International Arms Control and Law Enforcement in the Information Revolution:

An Examination of Cyber Warfare and Information Security

By Yury Barmin, Grace Jones, Sonya Moiseeva, and Zev Winkelman [*]

Introduction

Cyberspace influences nearly every human being in the world, as well as virtually every area of government, industry, commerce, and education. The developments of the revolution in information technology have been a source of tremendous innovation, but as the world has increased its dependency on technology for its most basic functions, it has also become more exposed to the underlying vulnerabilities in cyberspace. These vulnerabilities continue to be probed and exploited at an increasing rate, and as a result, cyberspace has become not only a major area of concern for international security, but also a new *de facto* military arena. The United States and Russia both possess significant capabilities in this realm, and their cooperation is essential to international safety and security in the era of the information revolution.

One of the biggest obstacles to greater cooperation between the U.S. and Russia in the area of cyber and information security is the U.S. emphasis on law enforcement, and Russia's concern with arms control. Both have identified criminal and terrorist use of the tools of the information revolution as potential threats to international security. However, they have not agreed as to whether military activities in cyberspace also require international regulation and control. In the early stages of international cooperation on cyber and information security, the greatest emphasis was placed on combating cybercrime. The most substantive achievement of this cooperation was the Council of Europe's (CoE) Convention on Cybercrime, which was opened for signature in Budapest on 23 November 2001.[1] The U.S. has signed and ratified the Convention, and was actively involved in its development.

Although Russia is a CoE member, it has neither signed nor ratified the Convention, primarily out of its objection to one of the Convention's provisions that allows for

---

[*] This article is drawn from the final report of Group 6 at the 2010–11 Stanford U.S.–Russia Forum. The members of Group 6 include: Yury Barmin, a fourth-year student at the Linguistic University of Nizhniy Novgorod; Grace Jones, a junior at Stanford University; Sonya Moiseeva, a first-year student at the Academy of the National Economy in Moscow; and Zev Winkelman, a Ph.D. candidate at the Goldman School of Public Policy at the University of California, Berkeley.

[1] Council of Europe, *Convention on Cybercrime* (2001); available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

unilateral trans-border access of data by law enforcement agencies of one country without notifying the authorities in another country, thus, Russia claims, violating state sovereignty. Russia's approach has been to call for international cooperation that also places some limitations on military uses of information communication technologies. The U.S. response to the Russian proposals has been a reluctance to engage in any formal discussion of limiting military operations in cyberspace, and an emphasis on the importance of the law enforcement approach. This reaction is in part due to skepticism that such limitations could be enforced in any fashion whatsoever, let alone symmetrically. Despite some recent positive signs of engagement,[2] this stalemate has held for more than a decade. The predicted cyber arms race has begun, resulting in the further expansion of cyber capabilities in the U.S. and Russia, as well as many other countries.[3]

The current stalemate between the two nations is only one piece of the puzzle in a long history of tensions over the cyber world, and more specifically cyber crime. There have been numerous significant attacks launched in cyberspace, including attacks by both Russia and the U.S. In 1982, Russia's infrastructure took its first hit from a cyberweapon, when a virus was inserted into the USSR's SCADA (Supervisory Control and Data Acquisition) software, resulting in a powerful explosion on the Soviet Urengoy–Surgut–Chelyabinsk natural gas pipeline. There have also been a number of cyber breaches in the U.S., including 2002 incident where a hacker illegally accessed computers at NASA's Jet Propulsion Laboratory; a teenager breaking into the systems of NYNEX in March 1997, the then-dominant telecom utility in the northeastern U.S., and cutting off Worcester Airport in Massachusetts for six hours, affecting both air and ground communications; and numerous other cases, involving both security threats and thefts of personal information.[4] A relatively new kind of cybercrime appeared in 1999, when an organized group of hackers allegedly based in Yugoslavia carried out a politically motivated, coordinated attack aimed at blocking NATO's computer networks.[5] Other attacks of this kind have been carried out

---

2 John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *The New York Times* (15 April 2010); available at http://www.nytimes.com/2010/04/16/science/16cyber.html?_r=1.

3 David Talbot, "Russia's Cybersecurity Plans," *Technology Review* (16 April 2010); available at http://www.technologyreview.com/blog/editors/25050/.

4 U.S. Department of Justice, "Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport," 18 March 1999; available at http://www.justice.gov/criminal/cybercrime/juvenilepld.htm.

5 Jose Nazario, "Politically Motivated Denial of Service Attacks," in The Virtual Battlefield: Perspectives on Cyber Warfare, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009); available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf

every year since then, including cyber attacks on U.S. military networks following the collision of a U.S. surveillance aircraft and a Chinese fighter plane in 2001, and a cyber attack organized by Russian hackers on a website called "Kavkaz Center" that promotes Chechen independence.[6] Cyber attacks have grown more frequent and destructive in recent years, including new forms of hacking called denial of service attacks (DoS) that have become a tactic of war since 2000. Today the Pentagon reports some 369 million attempts to break into its networks annually, compared to 6 million attacks in 2006.[7]

The immense threat that cyber attacks pose to critical infrastructures and state operations is clear, and recent developments in both the U.S. and Russia have emphasized the importance of addressing these issues now. In 2008, the U.S. experienced the most serious penetration of its classified military networks to date. Subsequently, on June 23 2009, U.S. Secretary of Defense Robert Gates directed U.S. Strategic Command to establish the new U.S. Cyber Command.[8] Though its cyber force structure is less clear, Russia has recently been contributing to the creation of an information security policy for the Shanghai Cooperation Organization (SCO), an alliance that includes another cyber "titan," China.

Though it is unlikely in the near term that Russia will sign the CoE Convention on Cybercrime, or that the U.S. will accept international regulations that limit its military cyber capabilities, we believe that there are several important steps that should be taken now to foster a continuous level of cooperation on cyber and information security issues that may allow for such agreements to be reached in the future. In order to provide adequate background and substantiation for our recommendations, we will first provide background on current U.S. cyber policy, Russia's information security policy, and the impact of international law in cyberspace. Finally, we will propose a set of recommendations for cooperation between the U.S. and Russia that we believe will solve some of the problems identified by both nations.

---

6 Ibid.

7 Randy James, "A Brief History of Cybercrime," *Time* (1 June 2009); available at http://www.time.com/time/nation/article/0,8599,1902073,00.html.

8 William J. Lynn, III, "Defending A New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September–October 2010); available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Background

U.S. Cybersecurity

In the United States, responsibilities for cybersecurity are scattered across many government agencies. One of the greatest areas of concern, especially for the Department of Homeland Security, is the protection of the nation's critical infrastructure. The Department of Justice focuses on the problem of cybercrime, as well as finding the balance between security and the protection of civil liberties and privacy rights. In order to understand the relationship between matters of cybersecurity and foreign policy, however, two other stakeholders are key: the executive branch and the military. President Barack Obama recently ordered a detailed review of cyberspace policy, which included an analysis of current threats and possible solutions.[9]

Released in May 2009, the "Cyberspace Policy Review" is the most current document detailing the executive branch's position on cyberspace. Numerous stakeholders are identified, including private sector enterprises, academia, international organizations, including the UN, NATO, and the CoE, as well as various domestic government agencies such as the National Infrastructure Advisory Council and the Joint Interagency Cyber Task Force.[10] Using these key stakeholders, the review identifies several major problems facing the United States in its approach to cyber and information security, including the lack of organization in the federal government to address the growing threat, the difficulties presented by maintaining security on a network owned by the private sector, and risks to security from non-state actors who could one day cause critical damage to the U.S. infrastructure and government by compromising or stealing information.[11] Among the evidence of these problems cited by the review is the lack of a coordinated response by government agencies to the Conficker worm, which was activated on 1 April 2009,[12] along with a continuing game of catch-up against exploitations leading to data theft resulting in USD 1 trillion lost as well as reports by the CIA of malicious activity.

The core proposals for the near term include increased coordination through a new central policy official who would be responsible for the nation's cybersecurity, the preparation of a response plan, improving collaboration between agencies and with other governments, and a continued campaign to inform the public about the

---

9 The White House, "Cyberspace Policy Review," May 2009. See also Melissa Hathaway, "Securing Our Digital Future," *The White House Blog* (29 May 2009); available at http://www.whitehouse.gov/CyberReview/.

10 The White House, "Cyberspace Policy Review."

11 Ibid.

12 Ibid.

issue.[13] Recently, this last recommendation was bolstered by the release of President Obama's new budget, which entailed a large increase in cybersecurity research and development.[14] In the medium term, the review proposes creating mechanisms to generate strategic warnings, further analyzing threat scenarios, and creating a network that will act during a crisis. Medium-term goals also focus on increased communication to solve interagency disputes, and using the Office of Management and Budget's framework to ensure that budgets are used for cybersecurity goals.[15] The report also emphasized some other key factors: improving the partnership between the private sector and the government through information sharing; partnering effectively with the international community through new agreements to enhance identification, tracking, and prioritization; building more resilient systems that will enhance the survivability of communications during a national crisis; and maintaining national security through a coordinated plan. The Cyberspace Policy Review clearly establishes cybersecurity as a top priority for the agencies of the U.S government.

In 2011, the Center for Strategic and International Studies reviewed the progress on the Cyberspace Policy Review in a report on called "Cybersecurity Two Years Later."[16] The report claimed that, although progress has been made in most areas, in no area has the progress been sufficient. Furthermore, the report described the debate on cybersecurity solutions as being stuck on old ideas of public–private partnerships, information sharing, and self-regulation that have fallen short for decades, and stressed the need for new concepts and strategies. The fear that only a cyber "9/11" would lead to any progress was made even greater by the prospect that waiting for such an event to take place would likely lead to suboptimal and possibly draconian policy solutions.

Among the report's revised observations are two that are particularly relevant to our analysis of opportunities for bilateral steps that can be taken by the U.S. and Russia. The first is a call for the development of a U.S. vision for the future of the global Internet that engages other nations, and acknowledges a shift away from the original U.S.-centric idea of governance by a private global community, as nations seek to extend their sovereign rights to cyberspace. This engagement could lead to an increase in the number of indictments, convictions, and extraditions related to cybercrime. The second is recognition that the cybersecurity community can now

---

13 Ibid., 37.

14 Patrick Thibodeau, "Obama Seeks Big Boost in Cybersecurity Spending," *Computerworld* (15 February 2011); available at http://www.computerworld.com/s/article/9209461/Obama_seeks_big_boost_in_cybersecurity_spending?taxonomyId=70.

15 The White House, "Cyberspace Policy Review," 38.

16 CSIS Commission on Cybersecurity for the 44th President, "Cybersecurity Two Years Later," January 2011; available at http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

identify practices that reduce risk, teach these practices to personnel, and measure their results. These observations provide support for the recommendations offered later in this article.

The U.S. military has also identified key issues in the cyber debate and has offered its own set of recommendations. Three important sources relevant to the military's stance on cybersecurity are: definitions of information operations concepts; recent comments from the commander of U.S. Cyber Command, General Keith Alexander; and Deputy Secretary of Defense William Lynn's recent article "Defending a New Domain."

First, the U.S. armed forces are expected to release the new U.S. Information Operations Concepts, in which they will offer a clear definition of "information war." It appears that the document will define "information war" as strictly information operations limited to offensive and defensive activities.[17] In addition, information superiority is the main goal of information operations, as it will allow commanders to seize, retain, and exploit the initiative.

William Lynn discusses additional background issues, concerns, and recommendations. Lynn begins by emphasizing the importance of cybersecurity in light of the most significant breach of U.S. military computers to date, in 2008, when classified military networks were compromised.[18] Lynn notes that the size and depth of the United States' digital infrastructure still gives it a critical advantage over any adversary. Although the U.S. offense is dominant, Lynn argues that this means that its defense needs to be dynamic, including ordinary inspections all the way to a third level of security using highly specialized active defensive tactics.[19] Lynn additionally recommends that the government increase the number of personnel dedicated to U.S. cybersecurity issues, and improve tactics to acquire the latest information technology. Lynn also focuses on the critical role of allies, and the necessity of shared warning systems and stronger agreements to facilitate the sharing of information and technology. Throughout Lynn's article he emphasizes the widespread impact that a cyber attack would cause, and ways to make the U.S. more secure, but his ultimate goal is to make cyberspace safe.[20]

General Alexander has defined some of the current problems with cybersecurity as the difficulty of centralizing command, the complexity of cyberspace systems, the growing threats that could seriously damage our ability to operate as a country, and the ability to work with other agencies to combat cyber terrorism.[21] As solutions to

---

17 T. Thomas, *Comparing U.S., Russian and Chinese Information Operations Concepts* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004).

18 Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

19 Ibid.

20 Ibid.

21 General Keith Alexander, Interview with Center for Strategic and International Studies, 3 June 2010.

these and other problems, General Alexander highlights the consolidation of command over cybersecurity in the creation of the U.S. Cyber Command. Cyber Command leads day-to-day protection efforts, distributes its cyber resources across the military, and works with many partners inside and outside of the U.S.[22] In addition, General Alexander suggests that we need to understand our own networks from the perspective of real-time operations, and to ensure freedom of movement in cyberspace. General Alexander goes on to say that part of the solution may require establishing clear rules of engagement.[23] Similar to Lynn's goal of making cyberspace safe, General Alexander defines the goal of cybersecurity as minimizing the effect of cyber attacks on U.S. persons and not infringing on civil liberties while protecting national security—similar to the balancing act described by the executive branch review.

When questioned about Russian proposals for a cyber treaty, General Alexander responded that such issues should be handled by policy leaders, not generals, and that the Russian proposal may serve as a starting point, but that the U.S. should develop a counter-proposal. Taken together, Lynn and Alexander offer a complete view of the U.S. military's perspective, emphasizing the security threat of cyber attacks and their potential widespread impact on the population. Both also offer tangible policy recommendations to increase cybersecurity and enhance cooperation at the domestic and international level. The U.S. executive branch and the military both have substantive ideas about how to make cyberspace safer. Initiatives like strategic warning, and better definitions for concepts in cyberspace and information operations, could be enhanced through international cooperation.

Russian Information Security[24]

Just like the United States, Russia is a "titan" of information security. Currently there are many perspectives on cybersecurity at play around the world, but Russia is primarily focused on the military aspects of the issue. Russian cybersecurity expert

---

22 Ibid. See also William Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

23 Ibid.

24 For further background on the Russian approach to information security, see Vladimir P. Sherstyuk, ed., *Scientific and Methodological Problems of Information Security* (Moscow: Information Security Institute of Moscow State University, 2004); Machulskaya I. A. Penjkov, "Information Security of the Russian Federation," The Council of the Federation of the Federal Assembly of the Russian Federation, Moscow, 2005; Doctrine on the Information Security of the Russian Federation," signed by President Vladimir Putin on 9 September 2000 (No. Pr-1985); Marko Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva: International Telecommunication Union (ITU), 2009); and Dylevski S. Korotkov and S. Komov, *Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law* (Geneva: United Nations Institute for Disarmament Research, 2007).

S. P. Rastorguyev defined "information war" as a battle between states involving the use exclusively of information weapons in the sphere of information models. The final objective of an information weapon's effect is the knowledge of a specific information system and the purposeful use of that knowledge to distort the model of the adversary's world. Rastorguyev emphasizes that there are two key aspects to any information war—information-technical and information-psychological—which makes it more dangerous than any conventional war.

Information war poses a new type of threat, and one that Russia is trying with difficulty to confront. In 2005, the Federal Council of the Russian Federation released a political analysis of cybersecurity in Russia, in which it acknowledged that Russia was not ready for the transition to an information society. Russia's critical infrastructure was threatened due to key vulnerabilities in cybersecurity, stemming from Russia's inability to keep up with the fast pace of information technology development at the time. The Russian Federation recognized several kinds of threats to the cyber sphere. The first threat is information weapons, which can influence the technical infrastructure of the society, and can also influence people psychologically. The second threat is that of financial crime, which involves the use of modern computer technologies. The third threat is that of electronic control, whereby one tracks the daily activities of individual citizens. And the final threat of information weapons is the potential political applications they possess to introduce informational totalitarianism, expansionism, and colonialism. Thanks to the latest technology, information technology's influence on the enemy has evolved from individual information sabotage and acts of disinformation to a way of exercising international policy that is both massive in its implications and pervasive in its application. Among its recommendations, the Federal Council stressed the need for even more global cooperation, and made specific recommendations for Russia, including improving legislation on cyber and information security, developing a state system of protecting information as well as classified information, and applying new Russian scientific technologies in the cyber sphere.

The fundamental document that defines the Russian government's position on the issues of information security and the threats posed by it is the Doctrine on the Information Security of the Russian Federation, signed by then-President Vladimir Putin in 2000. It explains the government's official views on the goals, tasks, principles, and main directions of ensuring the information security of the Russian Federation. This document provides the basis for shaping state policy regarding ensuring the information security of the Russian Federation; preparation of propositions on improving the legal, methodological, scientific-technical, and organizational support for Russia's information security efforts; and the development of target-specific programs for enhancing the Russian Federation's information security.

As defined by the Doctrine, Russia's main concerns deal with the military application of cyber technologies. The contemporary level of information technology may enable the commission of new kinds of terrorist acts. Cyberterrorism has been identified by the Russian government as another grave threat to international peace. Terrorist acts in cyberspace have several goals today, including destroying infrastructures at the national and transnational level, as well as accessing unauthorized information. To prevent all types of threats at the operational level, it is crucial to maintain the physical security (including physical access control) of key elements of network infrastructure and software, and on a technical level to have logging and active audit systems to detect abnormal situations that can destructively impact functionality. Early detection, as well as prompt and adequate responses to these situations, is also essential to providing a higher level of security.

In order to provide better security and counter the threats discussed above, Russian officials have always favored the idea of international cooperation. The Shanghai Cooperation Organization—founded by Russia, China, Kazakhstan, Kyrgyzstan, and Uzbekistan—aims at maintaining peace, stability, and greater security in the organization's member states in general, and in Central Asia more particularly. This stability includes strengthening trust between the members, opposing threats to international information security (IIS) by improving existing and building new counter measures, improving mechanisms for joint actions between the SCO member states, and opposing information terrorism. It is important to note that SCO states should align their military policies so as not to proliferate information weapons and technologies. This is a statement promoted by Russia. Russia believes that the most effective way to achieve this goal internationally would be a collective statement of the member states of the United Nations of their adherence to the principle of nonproliferation of information weapons.

Russia's commitment to international cooperation also includes joint work with law enforcement groups within the so-called 24/7 Network, consisting of forty-eight participating countries.[25] The idea of the 24/7 Network is based on the existing network for twenty-four-hour contacts for international high-tech crime from the G8 Nations. With the creation of the 24/7 network, law enforcement authorities of the participating states cooperate with law enforcement authorities of other countries in order to detect, prevent, combat, and disclose cross-border crime in the information sphere; exchange operational and other relevant information of interest; execute requests for assistance in preventing, combating, and solving crimes; and organize and conduct search operations on the Internet to identify, prevent, and document cross-border crime.

---

[25] Albert Rees, "24/7 High Tech Crime Network," Department of Justice Computer Crime and Intellectual Property Section (April 2007): available at http://www.oas.org/juridico/english/cyb20_network_en.pdf.

Russia's definition of "information security" is much broader than the United States' rubric of "cybersecurity," but this allows Russia to incorporate much broader security goals, extending from individual psychology to critical infrastructure. Russia is highly concerned with the threats posed by information security. Thus, its primary goals are focused on international efforts that limit military capabilities while protecting critical infrastructure and other key components of the nation threatened by cyber attacks.

International Cyber and Information Security Activity

Computer crime and warfare do not simply affect the cyber sphere, but can extend to elements of critical infrastructure, including power grids, hospitals, financial institutions, telecommunication systems, oil and gas pipelines and refineries, and numerous other areas not usually identified with cyberspace. It is critical to demonstrate the wide scope that cyber attacks can have when examining the threat of cyberwar. The most well-known cyber weapon of recent times is Stuxnet. This computer worm, which was uncovered in 2010, is reportedly the first malware to include a program logic controller rootkit.[26] Stuxnet was allegedly used to target the Iranian nuclear program, as it infected personal computers of the staff at Iran's first nuclear power station. It was then capable of seizing control of the plant and ultimately destroying it. Some Western experts say its complexity suggests it could only have been created by a "nation state," being beyond the capacity of an individual hacker.[27] A computer worm can easily spread and infect even highly secured objects, and its damage and lasting effects can be irrevocable.

The example of Stuxnet demonstrates how widespread the effects cyberwar can be, and thus cyber warfare, just like any other arena of war, does not take place solely bilaterally, but rather predominantly in an international sphere. Although both the United States and Russia each have their own prerogatives and goals when it comes to cyber and information security, the rest of the international community is also involved in the effort, and has grappled with the same problems that the two individual states have been confronting. However, international law has struggled to keep pace with the impact of the emerging technologies of the information revolution on international security. In what might be called the first phase of the international debate on these issues, a significant discussion took place on how existing international law regarding the use of force and armed conflict should be applied to new cyber-enabled scenarios.

---

[26] Liam O'Murchu, "Last Minute Paper: An In-depth Look into Stuxnet," *Virus Bulletin* (2010); available at http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml.

[27] "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," *BBC Online* (26 September 2010); available at http://www.bbc.co.uk/news/world-middle-east-11414483.

In the second phase of the debate, those carrying out mischievous cyber actions were often criminals, and the international community began grappling with the problem of cybercrime. In the third and current phase, the unsolved cybercrime problem has been compounded by a greater military focus on attack and defense in what has been recently labeled as a new domain of warfare comparable to land, sea, air, or space. In each phase, problems that went unaddressed have become almost inextricably tangled with each other, further complicating the international community's response.

Phase I: International Law[28]

In the first phase of applying current international law to the area of cybersecurity, three critical problems emerge: ambiguity, anonymity, and espionage. Defining what constitutes a threat or use of force in cyberspace depends on the facts, cases, context, relevant law, and circumstances. One must understand the law of conflict management and the contemporary norms of the UN Charter that regulate the use of force during peacetime, including necessity, proportionality, unnecessary collateral damage, and anticipatory self-defense. Short of a declaration of war or an occupation, there is no international armed conflict until a given use of force of a specific scope, duration, and intensity reaches the level of armed attack as defined under Article 51 of the UN Charter.

International law clearly permits self-defense in response to cyberspace attack under certain circumstances. Anticipatory self-defense is permissible when the necessity of self-defense is instant, overwhelming, leaves no choice of means, and no moment for deliberation. States have an obligation to refrain from a threat or the use of force against the territorial integrity or political independence of another state. But states never lose the right to necessary and proportional self-defense. Nevertheless, the right to self-defense may not justify an armed response. Any response must be necessary and proportional, and it requires a determination of the potential threat posed by the penetration of specific computer systems to the national interests of the state. Any computer network attack that intentionally causes any destructive effect within a sovereign state is an unlawful use of force under Article 2(4) to the extent that it may produce the effects of an armed attack, and thus prompt the right of self-defense.

If the identity of the attacker is known, a victim may respond in a manner that is both necessary and proportional, in kind in cyberspace or with more traditional use of force. The difficulty remains to determine identity. Anonymity undermines both deterrence and the ability for self-defense. The real challenge may not be whether international law will permit the use of force in self-defense, but whether technology will enable a state to respond by identifying an intruder or attacker.

---

[28] Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research Corporation, 1999).

Espionage, including non-consensual penetration of computer systems, is recognized as an essential part of self-defense, whose lawfulness during armed conflict is recognized by the 1907 Hague Convention IV regarding the laws and customs of war, and in peacetime by the 1961 Vienna Convention on Diplomatic Relations. It may demonstrate hostile intent on the part of an intruding state, and it may invoke the victim state's right to anticipatory self-defense, but state practice has recognized a right to clandestine intelligence collection as part of foreign relations policy. It is only unlawful under the domestic law of most states. Elements of cyberspace infrastructure, such as telecommunications systems, computers, and satellites, have been used in intelligence collection since their invention under the tactical concept of information operations. However, the same tools that are used for espionage can also enable pre-attack exploration, or an actual attack. Hostile and potentially destructive acts are only one keystroke away, and may materialize into unlawful use of force at the speed of light. But, short of an actual destructive attack, it is difficult to be sure of intent. A legal regime that fails to recognize the ability of a state to defend itself before it has been attacked is unacceptable, and the difficult problem of attribution of responsibility for an attack remains.

Phase II: Convention on Cybercrime[29]

The Council of Europe's Convention on Cybercrime is the most substantive, and broadly subscribed, multilateral agreement in existence today that focuses on issues related to cybercrime. Its most relevant properties with regard to the U.S. and Russia are its heavy Western influence, and a controversial provision for unilateral trans-border access by law enforcement agencies to computers or data with the consent of the computer or data owner.

The U.S. actively participated in the negotiations in both the drafting and plenary sessions, and both the U.S. Department of Justice and the U.S. Senate took the position that the Convention required no implementing legislation in the United States. Though the CoE includes forty-seven member states, including all twenty-seven members of the European Union as well as Russia, China is not a part of the CoE, and Russia has frequently repudiated the Convention. Given that these two countries have been widely identified as the source of some of the most serious cyberattacks in recent years, and that some of these attacks are suspected to be state sponsored (or, at least, state tolerated), their absence from the treaty is all the more troubling. Com-

[29] Michael Vatis, *The Council of Europe Convention on Cybercrime*, Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options (Washington, D.C.: National Academies Press, 2010); available at http://sites.nationalacademies.org/CSTB/CSTB_059441.

pounding the lack of participation from these two key players is the fact that there is not a single nation from Asia, Africa, or South America that has ratified the treaty.

Russia has not signed the Convention, let alone ratified it, largely due to the controversial remote search provision, which is seen by Russia as an unacceptable violation of national sovereignty. The UN has also expressed concern about the reluctance of non-CoE states to accede to a treaty that they had no hand in developing. The International Telecommunication Union (ITU), the UN agency responsible for information and communication technology issues, has advocated for its ITU Toolkit, created with global participation, as a model for legislation for countries to adopt, allowing them to harmonize national legislation without a requirement to join an international treaty. Despite these criticisms, the CoE has pushed back, arguing that what is needed is to get more countries to accede to the Convention, not to reinvent the wheel. The convention has received strong support from the Asia-Pacific Economic Cooperation, the European Union, Interpol, the Organization of American States, and the private sector.

The goal of the Convention is to protect society from cybercrime by providing for the criminalization of such conduct, the adoption of powers sufficient for effectively combating such criminal offenses, the facilitation of their detection, and ultimately their investigation and prosecution. These objectives are accomplished primarily through arrangements for fast and reliable international cooperation.

The Convention requires signatories to establish certain offenses as criminal under their domestic law, when they are committed intentionally. These offenses include but are not limited to: obtaining access to or seriously hindering the functioning of a computer system without right; interception of communications without right; input, damaging, deletion, deterioration, alteration or suppression of computer data without right; and the willful infringement of copyright and related rights.

Two of the most important provisions designed to facilitate investigation address the preservation of data and the establishment of jurisdiction. The Convention seeks to enable a signatory's competent authorities to order or similarly obtain the expeditious preservation of specified computer data from another signatory. Signatories must also establish jurisdiction over any of the substantive offenses set forth in the Convention that are committed in their territory. However, the term "committed in the state's territory" is not defined. The examples neither explicitly include nor exclude the most critical case for international cooperation, that where the computer system attacked is outside the state's territory but the attacker is within it. Other forms of mutual assistance addressed by the convention include extradition, real-time collection of traffic data and recording of content data, wiretapping, the ability to spontaneously forward information to another party, and the designation of a point of contact available on a twenty-four-hour, seven-day-a-week basis to facilitate the necessary assistance.

The most controversial aspect of the Convention is the ability granted to states to access or receive through a computer system in its territory stored computer data located

in another state if the lawful and voluntary consent of the person who has the lawful authority to disclose the data is obtained, without the authorization of any other concerned state. During the negotiations of the Convention the controversy was settled by limiting unilateral actions to two types all could agree on, the other being open source data.

The Convention does not address the particular concerns that may be raised by cyberattacks that are not just criminal acts, but may also constitute espionage or the use of force under the laws of war. This gap is created by the caveat that offenses are committed "without right," where the protection of national security is included. The negotiators of the Convention were primarily representatives of ministries of justice and foreign affairs ministries and law enforcement agencies; there was relatively little representation from any branches of the military. Therefore, the Convention does not deal with the issues that might arise when a nation is under cyber attack and cannot afford to wait for another state's cooperation.

Phase III: Russian Proposals for a Cyber Treaty at the UN[30]

As an alternative to the Convention on Cybercrime, Russia has focused on promoting a proposal in the UN to restrict what nation-states can do with cyber weapons. On 23 September 1998, the Russian Minister of Foreign Affairs Igor Ivanov wrote a letter to the UN Secretary-General calling for measures to be taken immediately to prevent a new area of international confrontation from emerging as a result of the information revolution. The letter identified the threat as emanating from information weapons, and described the resulting conflict as information warfare, which was defined as actions taken by one country to damage the information resources and systems of another while protecting its own. Furthermore, the letter suggested that the destructive effects of such information weapons were comparable to weapons of mass destruction.

The letter also included a draft resolution identifying the following three concerns:

---

[30] For more on Russia's proposals to the UN for a treaty dealing with cyber and information security, see UN General Assembly A/C.1/53/3 (30 September 1998), available at http://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/284/58/pdf/N9828458.pdf?OpenElement; UN General Assembly 53/70 (4 January 1999), available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement; UN A/54/213 (10 August 1999), available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/235/97/PDF/N9923597.pdf?OpenElement; UN General Assembly 54/49 (23 December 1999), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement; and UN General Assembly A/55/140 (10 July 2000), available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/535/02/PDF/N0053502.pdf?OpenElement.

- The technology of the information revolution may potentially be used for purposes incompatible with the objectives of ensuring international security and stability and the observance of the principles of non-use of force, non-interference in internal affairs, and respect for human rights and freedoms
- In addition to military applications comparable to WMD levels of destruction, these technologies might be used to improve existing weapons or create new ones
- Beyond military use, such technologies might also be exploited by criminals and terrorists.

The draft also proposes to begin work on defining concepts such as "information weapons" and "information war"; to investigate international legal regimes to prohibit the development, production, or use of information weapons; and the establishment of an international center for monitoring threats to global information security.

On 10 August 1999, responses from Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, the Russian Federation, Saudi Arabia, the U.K., and the U.S. were reported in UN document A/54/213. The Russian response expanded on the initial proposal, adding emphasis to concerns over the military use of information weapons. The response stated that, as a result of the information revolution, the global and regional balance of power could be altered, giving rise to tension between traditional and emerging centers of power and influence. The cyber arms race that could ensue would threaten both individual states and collective security. Furthermore, the universality, efficiency, economy, secrecy, and impersonality of information weapons make them an extremely dangerous means of exerting influence. The Russian response explicitly stated that contemporary international law has virtually no means of regulating the development and applications of such threats. For these reasons, international legal regulation of civilian and military information technology is required to meet the needs of international security and to reduce the threat of the use of information technology for terrorist, criminal, or military purposes. This could be achieved by developing a code of conduct for states that could evolve from a multilateral declaration to an international legal instrument.

The U.S. response in A/54/213 was structured in five parts: general appreciation of the issues; international security aspects; economic, trade, and technical factors; law enforcement and anti-terrorist cooperation; and the advisability of developing international principles. With regards to international security and information security, the U.S. response cited the long history of national use of radio frequency jamming and electromagnetic counter-measures, and the likely future military use of technology to protect its own data links, as well as several other legitimate uses. In reference to economic, trade, and technical factors, the U.S. highlighted the importance of the need to protect scientific research and intellectual property, and of regulations that promote compatibility and safety in electronic systems.

The bulk of the U.S. response was a discussion of law enforcement and anti-terrorist cooperation. The U.S. pointed out the increased global vulnerability to criminals or terrorists as a result of the information revolution, and the fact that all states were both vulnerable and would remain increasingly so. It therefore focused on the criminal misuse of information technology. The United States' response called attention to domestic efforts to protect its own critical infrastructure, recognizing that these efforts depend in some part on the security of systems beyond its borders. Because of this dependence, the U.S. expressed the hope to place the focus on getting other states to take the necessary steps to secure their domestic information systems and to prosecute those who attempt to disrupt such systems to the fullest extent of the law. The U.S. cited its own long history of amending computer-related statutes to improve them in order to meet new problems.

Given these complexities, the U.S. response expressed the belief that it would be premature to formulate overarching principles pertaining to all aspects of information security. However, the U.S. recognized the importance of international cooperation to combat information terrorism and criminality, and cited the work being done by the CoE, the Group of Eight High-Tech Crime Group, the Organization of American States, and the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders. The U.S. response advised that it would be unwise for the General Assembly to formulate strategies that would interfere with work already under way.

Recommendations

Several goals for the U.S., Russia, and the international community have been defined above, as have preexisting conditions within each arena that would prohibit or accelerate existing policy recommendations related to cyber and information security. The pressure to develop offensive and defensive capabilities in the cyber realm is spreading, and 120 countries around the world are working on or have already developed information weapons.[31] In addition, the issue of attribution of responsibility for cyber attacks is exceedingly difficult. One of the biggest obstacles to greater cooperation between the U.S. and Russia in addressing these problems is the United States' emphasis on law enforcement, and Russia's concern with arms control. Despite important differences in their perspectives on many core issues related to cyber and information security, both nations have emphasized the importance of working with the international community. Immediate bilateral cooperation between Russia and the U.S. could provide a foundation for further international cooperation including involvement with other key stakeholders in the cyber arena, most importantly China. Action can and should be taken in the fol-

[31] Vladimir Sherstyuk, *Scientific and Methodological Problems of Information Security*, 87.

lowing three general areas: reducing vulnerabilities that lead to cyber attacks; expanding domestic initiatives for cyber and information security, where possible, to bilateral participation; and creating paths for increased levels of cooperation through ongoing engagement on cyber and information security which could someday lead to the level of engagement and trust necessary for a comprehensive bilateral or multilateral treaty.

Reducing Vulnerabilities

Though the attack vectors in cyberspace seem to be limitless, the vulnerabilities on which they depend are much more finite.[32] This key asymmetry makes computer network exploitation (CNE) depend on the existence of such vulnerabilities, regardless of who originates the attack, for what purpose, or where they are located. An effort to eliminate as many of these vulnerabilities as possible might make the development of military weapons that exploit them more difficult, but it may not be as controversial as a limitation on the military's option to do so. Raising the bar of CNE to the point where it would only be an option for military organizations might simultaneously reduce the total number of incidents of CNE, and make the problem of attribution slightly less daunting.

Furthermore, CNE-enabling vulnerabilities in particular pieces of software or hardware are not the only vulnerabilities that can be targeted. Resilient system design, especially of critical infrastructure, and systems of systems, can help to mitigate the damage caused by individual component failures, or corruption at various stages in complex processes. By reducing the impact of such failures, the original incentive to attack these targets can be reduced, thereby increasing safety and security.[33] Again, contributing to such design improvements may make it more difficult for a military cyber weapon to take out a power grid, but doing so may be more feasible and acceptable than outright prohibitions on such actions.

Recommendation 1. The United States and Russia should jointly sponsor a bilateral research center for resilient system design and vulnerability mitigation by nominating one lead academic institution in each country and funding several yearly activities to be conducted by these organizations. Such yearly activities would include conferences to discuss joint research on resilient design, "bounty hunter" contests that reward researchers who discover existing vulnerabilities in widely used commercial and open source software and hardware, and possible joint research exercises in network security and forensics. All scholarship produced by this research center would be shared, contributing to the safety and security of both countries, as well as increasing engagement and trust in cyber and information security.

---

[32] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

[33] Devabhaktuni Srikrishna, "Cyberwarfare: Surviving an Attack," *Public Interest Report* 63:3 (Fall 2010); available at http://www.fas.org/pubs/_docs/PIR_Fall_2010.pdf.

Expanding Domestic Initiatives to Bilateral Participation

The United States' Cyberspace Policy Review identified many domestic initiatives to secure cyberspace and harness the full power of the information revolution. Not all of these initiatives would be suitable for extension to bilateral participation. Nevertheless, any alternatives that could be identified as such would represent actions that have been deemed important to effectively coordinating a U.S. response across a complex and, in some ways, competing set of stakeholders. If such mechanisms enable a more effective national response to incidents of cyber attack, it would be reasonable to expect that some of them might also enable a more effective international response, provided that the issues of sovereignty, control, and unified purpose could be adequately balanced.

Several promising examples of alternatives that might fit include: developing mechanisms to obtain strategic warnings, maintain situational awareness, and inform incident response capabilities; developing a set of threat scenarios and metrics; developing mechanisms for cybersecurity-related information sharing; and expanding sharing of information about network incidents and vulnerabilities with key allies.

Recommendation 2. The U.S. and Russia should search for domestic cyber and information security initiatives currently underway that are potentially suitable for extension to bilateral participation. Any collaboration on such substantive matters—even if narrowed in scope, or spun off from a domestic initiative—would require a great deal of trust, but could also be tremendously important. It could be critically important, for example, to create a common vocabulary and efficient mechanisms that enable the U.S. and Russia to exchange incident-related information in circumstances where both states wish to do so, and to clear (or at least identify) any bureaucratic hurdles that might exist in times of crisis that might hinder the use of such mechanisms. Existing channels of communication for such communication may not be sufficient to mitigate the risks associated with crises that occur at Internet speed.

Recommendation 3. We recommend a shared warning system stemming from a domestic initiative turned bilateral. The U.S. has already promoted the idea of shared warning in Australia and the U.K.[34] However, it is critical that this shared warning system be extended to Russia, if not started bilaterally between Russia and the U.S. A shared warning system would consist of an agreement that if either side experienced a cyber attack or discovered information about an upcoming attack on itself or the other nation it would warn the other nation so that they may learn and adapt. It

[34] Transcript of speech by U.S. Deputy Secretary of Defense William Lynn, III, "Defense Department Outlines New Infosec Approach," *Gov Info Security* (26 May 2010); available at http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1.

would require direct communication between the organizations in the U.S. and Russia responsible for cybersecurity, such as the U.S. Cyber Command, and the relevant stakeholders in Russia. As Lynn stated, "Collective cyber defenses are similar to air and missile defense in that the more attack signatures that you see, the better your defenses will be."[35] The warning system would not only serve to warn the other nation about possible attacks from nation-states, but also attacks from non-state actors, which represent one of the biggest cyber threats today. It is crucial that Russia and the U.S. work together to warn one another of upcoming threats and current attacks in order to build better defense systems and a more secure world, both in cyberspace and on the ground.

Creating a Path for Increased Cooperation

Returning to the core problem of the United States' orientation towards a law enforcement approach, as opposed to the arms control approach advocated by Russia, it has been noted that these goals are by no means mutually exclusive. Therefore, despite any current differences in opinion, the two approaches could in theory coexist to the benefit of all parties. Nevertheless, the road between where we are today and this ideal outcome still seems quite long.

Several incremental steps on this path could go a long way towards creating an environment where both parties could work together towards addressing each other's concerns and building a sufficient level of trust to proceed further. One such step would be to evaluate all the ideas put forward unilaterally by each side as actions for international cooperation, and from these actions to identify and advance actions that would be most attractive to the other party.

Recommendation 4. In order to go forward with bilateral negotiations, both sides need to come together to define what cybersecurity and information security are. We recommend establishing a collaborative definition database. One of the primary issues with cybersecurity today, as discussed above, is the lack of agreement about definitions, which inhibits both law makers and military actors. In order to overcome the divide on definitions, we recommend that a research center be established where academics and policy makers from both the United States and Russia would collaborate and define the critical issues of cybersecurity. The definitions will cover a wide range of issues, but will focus on what is cybersecurity or information security, what is cyber warfare, what is a cyber weapon, and what constitutes a cyber attack. Once the center establishes what it believes is a set of definitions that both countries could accept, it would submit these definitions to the respective nations' executive bodies.

[35] Ibid.

If the presidents approve of the negotiated definitions, the definitions would then be submitted to the United Nations General Assembly for global approval because—although we believe bilateral negotiation is a strong starting point—cybersecurity must be tackled at the international level. It is essential to define what cybersecurity and other related issues mean and what constitutes an attack so that law makers and policy makers can work more effectively in the complex realm of cyberspace. Since cyberspace is constantly changing, we imagine that this definition process will be ongoing, with a new set of definitions submitted to the UN once every year. In the long term, this process of defining the world of information technology and security would be a springboard to eventually defining the rules of engagement, so that militaries can know how to strategize and act.

Recommendation 5. The United States should find a way to engage Russia in as many of the law enforcement mechanisms from the CoE Convention on Cybercrime as Russia is willing to try without requiring formal ratification of the Convention. Similarly, Russia should find a way to engage the U.S. in as many of the activities of the Shanghai Cooperation Organization on information security without requiring any formal participation. These arrangements, if found, might be optimal places to explore the other party's reactions to any unilateral suggestions for international cooperation. Though these arrangements will face many challenges—such as Iran being an observer of the SCO, and Russia already being a member of the CoE—similarly challenging situations have been successfully circumvented in other arenas with some degree of success. The NATO-Russia council, for example, has kept valuable lines of communication open to the benefit of both parties, and has allowed for progress that otherwise might not have been possible. The chances for the successful resolution of the stalemate over cyber and information security will be greatly increased if the parties are given substantive opportunities to work through their issues together in the most meaningful forums.

Conclusion

As progress within the cybersphere increases in speed, more and more issues are being drawn into this new realm. The information technology revolution represents one of the greatest technological advances in human history, with the dual power to push humanity forward, but also with a grave power to harm essential components of life. Both Russia and the United States are recognized world leaders within the cyber sphere, and both countries are using this technology in its dual purposes as an innovator and a weapon. As cyberspace becomes a declared domain of warfare, comparable to land, sea, air, and space, the U.S. and Russia face a crucial test of their ability to work together on important issues of international security. The two nations' diffe-

rent approaches to cyber are information security are not incompatible. Arms control and law enforcement are both critical components of international security in the era of the information revolution. Taking action on the recommendations presented here will help to create an environment where both countries can find an appropriate balance, and set an example for the international community. Though we understand that the sphere of cyber and information security is predominantly the sphere of international collaboration, it is also true that the variety of views and positions on this issue are so varied from country to country that the states are not likely to be able to come to any agreement. Cooperation between the United States and Russia is a good start, and the implementation of these recommendations could be ultimately extended to other nations that express their willingness to participate.

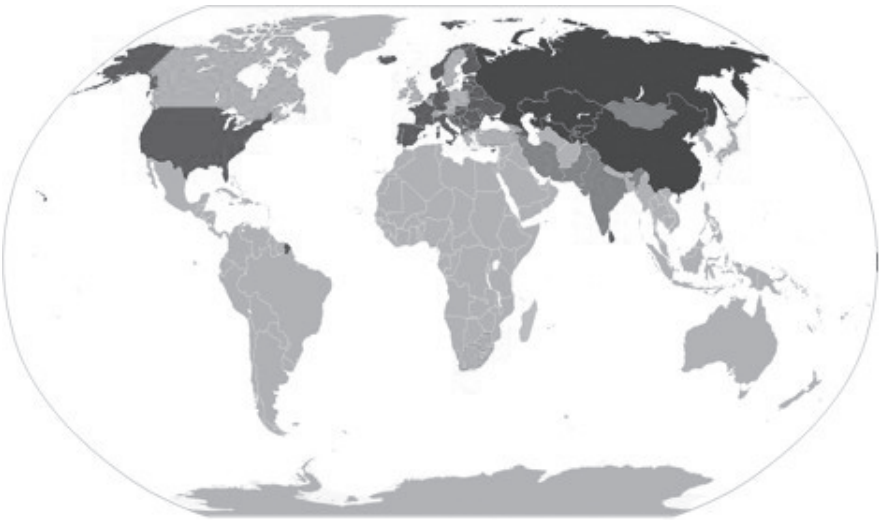

Figure 1: Arms Control and Law Enforcement in the Information Revolution	
	Shanghai Cooperation Organization Member States
	Shanghai Cooperation Organization Dialogue Partners
	Shanghai Cooperation Organization Observer States
	States that have ratified the Council of Europe Convention on Cybercrime
	States that have signed but not ratified the Council of Europe Convention on Cybercrime

Bibliography

Dylevski, Igor, Sergei Komov, and Sergei Korotkov. *Military Aspects of Ensuring International In- formation Security in the Context of Elaborating Universally Acknowledged Principles of International Law*. Geneva: United Nations Institute for Disarmament Research, 2007.

Gercke, Marko. *Understanding Cybercrime: A Guide for Developing Countries* . Geneva: International Telecommunication Union (ITU), 2009.

J, William, and I Lynn. "Defending A New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (2010).

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

Markoff, John. "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia ." *The New York Times* (2010).

Nazario, Jose. "*Politically Motivated Denial of Service Attacks*." In *The Virtual Battlefield: Perspectives on Cyber Warfare*., 2009.

O'Murchu, Liam. "Last Minute Paper: An In-depth Look into Stuxnet." *Virus Bulletin* (2010).

Sharp, Walter Gary. *Cyberspace and the Use of Force* . Falls Church, VA: Aegis Research Corporation, 1999.

Sherstyuk, Vladimir P.. *Scientific and Methodological Problems of Information Security* . Moscow: Information Security Institute of Moscow State University, 2004.

Srikrishna, Devabhaktuni. "Cyberwarfare: Surviving an Attack." *Public Interest Report* 63, no. 3 (2010).

Talbot, David. "Russia's Cybersecurity Plans." *Technology Review* (2010).

Thibodeau, Patrick. "Obama Seeks Big Boost in Cybersecurity Spending." *Computer-world* (2011).

Thomas, T.. *Comparing U.S., Russian and Chinese Information Operations Concepts*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

Vatis, Michael. *The Council of Europe Convention on Cybercrime, Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options*. Washington, D.C.: National Academies Press, 2010.