney General Eric Holder and High-Level Officials Launch Global Alliance against Child Sexual Abuse Online," Department of Justice Web Site (4 December 2012); available at www.justice.gov/opa/pr/2012/December/12-ag-1438.html.

[173] Ellen Barry, "After Boston Bombing, American Ties with Russia Improve," *New York Times* (29 April 2013).

ship and improve interaction by both sides in keeping with the countries' Mutual Legal Assistance Treaty.[174] Improved coordination should not be taken as a given in spite of the recent thaw, but a narrow window has opened for the U.S. to complement its usual efforts to press Russia on cybercrime in a way that could help address this critical organized crime issue.

Adopting Shared Public Key Infrastructure Standards. Public Key Infrastructure (PKI) is a technical concept that uses a "digital electronic signature" to verify the integrity of data and the identity of the sender during an exchange of electronic information. A 2008 report prepared for then-President-elect Obama warned, "Creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy."[175] PKI technology is an important means of providing that assurance. Its implementation in the U.S. DoD by means of Common Access Card (CAC) login, for example, resulted in a 50 percent drop in the frequency of cyber attacks the year after it was introduced.[176] The U.S. committed to working with other nations in its 2011 *National Strategy for Trusted Identities in Cyberspace*,[177] but it has proven hesitant to accept Russian overtures toward collaboration over fears of Russian attempts to control Internet content and limit its use by dissidents.[178] In spite of this, a technical working group should conduct a joint assessment of requirements and standards, with the short-term goal of developing common U.S. and Russian PKI standards in a manner that balances security requirements with civil liberties.[179] A bilateral agreement on such standards—particularly one that was technically compatible with other existing agreements—would be an important milestone toward a broader, multilateral consensus on electronic identity management.[180] Subsequent efforts could focus on creating structure and incentives for the U.S. and Russian private sectors to cooperate on future PKI standards and policy recommendations.[181] All of these measures would also help address U.S. concerns about cybercrime, Russian worries about "false flag" attacks, and shared problems in securing critical infrastructure from cyber threats.

---

[174] *Mutual Legal Assistance Treaty between the United States of America and the Russian Federation* (17 June 1999); available at www.state.gov/documents/organization/123676.pdf.

[175] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency. Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2008), 62.

[176] Ibid.

[177] Office of the President of the United States, *National Strategy for Trusted Identities in Cyberspace* (Washington, D.C.: Government Printing Office, 2011), 4.

[178] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times* (28 June 2009).

[179] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 9–12.

[180] See Combined Communications-Electronics Board, "PKI Cross-Certification Between CCEB Nations" (30 July 2007) as an example, outlining PKI standards for Australia, Canada, New Zealand, the United Kingdom, and the United States. Available at http://info.publicintelligence.net/CCEB-PKI.pdf.

[181] Gady and Austin, *Russia, the United States, and Cyber Diplomacy*, 11.

Reaching Consensus on International Law for Cyberspace. Because of the disagreement between the U.S. and the Russian Federation and their respective allies on the basic issue of the adequacy of existing international law in addressing cybersecurity issues, the development of a global consensus on these important subjects has been slow and uneven. Although Russia has long urged the development of a global treaty to regulate cyberspace, the lack of broad international support makes such an agreement extremely unlikely. Nevertheless, concurrence on norms of behavior in cyberspace is overdue and essential – and still achievable without a comprehensive international legal accord. Rather, a patchwork of bilateral or more limited multilateral agreements that share commonalities will, over time, generate agreement on the principles that are most broadly shared. While holding opposing views on many issues, the U.S. and Russia share similar perspectives on some important points. For example, a 2011 Russian document on military operations in cyberspace conceded that the international humanitarian law principles of discrimination, use of protective indicators, and prohibition on treachery apply in cyberspace.[182] While hardly earth-shattering, this concession does reveal some points of overlap in U.S. and Russian interests, and provides a point of departure for a program of engagement. This is an effort that the East-West Institute has already undertaken as a Track 2 diplomatic initiative to explore how to handle "humanitarian critical infrastructure" and how to apply the "distinctive Geneva emblem concept" (like the Red Cross or Red Crescent) in cyberspace.[183] Efforts like these should be encouraged and reinforced and, when sufficiently mature, moved into official diplomatic channels for codification – essentially adding one tile at a time to the mosaic of customary international law that will have to suffice in the absence of a comprehensive international treaty.

Conclusion

The relationships between the United States and Russia and NATO and Russia are difficult, messy affairs, with occasional highs punctuating long stretches of uncomfortable coexistence, periods of contentiousness, and intermittent unbridled acrimony. The policy issues that keep the two sides at loggerheads seems to continually refresh, with each resolved problem being replaced by another seemingly intractable dilemma almost immediately. Trust is in short supply in these relationships, along with a deficit in perceived mutual respect and equality from the Russian side that colors all interactions with the other side. In spite of these problems, Russia, NATO, and the U.S. share highly interdependent relationships politically, diplomatically, military, economically, and in many other important dimensions. In short, they need one another, particularly to address

[182] Ministry of Defense of the Russian Federation, "Conceptual Views Regarding the Activity of the Armed Forces of the Russian Federation in the Information Space."

[183] Karl Frederick Rauscher and Valery Yashchenko, eds., *Russia–U.S. Bilateral on Cyber Security: Critical Terminology Foundations* 1 (New York and Moscow: EastWest Institute and Moscow State University, April 2011), 7; available at www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf.

many of the key challenges in the current international environment, many of which demand regional or even global responses. One such issue is cybersecurity, where all three parties are among the leaders in terms of capability but where contradictory understandings of the nature of cyberspace and its uses have prevented them from banding together to tackle the many challenges posed by the cyber realm. Although progress will not be easy, U.S., NATO and Russian interests intersect in several key areas—technical capacity and standards development, threat intelligence sharing, interoperability enhancement, and consensus building on international law—that are fit for further exploration. By accepting limited and prudent risks in order to pursue this agenda, all sides stand to gain, with early advances on these subjects setting the conditions for further collaboration on cybersecurity and perhaps on a broader range of subjects as trust is generated and the habits of cooperation take hold.

Bibliography

About NRC. NATO-Russia Council Web Site, 2013.

Active Engagement, Modern Defence. Lisbon Summit, 2010.

Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Brussels: NATO, 2010.

Alexander, Keith. *U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM* In *CSIS Cybersecurity Policy Debate Series*., 2010.

Angell, Norman. *The Great Illusion: A Study of the Relation of Military Power in Nations to Their Economic and Social Advantage*. New York: Putnam, 1910.

Apply International Law to Cyber-Warfare? Good Luck. *The Economist* (2013).

Barr, Stephen. "U.S., Russia Agree to Establish Y2K Center." *Washington Post* (1999).

Barry, Ellen. "After Boston Bombing, American Ties with Russia Improve." *New York Times* (2013).

Becker, Elizabeth. "U.S. and Russia Agree on Joint Defense Against Y2K Debacles." *New York Times* (1999).

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. New York: Routledge, 2011.

Beyrle, John. *Priorities for Russia-U.S. Relations: A Statement by Former Ambassadors to Washington and Moscow*. Carnegie Endowment for International Peace Web Site, 2013.

Blank, Stephen J.. "*Introduction*." In *Prospects for U.S.-Russian Security Cooperation*, 1. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2009.

Boudreaux, Benjamin. "Cyber Diplomats." *State Magazine* (2013): 32.

Bowman, Tom. "U.S., Russian Military Ally Against Y2K Bug." *Baltimore Sun* (1999).

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2010.

Carr, Jeffrey. *OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous*. Digital Dao, 2012.

Carr, Jeffrey. *The Myth of the CIA and the Trans-Siberian Pipeline Explosion*. Digital Dao, 2012.

Churchill, Winston. "The War Memoirs of Winston Churchill." *Life Magazine* (1948): 63.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins, 2010.

Clarke, Richard A.. *War from Cyberspace* In *The National Interest*., 2009.

Clinton, Hillary. *Remarks on Internet Freedom*., 2010.

Coalson, Robert. *Former U.S. State Dep't Official Pifer Asks, 'Are the Russians Ready to Reengage?'*. Radio Free Europe/Radio Liberty, 2012.

Comprehensive National Cybersecurity Initiative. Washington, D.C.: The White House, 2009.

Concept of the Foreign Policy of the Russian Federation. Ministry of Foreign Affairs of the Russian Federation, 2013.

Convention on Cybercrime, Chart of Signatures and Ratifications. Council of Europe, 2013.

Cutts, Andrew. "*Warfare and the Continuum of Cyber Risks: A Policy Perspective*." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 69. Amsterdam: IOS Press, 2009.

Dempsey, Martin E.. "From the Chairman: Making Strategy Work." *Joint Forces Quarterly* 66 (2012): 2-3.

Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, 2009.

Dictionary of Military and Associated Terms In *Joint Publication*. Vol. 1-02. Washington, D.C.: United States Department of Defense, Government Printing Office, 2011.

Dion, Maeve. "*Different Legal Constructs for State Responsibility*." In *International Cyber Security Legal & Policy Proceedings 2010*, 69. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Essers, Loek. *Russian Cybercriminals Earned $4.5 Billion in 2011*. ComputerWorld, 2012.

Fallows, James. *Cyber Warriors*. The Atlantic, 2010.

Flook, Kara. *Russia and the Cyber Threat*. American Enterprise Institute Critical Threats, 2009.

Four Legal Experts Appointed as Centre's Senior Fellows. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

Fulghum, David A.. "China Cyber-skills Are Improving But Still Don't Top Russia and Israel." *Aviation Week* (2012).

Gady, Franz-Stefan, and Greg Austin. *Russia, the United States, and Cyber Diplomacy*. New York City: EastWest Institute, 2010.

Gearan, Anne. "Sour U.S.-Russia Relations Threaten Obama's Foreign Policy Agenda." *Washington Post* (2013).

Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare." *SC Magazine* (2008).

Geers, Kenneth. *Strategic Cyber Security*. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2011.

Giles, Keir. "*'Information Troops'—A Russian Cyber Command?*" In *3rd International Conference on Cyber Conflict*, 50. Tallinn: CCD COE Publications, 2011.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102-35.

Graham, Thomas E., and Dmitri Trenin. "Why the Reset Should Be Reset." *New York Times* (2012).

Greenberg, Andy. *McAfee Explains the Dubious Math behind Its 'Unscientific' $1 Trillion Data Loss Claim*. Forbes, 2012.

Greene, Samuel A., and Dmitri Trenin. *(Re) Engaging Russia in an Era of Uncertainty* In *Policy Brief*. Washington, D.C.: Carnegie Endowment for International Peace, 2009.

Grigoriev, Dmitry I.. "*Russian Priorities and Steps Towards Cybersecurity*." In *Global Cyber Deterrence: Views of China, the U.S., Russia, India and Norway*. New York: EastWest Institute, 2010.

Harris, Shane. "The Cyberwar Plan." *National Journal* (2009).

Häußler, Ulf. "*Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty*." In *International Cyber Security Legal & Policy Proceedings 2010*, 104-5. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Healey, Jason. *Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms*. New Atlanticist.

Healey, Jason. *Comparing Norms for National Conduct in Cyberspace*. New Atlanticist, 2011.

Hudson, Carl. *Pacific Endeavor 2012 Begins*. United States Pacific Command Web Site, 2012.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86, no. 2 (2010): 533.

International Law of Cyber Operations. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. Washington, D.C.: Government Printing Office, 2011.

Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin: U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace., 2011.

Joint Statement on Bilateral Discussions on Cooperation in Cybersecurity, China Institute of International Relations (CICIR)–Center for Strategic and International Studies (CSIS). Center for Strategic and International Studies, 2012.

Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century., 1998.

Joubert, Vincent. *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO* In *NATO Defense College, Research Paper*. Rome: Imprimerie Deltamedia Group, 2012.

Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. Vol. 3rd ed. New York: Longman, 2001.

Kramer, David J.. *The Russia Challenge: Prospects for US-Russian Relations* In *Policy Brief*. Washington, D.C.: The German Marshall Fund, 2009.

Kramer, Franklin D.. "*Cyberpower and National Security: Policy Recommendations for a Strategic Framework*." In *Cyberpower and National Security*, 12. Washington, D.C.: National Defense University Press, 2009.

Krastev, Nikola. *In U.S. Cybercrime Case, Track Record Indicates Russia Willing to Cooperate*. Radio Free Europe/Radio Liberty, 2010.

Kuehl, Daniel T.. "*From Cyberspace to Cyberpower: Defining the Problem*." In *Cyberpower and National Security*. Washington, D.C.: National Defense University Press, 2009.

Lavrov, Sergey. *Speech of and Answers to Questions of Mass Media by Russian Foreign Minister Sergey Lavrov Summarizing the Results of the Session of NATO-Russia Council at the Foreign Minister Level*. Brussels, 2013.

Lewis, James. "Five Myths about Chinese Hackers." *Washington Post* (2013).

Libicki, Martin. *Cyberdeterrence and Cyberwarfare*. Santa Monica, CA: RAND, 2009.

Linkevicius, Linas. "Reset with Russia, but with Reassurance." *International Herald Tribune*.

Markoff, John, and Andrew E. Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace." *New York Times* (2009).

Masters, Greg. "Global Cybercrime Treaty Rejected at U.N." *SCMagazine* (2010).

Mazanec, Brian M.. "The Art of (Cyber) War." *Journal of International Security Affairs* (2009).

McGee, Joshua. *US-Russia Diplomacy -The "Reset" of Relations in Cyberspace*. Center for Strategic and International Studies Web Site, 2011.

Measuring the Information Society 2012 . Geneva: International Telecommunications Union, 2012.

Mullick, Haider Ali Hussei. "Catching the BUG (Belarus, Ukraine and Georgia)-Russia's Buffer or NATO's Annex? A New Framework for Euro-Atlantic-Russian Cooperation." *Georgetown Journal of International Affairs* (2013).

Mulvenon, James C., and Gregory J. Rattray. *Addressing Cyber Instability: Executive Summary*. Cyber Conflict Studies Association Web Site, 2012.

Mutual Legal Assistance Treaty between the United States of America and the Russian Federation., 1999.

Nakashima, Ellen. "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity." *Washington Post* (2012).

National Strategy for Trusted Identities in Cyberspace. Washington, D.C.: Government Printing Office, 2011.

NATO Team Wins the Locked Shields Cyber Defence Exercise. NATO Cooperative Cyber Defense Centre of Excellence Web Site, 2013.

No Clearance Required: Using Commercial Threat Intelligence in the Federal Space. Mandiant Web Site, 2013.

Nye, Joseph S.. "*Independence and Interdependence*." In *Power in the Global Information Age*, 154. New York: Routledge, 2004.

Nye, Joseph S.. "*The Information Revolution and American Soft Power*." In *Power in the Global Information Age*, 81-82. New York: Routledge, 2004.

Nye, Joseph S.. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, 2010.

Nye, Joseph S.. *Understanding International Conflicts*. Vol. 4th ed. New York: Longman, 2003.

O'Dwyer, Gerald. *Norway Hails Northern Eagle as Bridge-Builder*. DefenseNews, 2012.

Obama, Barack. *Remarks by the President on Securing our Nation's Cyber Infrastructure*., 2009.

Oliker, Olga, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov. *Russian Foreign Policy: Sources and Implications*. Santa Monica, CA: RAND Project Air Force, 2009.

Panetta, Leon E.. *America's Pacific Rebalance* In *Project Syndicate*., 2012.

PKI Cross-Certification Between CCEB Nations. Combined Communications-Electronics Board, 2007.

R. Nation, Craig. "*Results of the "Reset"*." In *US-Russian Relations*, 9. Vol. Russie.Nei.Visions No. 53 . Paris: IFRI, 2010.

Rauscher, Karl Frederick, and Valery Yashchenko. *Russia–U.S. Bilateral on Cyber Security: Critical Terminology Foundations*. New York and Moscow: EastWest Institute and Moscow State University, 2011.

Russia Calls for Cooperation in Combating Child Pornography. Voice Of Russia Radio, 2012.

Russia's National Security Strategy to 2020. National Security Council of the Russian Federation, 2009.

S., Nye Joseph. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (2011): 31.

Sanger, David E.. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times* (2012).

Schmidt, Howard. *U.S. and Russia: Expanding the "Reset" to Cyberspace* In *The White House Blog*., 2011.

Schmitt, Michael N.. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Securing Cyberspace for the 44th Presidency. Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, D.C.: Center for Strategic and International Studies, 2008.

Sestanovich, Stephen. *Reassessing the U.S.-Russia 'Reset'* In *Interview by Bernard Gwertzman*. Council on Foreign Relations Web Site, 2012.

Shackelford, Scott J.. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (2009): 196-97.

Sherr, James. *NATO and Russia: Doomed to Disappointment?*. NATO Review, 2011.

Shleifer, Andrei, and Daniel Treisman. "Why Moscow Says No." *Foreign Affairs* (2011): 122-38.

Shogren, Elizabeth. "U.S., Russia Cooperate on Y2K Concerns." *Los Angeles Times* (1999).

Soboleva, Inna. *NATO, Russia Consider Joint Missile-Defense System*. Russia Beyond the Headlines, 2013.

Spade, Jayson M.. *China's Cyber Power and America's National Security*. Carlisle, PA: U.S. Army War College, 2012.

Stavridis, James C., and Elton C. Parker. "Sailing the Cyber Sea." *Joint Forces Quarterly* 65 (2012): 62.

Stavridis, James G.. *Testimony before the 113th Congress, House and Senate Armed Services Committee Testimony*., 2013.

Sternstein, Aliya. *U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact*. Nextgov, 2012.

Strategy for Operating in Cyberspace. Washington, DC: United States Department of Defense, Government Printing Office, 2011.

The Applicability of International Law in Cyberspace-From If to How?. Panel Three at the Georgetown University Conference on the International Law on Cyber, 2013.

The G8 24/7 Network of Contact Points Protocol Statement., 2007.

The Right Direction for U.S. Policy toward Russia. Washington, D.C.: The Nixon Center, 2009.

Thomas, Timothy L.. *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* . Fort Leavenworth, KS: Foreign Military Studies Office, 2011.

Thomas, Timothy. "*Nation-State Cyber Strategies: Examples From China and Russia*." In *Cyberpower and National Security*, 475-76. Washington, D.C.: National Defense University Press, 2009.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, 2010.

Trenin, Dmitri. *The Russian Awakening*. Moscow: Carnegie Moscow Center, 2012.

Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency. McAfee and SAIC, 2011.

Whitlock, Craig. "'Reset' Sought on Relations with Russia, Biden Says." *Washington Post* (2009).

Wilson, Clay. "*Cyber Crime*." In *Cyberpower and National Security*, 415. Washington, D.C.: National Defense University Press, 2009.

2012 Norton Cybercrime Report. Symantec, 2012.