GOOD HARBOR

SECURITY RISK MANAGEMENT, LLC

Securing Cyberspace Through International Norms

Recommendations for Policymakers and the Private Sector

Richard A. Clarke

Chairman, Good Harbor Security Risk Management, LLC

Authored by Richard A. Clarke with contributions from Jacob Gilden, Jacob Olcott, William Howerton, and Emilian Papadopoulos

About Good Harbor Security Risk Management

Good Harbor works with senior corporate executives, investment professionals, and government leaders to assess and develop strategic cybersecurity programs that mitigate organizational risk in the face of advanced cyber threats. Good Harbor's consulting services include the Executive Cybersecurity Risk Profile and Action Plan as well as specialized services in threat awareness, risk assessment, strategy and governance, crisis management and communications, regulatory and policy analysis, thought leadership, and investment diligence. The firm is led by Chairman Richard A. Clarke, a former, senior White House advisor on cybersecurity, counterterrorism, and national security, and the author of *Cyber War: The Next Threat to National Security and What To Do About It*. To learn more about Good Harbor, visit http://www.goodharbor.net

Table of Contents

1 Introduction

The 21st century has thus far been a period of increasingly sophisticated, serious, and widespread malevolent activity in cyberspace. Cyber crime, cyber espionage, and even cyber war have in recent years become issues of immediate concern to senior government leaders and industry executives, threatening to undermine the great benefits of a globally networked society. Nations have built cyber armies. Cyber criminals have stolen hundreds of billions of dollars worth of personal, business-sensitive, and financial information, largely from the private sector. Those conducting cyber espionage have successfully penetrated both governments and corporations at the highest levels.

Such dangerous and difficult transnational issues require concerted global attention. As a result of these troubling trends, interest has grown among leaders in many countries and companies about the development of international norms concerning cybersecurity. What, however, are international norms, and what could such norms do? Who would be involved and how? Could international norms for cyberspace enhance security? Is norm creation only the province of government or is there a role for the private sector?

This paper seeks to help international policymakers, diplomats, information and communications technology (ICT) companies, and the private sector generally understand the important issues surrounding cybersecurity norms development and their unique roles in creating and implementing these norms. The paper also recommends specific cybersecurity norms that could realistically gain international acceptance in the near term. If accepted and implemented, these key recommendations for norms governing cyber crime and cyber war would likely create a more secure cyberspace in the 21st century.

2 Definitions

Defining the scope of norms and cybersecurity is an appropriate way to introduce the topics for those unfamiliar with either area, but it also serves an important function. Reaching international agreements is much more difficult than might initially be thought, in part because there is much disagreement about the scope of the terms being used. Nations may believe that a subject like cybersecurity is deserving of concerted attention by diplomats and international experts, but that belief does not by itself create a mutually held definition of precisely what the scope of the problem is or exactly what the discussions are intended to do about it. In fact, nations that think something should be done about a subject often have vastly different ideas about what that subject actually is. Thus, definitions in international agreements are not the simple transposition of dictionary texts to diplomatic documents. Definitions in international agreements may, instead, be the mutual delineation of areas where nations believe they can find common ground for action.

When it comes to cybersecurity norms, there are a broad sweep of diverse types of issues and actions in cyberspace, with an equally broad number of definitions of international norms that include everything from, on one extreme, informal understandings created by experts from several countries to, at the other end of the spectrum, multilateral treaties among nation-states, perhaps enforced by international bureaucracies. Among the most important of these are the following terms:

2.1 Norms: Explicit, agreed-upon rules of behavior, procedures, or codes of conduct. They may be established and agreed to by experts, non-governmental organizations, or nation-states.

A LESSON IN DEFINITIONS

The first international negotiation in which I participated met almost forty years ago for the purpose of reducing troops in Europe. That purpose seemed, at first, to adequately define the scope of the project. Yet, it took over a decade for the participating nations to agree upon what “troops” were and what geographic area was covered for purposes of the agreement by the phrase “Europe.” That long process was not just the result of foot dragging. The different definitions of what was included and what was excluded were substantive because they would have created vastly diverse results, creating advantages for some nations over others.

-Richard Clarke

2.2 International Agreements: Documents to which nation-states have confirmed their adherence, committing to do or not to do certain activities domestically and/or internationally. International agreements include mutual declarations, executive agreements, and treaties.

2.3 International Standards: Procedures, definitions, or measures used by non-governmental organizations and/or governments in the conduct of certain agreed-upon activities.

2.4 International Organizations: Multinational institutions created by governments or non-governmental organizations. Some governmental international organizations are simply groups of like-minded nations, which meet together periodically. Some are permanent organizations with seconded staff and mutually funded infrastructure.

2.5 Confidence Building Measures (CBMs): Activities carried out, usually pursuant to an international agreement, to reduce the likelihood of misunderstanding the scope, meaning, intent, or consequences of activities about to be or being conducted. CBMs may involve exchange of information, steps to increase transparency, enhanced communications, the use of observers, and agreement to limit the scope or nature of certain activities.

2.6 Cyberspace: Digital networks and the objects that can be connected to them, including hardware and software engaged in digital data creation, digital data storage, digital data transfer, and digital control systems. Cyberspace includes, but is not limited to, the Internet. Digital data includes, but is not limited to, voice communication, packet-switched messages, and control system commands.

2.7 Cybersecurity: Policies, procedures, regulations, standards, software, and hardware designed to deal with malevolent or unauthorized activity on digital networks and devices. Such unauthorized activity is typically associated with theft, espionage, privacy violations, or actions that alter, disrupt, damage, or destroy data or physical objects.

2.8 Cyberspace-Enabling Information and Communications Technology (ICT): Hardware, software, and physical infrastructure that allows global access to and the smooth functioning of cyberspace. Cyberspace-enabling ICT includes, but is not limited to, domain name servers, cables, switches, routers, public key infrastructure, certificate authorities, data centers, and hardware and software that manages these technologies.

2.9 Cyber Crime: The theft of funds or personally identifiable information (such as credit card numbers, dates of birth) through unauthorized network penetration.

2.10 Cyber Espionage: The collection of protected, non-publicly available information by governments or non-state actors through unauthorized network penetration.

2.11 Cyber War: The use of cyberspace to cause the destruction, damage, or disruption of digital networks or physical objects including weapons and critical infrastructure systems (including systems supporting transportation, electric power, banking and finance, telecommunications, oil and gas, and health care).

3 International Norm Agreements: Characteristics and Substance

Developing international cybersecurity norms can seem challenging and intimidating because of some of the unique characteristics of cyberspace, the broad scope of issues involved, the rapid pace of technological development, the significant number and impact of attacks today, and the incredibly diverse set of interests and backgrounds of the many parties involved. While these present difficult challenges, the history of international norm development suggests that agreements have often been reached on subjects of great difficulty. Those seeking to advance international cybersecurity norms can benefit from examining other norms regimes that have been successfully developed through a variety of models and approaches to manage issues of great complexity ranging from arms control to commerce and technology to transportation.

3.1 Characteristics of Various Norms Regimes

Successful norms regimes have varied in their characteristics immensely and do not suggest a one size fits all or cookie cutter approach to developing cyber norms. Norms regimes have differed on issues like the mechanism establishing them (informal, formal, treaty), the level of institutional support involved, membership (open, closed, bilateral or multilateral, universal or like-minded), the function they perform, and the extent to which private sector and other non-governmental actors have been involved in developing or implementing them.

3.1.1 Legal Status: Norms are established as formal treaties between countries, as executive agreements that have not been ratified as treaties, or as other formal or informal agreements. Norms can be established as "politically binding" and/or legally binding.

3.1.2 Supporting Organization: Norms regimes can involve large institutions with significant resources and authority, small supporting secretariats, or hardly any institution at all.

3.1.3 Membership: Norms regimes vary significantly in their membership: they can be bilateral or multilateral; they can offer open membership or impose conditions or criteria for membership; and, they can be universal or focused as regional regimes or regimes of like-minded nations. In many cases, the scope of norms regimes evolves over time, often beginning with a limited set of like-minded nations and expanding to include new members.

3.1.4 Function and Purpose: Norms regimes exist for a range of purposes, including providing technical assistance, building indigenous capacity, creating or setting standards, verifying compliance with standards, serving as a forum for dispute resolution and development of formal agreements, prescribing specific activities (limiting behaviors, prohibiting behaviors, and requiring behaviors), and putting in place confidence building measures (CBMs).

3.1.5 Domestic Implementation and Impact: Some norms are enshrined through domestic legislation, while others are not. In addition, domestic implementation has sometimes surrendered some level of sovereignty to international inspection, verification, or audit procedures, while in other norms regimes this has not been the case.

3.1.6 Role of the Private Sector and Non-Government Actors: Norms regimes vary widely in the level of involvement of private sector and other non-government actors in consulting on norms, developing norms, and implementing norms.

3.2 Examples of Other International Norms

With the essential characteristics in mind, reviewing a sample of international norms regimes reinforces key points that are instructive for the development of international cybersecurity norms. International norms and norms regimes vary widely, and success can be achieved through a variety of approaches, from bilateral agreements with minimal institutional support focused on confidence building measures to multilateral treaty organizations with robust secretariats and functions ranging from prescriptive rule-making to inspection and verification.

3.2.1 Maritime Transportation: One area that has enjoyed a long history of evolving and effective norms is the behavior of ships at sea. Driven by necessity and the perils of maritime travel, nations established a norm centuries ago that all ships had a "duty to assist" each other in cases of danger or distress. Over time, the norm became enshrined in international law as a bedrock principle in the UN Convention on the Law of the Sea and the activities of the International Maritime Organization (IMO), gaining the support of a multilateral treaty that imposes legal obligations on member countries. Building on a long history of international cooperation at sea, the IMO has helped develop other norms, propagate standards, and provide technical assistance. Private sector companies have played key roles in developing norms for safety and security in the IMO, since it is their ships and container ports that are regulated.

3.2.2 Air Transport: The International Civil Aviation Organization (ICAO) and the norms it promotes in civil air travel are another example of a successful norms regime. ICAO is an open-membership treaty organization supported by member countries and with significant input from private sector actors such as airlines, airport operators, and industry groups. In its own words, ICAO supports stakeholders as they "develop policies and standards, resolve strategic directions on critical issues, coordinate global initiatives, monitoring, analysis and reporting and pursue targeted assistance and capacity build-

ing objectives." ICAO's success is attributable in part to its open membership, the provision of technical expertise, and the member countries' agreement to focus on civil aviation rather than military aviation practices. Keeping ICAO's focus on civilian air travel has allowed more members to join the organization and to reach agreement on important issues in civil aviation without necessitating discussion on politically charged national security issues.

3.2.3 Behavior of Navies: The purpose of the US-Soviet Incidents at Sea Agreement (INCSEA) was to reduce behaviors that could unintentionally create or escalate incidents at sea between the US and USSR. It began as a bilateral rather than multilateral agreement and is an executive, non-treaty agreement. INCSEA relies less on the support of a secretariat or institution and instead uses periodic meetings to uphold and revise a series of prescriptive behaviors. INCSEA's prescriptions include behavioral prescriptions, such as a requirement to notify ships when submarines are exercising nearby, a requirement to notify the other party when planned exercises or maneuvers could pose a danger to nearby air or sea navigation, and a requirement to meet annually to manage implementation of the Agreement. They also include banned behaviors, such as prohibiting interference in the formations of other parties or certain maneuvers that increase the chance of collision.

3.2.4 Risk Reduction and Authorized Communication Channels: The Nuclear Risk Reduction Centers (NRRC) also have their origins in a bilateral, non-treaty agreement to reduce uncertainty and unnecessary or unintentional escalation. The NRRCs, created by an executive agreement between the US and Soviet Union in the late 1980s, enhanced communications and information exchange to minimize the risk of nuclear war between the U.S. and Soviet Union. Over time, the NRRCs have become a valuable mechanism supporting multiple bilateral and multilateral security agreements through communications, information exchange, training, and the coordination of technical support.

> My personal experience with some of these regimes convinces me that private sector involvement is critical to the long-term success of such regimes. I headed the US Nuclear Risk Reduction Center and chaired the multilateral Missile Technology Control Regime, led the US Delegation to the Australia Group, participated in the European troop reduction talks, and helped to shape the Financial Action Task Force and the Biological Weapons Convention. We needed private sector assistance in shaping most of those agreements and in gaining Congressional support for all of them.
>
> -Richard Clarke

3.2.5 International Trade and Customs Taxation: Trade is another area with an instructive history of effective norms regimes. Like the "duty to assist," the norm of one country granting another "Most Favored Nation" (MFN) status has a long history of bilateral and multilateral implementation. In granting MFN status, a state agrees to treat another country as it would its "most favored" trading partner. MFN eventually became enshrined as a foundational element of the General Agreement on Tariffs and Trade (later the World Trade Organization), with all members granting each other MFN status. This condition of membership is strong enough that it has at times slowed the

accession of countries into the WTO. However, the norm of MFN has also been challenged by exceptions granted for trade with developing countries and for certain regional blocs, highlighting how even treaty-based legal norms can be marginalized by changing circumstances and new international structures.

3.2.6 Military Confidence Building: The Treaty on Conventional Armed Forces in Europe (CFE) is a multilateral treaty between NATO and now-former Warsaw Pact countries that imposes significant prescriptions, including specific limits on the numbers and types of armed forces each party may have and requirements around participating in a forum that supports the Treaty, answering technical questions, and resolving disputes. The CFE is notable because, even without a particularly large institutional structure or secretariat, the Treaty imposes significant verification requirements on member states, including allowing on-site inspections.

3.2.7 Missiles and Components Export: The Missile Technology Control Regime (MTCR), focused on preventing the proliferation of "unmanned delivery systems capable of delivering weapons of mass destruction," adopts a different approach to its mission. The MTCR is an informal, voluntary, non-treaty association of countries that coordinate their national export licensing, most notably through shared information exchange and common export control lists and guidelines. Like many successful norms regimes, the MTCR, which has no secretariat and relies minimally on liaison provided by a member country, began as an association of like-minded states (Canada, France, Germany, Italy, Japan, the United States, and the United Kingdom) but has since expanded its membership significantly to 34 countries, including Russia, The Republic of Korea, and Turkey. The MTCR admits new members by consensus and has at times declined countries' applications, but non-member states can choose to adopt the group's export guidelines without formally becoming members, as some have.

The regime is of interest because it causes governments to regulate the activities of private corporations engaged in international activities. The MTCR is also an interesting case study because of its involvement with the International Code of Conduct against Ballistic Missile Proliferation, also known as the Hague Code of Conduct. The Hague Code of Conduct, which also combats proliferation of ballistic missiles and technology, has its origins in a draft text that was initiated by the MTCR partners, but it evolved independently. The Hague Code of Conduct imposes less specific restrictions than the MTCR and has open membership for all countries. It has 134 members, nearly four times as many as the MTCR, thereby successfully broadening the ballistic non-proliferation movement to countries that are not interested in, or have not secured, MTCR membership.

3.2.8 Bio-Chemical Weapons: The Australia Group is another voluntary, informal group focused on export controls and helping countries coordinate their national policies to limit the export of chemical and biological agents and related equipment, technologies, and expertise. The Australia Group's scope and function has expanded over time from an initial focus on chemical weapons proliferation to state actors to encompass biological weapons and the flow of weapons to non-state groups. The Australia Group's membership has also expanded over time, from 15 to 40 countries. Like the MTCR, membership is only granted by consen-

sus. In the case of the Australia Group, this has created tension with some non-participating states that have complained about the reasons or circumstances surrounding their denied applications for membership.

In the past, the Australia Group has sought advice from chemical manufacturers, whose exports the Group's standards regulated. The activities of the Group led to the successful resuscitation of multilateral treaty negotiations to ban the production or storage of any chemical weapon, the Chemical Weapon Convention (CWC). The CWC, and later the Biological Weapons Convention (BWC), both required international inspection of private bio-chemical companies. Companies were active advisors in these negotiations to give their expert advice on manufacturing and to insure that verification measures did not reveal corporate secrets and proprietary data.

3.2.9 Money Laundering: The Financial Action Task Force (FATF) is another successful norms regime that has expanded in scope, membership, and effect over time. Originally designed to combat money laundering, FATF was created by the like-minded Group of 7 (G7) and nine other countries. Its membership has since expanded to over 30 countries, including Russia, Singapore, and China, as well as the Gulf Cooperation Council, the European Commission, and approximately ten associate or observer members. FATF, a non-treaty agreement, is buttressed by a small institution, which supports member countries as they issue recommendations, set standards, and exchange technical expertise. After the September 11, 2001 terrorist attacks, FATF expanded its mandate to combat terrorist financing and issued an additional set of recommendations.

Throughout its work, FATF has been notable for incorporating the input and expertise of the private sector and key financial institutions. FATF is also noteworthy because it both involved the creation of model domestic laws and the potential of sanctions against scofflaw nations and money laundering sanctuaries. The participating nations also agreed to mutual inspection. Each nation undergoes audits by a committee of three other participants. This peer review increases confidence of participating nations in each other's compliance.

3.2.10 International Financial Communications: A final successful norms regime with even greater private sector involvement is the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a member-owned cooperative whose original mission was to create the communications and data processing systems that underlie international financial transactions. SWIFT was created with the support of 239 banks in 15 countries. Its operations and presence expanded successfully, fueled in large part by a transparent and inclusive process that incorporated private sector inputs and expertise. The use of SWIFT for sending interbank messages has largely become ubiquitous and a norm for financial institutions.

4 Existing and Potential Cybersecurity Norms

As malicious behavior in cyberspace rises, nation-states, diplomats, and private sector companies are increasingly considering whether current norms need modification or if new "cybersecurity norms" are necessary. There are at least six different subjects that fall into the bucket of cybersecurity norms, including Internet governance, Internet freedom, online privacy, cyber espionage, cyber crime, and cyber war. While each of these areas would benefit from widely accepted and clearly defined international agreements, seeking a common negotiating process or regime to articulate norms for all six areas is unlikely to be fruitful. Indeed, part of the difficulty to date in achieving progress on norms of international behavior related to cybersecurity has been the jumbling of the six various topics. Instead, it is important to disaggregate and disentangle these issues to allow for the development of international understandings concerning each issue to occur on separate paths at their own pace. Separating the issues may also allow for more rapid progress on some aspects that can be more readily agreed, and this progress may create a diplomatic environment in which progress on others may become easier to achieve.

The following sections define each of these topics, note what activity has taken place in each area, and offer an outlook regarding the feasibility of short-term progress on norms in the area, prescribing several recommendations for norm development where appropriate. It is concluded that in the short term, the international community is more likely to reach agreement on cybersecurity norms related to cyber crime and cyber war, and it should incorporate the private sector into these discussions immediately.

4.1 Internet Governance

As the Internet evolves, so too does the governance of the technical workings of cyberspace. In previous decades, Internet governance structures and issues have been shaped and influenced by the growth in size, international scope, and economic importance of cyberspace. Along the way, nation-states have often disagreed about the role that they should play in the governance of the Internet. This topic is becoming a source of increasing international tension.

During the birth of the modern Internet and the early stages of the development of the World Wide Web, the technical functioning of the Internet was largely controlled by Americans and done with little government influence. In

1986, the Internet Engineering Task Force (IETF) was founded as a venue for developing Internet protocol standards to ensure that the fledgling networks operated smoothly. Participants in the IETF were then and remain researchers, operators, and other vendors, not government officials. Until the early 1990s, the Domain Name System (DNS), which allows the easy lookup of websites, was managed largely by a single man, Jon Postel. In 1998, at the suggestion of the U.S. Department of Commerce, a non-profit organization called the Internet Corporation for Assigned Names and Numbers (ICANN) was created to better manage the DNS with the growth of the Internet. By most accounts, overall state influence in the Internet governance process was minimal and issues of national cybersecurity were peripheral.

By the early 2000s, as international online populations began to rapidly grow, nation-states had begun to lobby for a more substantial role in Internet governance. At the 2003 and 2005 World Summit on the Information Society meetings in Geneva and Tunis, there was heavy criticism, especially for developing nations, that ICANN and the Internet governance process was dominated by the United States. What emerged from WSIS was the preservation of a multi-stakeholder model, which gives a voice to government, industry, and civil society, but also a clarified position for states with regards to Internet public policy. The 2005 Tunis Agenda set out that the multi-stakeholder model would be preserved for the day-to-day management of the Internet but also introduced the norm that public policy issues, such as cybersecurity, were critical to overall Internet management. The Tunis Agenda held that states had the sovereign right to deal with public policy online while creating a non-binding venue for discussions on public policy and technical issues by both states and private stakeholders in the Internet Governance Forum (IGF).

Norms about the role of national governments, which forum should lead in Internet governance, and what issues should be on the table are still not settled. In recent years, there has been a push by some countries, including China, for the government-only International Telecommunications Union (ITU) to play a larger role in Internet governance as well as cybersecurity. Many Group of 77 (G77) developing countries are also suspicious about what is seen as a dominant Western Internet governance system. Western observers worry that the ITU could act as a forum to regulate the basic Internet infrastructure, allowing governments to exert greater control over online content and networks in the name of cybersecurity. The ITU World Conference on International Telecommunications (WCIT) in 2012, which was tasked with reviewing the 1989 International Telecommunications Regulations (ITRs), highlights the deep divisions on Internet governance. While Russia and states in Africa and the Middle East pushed for a greater nation-state role in Internet functions, including direct control over the DNS, the United States, Canada, and allies in Europe, Latin America, and Asia argued that Internet governance issues should not even be on the table in the state-only ITU negotiation of the ITRs.

4.1.1 Outlook for Norms Development on Internet Governance

With the near ubiquity of cyberspace in all facets of life around the world, nation-state interests in controlling the technical functions of the Internet will not fade. States, including both China and Russia, see international and

domestic benefits in having a more direct say in the day-to-day functioning of global networks, especially in helping them exert greater control over the flow of information to their populations. Many developing countries, given their limited resources, have felt largely left out of the multi-stakeholder model and have a difficult time navigating the current fragmented system. A more central ITU role, which would give them greater certainty about venue and more authority, will likely continue to be seen as being in their interests.

The United States, on the other hand, has firmly placed its support behind the status quo and the current multi-stakeholder system. Moving towards a state-based, ITU-dominated Internet governance norm would isolate the United States and other like-minded nations. The ITU system allows each member state a single vote, subjugating strong private actors' voices and empowering non-Western nations. The United States and other Western countries see a clear benefit to an open and innovative Internet, and the best way for that goal to be accomplished is through multi-stakeholder governance and keeping issues of cybersecurity out of forums such as the ITU.

With these two competing positions, Internet governance is unlikely to be an area where strong, global norms are built in the short-term. Both sides, but especially the United States, appear entrenched in their positions and have strong competing interests. The battle between multi-stakeholder governance and ITU and nation-state control is likely to be a protracted and potentially bitter diplomatic fight.

4.2 Internet Freedom

Internet freedom has emerged as an area of international concern based on basic human rights norms protecting the freedom of speech and expression. Article 19 of the 1948 Universal Declaration of Human Rights holds that freedom of expression is protected through any media, which many have said applies in cyberspace. In the United States, cyberspace is generally considered to be a venue where all speech, no matter how objectionable, is allowed just as it would be in any other medium as protected by the First Amendment to the Constitution. There are limited exceptions to this right, including defamation and child pornography. Europe takes a similar view to speech, but unlike the United States, hate and xenophobic speech is banned within much of the continent. The criminalization of hate speech online is also enshrined through international treaty in the 2001 Council of Europe Convention on Cybercrime Additional Protocol. It has been signed and ratified by a number of European countries, but not the United States.

Private sector-driven organizations have helped support human rights norms around Internet freedom. The Global Network Initiative (GNI), a non-profit organization made up of private ICT firms, civil society groups, investors, and universities, has created a set of principles and implementation guidelines for ICT sector companies to follow to ensure that they are supporting Internet freedom. The GNI's principles hold that participating firms must respect freedom of expression when confronted by government requests or laws that would

suppress such liberties, pushing companies to implement Internet freedom norms around the world. Members of the GNI include Google, Microsoft, Yahoo, the Center for Democracy and Technology, and Human Rights Watch.

However, even with private sector actions to support Internet freedom norms, governments still are able to stifle speech. In many authoritarian and semi-authoritarian regimes, respect for freedom online and the ability to operate without censorship is often non-existent, just as the human right protecting freedom of expression in the physical realm is stifled. There have been high-profile cases of governments using their sovereign control over their domestic cyberspace to censor what is seen as speech that could be harmful to their regime or attempting to silence dissident voices online during times of crisis; China, for instance, filters search results and web pages through what has been called the Great Firewall, and several despotic regimes attempted to block Internet access to quell dissent during 2009 post-election protests in Iran and the 2011 Arab Spring demonstrations.

Many authoritarian and semi-authoritarian states view this ability to control the information flowing into their countries as a key component of their national cybersecurity. In a 2011 draft International Code of Conduct for Information Security presented to the United Nations, China, Russia, Tajikistan, and Uzbekistan called on states to agree to curb the "dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment." The United States and other liberal democratic nations would never accept such a norm and view cybersecurity as separate from the speech that is carried out online.

4.2.1 Outlook for Norms Development on Internet Freedom

Because Internet freedom is deeply rooted in national governance and philosophies on state control over the flow of information in all forms of communication, not just online, a norm protecting Internet freedom within sovereign nations will be unlikely to emerge in coming years.

The United Nations Human Rights Council (HRC) took a step toward developing a norm in the area of Internet freedom when on July 5, 2012 it adopted by consensus resolution A/HRC/20/L.13, which affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression." This resolution established an important point of reference by a UN body whose membership includes the United States and Russia, among others.

Authoritarian countries, however, continue to see their control over information, both online and off, as a key method of regime stability and maintaining their hold on power. China,

TWITTER'S ROLE IN INTERNET FREEDOM

In October 2012, Twitter, at the request of German authorities, blocked the account of a banned neo-Nazi group. It was the first time Twitter had taken down an account in one particular country at the behest of the government. Twitter kept the page up in other countries, including the United States, where such speech is protected.

Russia, and other like-minded states have made clear that controlling information is a critical part of what they see as their national security. Therefore, without serious shifts in domestic governance structures in much of the world towards more democratic, pluralistic institutions, respect for Internet freedom will remain a fleeting ideal. Policymakers should focus on making slow, incremental progress on respect for freedom online but must understand that universal norms are not likely to rapidly come to the fore.

4.3 Online Privacy

Norms protecting privacy online derive from various national philosophies in the physical realm. Divisions between both Western nations and democratic and authoritarian states persist online as they do regarding traditional privacy rights. Unlike with Internet freedom, where democratic states see largely eye-to-eye with some minor divisions, the split between the United States and much of Europe on privacy rights and the very philosophy about how to protect privacy is significant. However, as with Internet freedom, both models stand in stark contrast to the complete disregard for privacy in many undemocratic states. Both see the need to balance privacy rights with cybersecurity programs.

In the United States, the Fourth Amendment to the Constitution outlaws unreasonable search and seizure by the government, giving individuals a right to privacy. Courts have clarified that this individual right extends to everything that the individual has an expectation will be private. However, online such an expectation of privacy would be difficult to conceptualize, as everything sent on the Internet has to be done through private channels controlled by Internet Service Providers (ISPs). To offer greater protection, the U.S. government passed the Electronic Communications Privacy Act in 1986. Under normal circumstances, any data given to an ISP would have no expectation of privacy and thus the U.S. government could gain access to it with a simple subpoena. ECPA requires that the government receive a warrant for communications stored for up to 180 days. However, even with these privacy protections against governmental access to private data, within the United States there are limited legal controls on how private corporations may use data passed by individuals. One such legal requirement is that companies report a breach of personally identifiable information to consumers, but no single federal reporting requirement exists.

Europe offers a different model. After data becomes public or is sent to a third-party in Europe, there are binding and stringent legal requirements on what that data can be used for and what may be done with that information. For example, companies in Europe are often banned from reading the email of employees, which has largely been considered legal in the United States. Even in cases where an individual has willingly given over data, European governments and regulators have still placed restrictions on how that data may be handled and exploited. However, unlike in the United States, there is greater trust in governmental handling of private information and less stringent restrictions on government data collection.

The difference in privacy approaches between the United States and Europe has been described by Omer Tene of the Center for Democracy and Technology as "privacy as what you think it is" versus "privacy as what we tell you it is." The United States views privacy as an individual right, while in Europe it is viewed as a societal value. The check on abuse of privacy in Europe is the state, while in the U.S. government is more feared. These philosophical divides can be very difficult to bridge in both traditional and digital privacy.

Even as there are serious philosophical divides between the United States and Europe regarding privacy rights, both still have basic legal protections that are not present in much of the world, especially those states with despotic authoritarian leadership. In 2004, China pushed Yahoo to turn over emails by Chinese journalist Shi Tao regarding Chinese efforts to suppress reporting on the 15th anniversary of Tiananmen Square. He was later arrested and sentenced to ten years in prison. Similarly, during the early stages of the uprising in Syria, the Assad regime allowed social networks to stay online but actively eavesdropped on network traffic, arresting dissidents.

4.3.1 Outlook for Norms Development in Online Privacy

Much like the fight over Internet freedom, the philosophical and societal divides between states on online privacy are too wide to expect universal norms to emerge quickly and easily. Creating universal respect for online privacy must be a long-term, sustained diplomatic process and it likely will not come without the parallel growth of liberal democratic governance. Even if respect for privacy is normatively enshrined, how to legally protect privacy is not universally agreed upon, as seen with the divides between the US and continental Europe. Creating greater harmony in privacy law and practice around the world will be a long, slow process.

4.4 Cyber Espionage

The rise of cyberspace has completely changed the nature of espionage. Cyber espionage is relatively risk-free and can be vastly more productive than traditional spying. Moreover, cyber espionage can be conducted against a target in almost any nation in the world from almost any place in the world. Multiple targets can be infiltrated simultaneously and data can be exfiltrated continuously for years, most often without the target becoming aware of the espionage.

One result of this revolution in espionage is that attacks on private sector targets have increased significantly. Nation-states now have the resources to conduct espionage on large numbers of targets and the cost of an unfruitful search is minimal. Non-state actors, both corporations and criminal gangs, have become major players in cyber espionage, acting both for government and for private sector clients.

Norms around cyber espionage have been derived from those surrounding traditional state-on-state spying. Under international law, traditional political and security motivated espionage is not illegal and is generally considered common state practice. Nearly every country with the resources and technical ability to do so carries out espionage both in

cyberspace and through human, signals, image, and geospatial intelligence collection. Even with this acceptance internationally, countries have almost universally outlawed espionage on the domestic level. These same norms have been applied to cyberspace.

Unlike with political and security motivated espionage, there remains divergent state practice regarding financially motivated corporate espionage by governments for the benefit of the private sector. The United States has strongly rejected such state-sponsored corporate espionage and does not take part in the practice. However, a multitude of other countries both engage in it themselves for the benefit of their domestic industry and/or allow private business intelligence companies or criminal groups to do so, causing what appears to be significant damage to corporate businesses. In an unclassified 2011 report, the United States Office of the National Counter-Intelligence Executive pointed to Russia and China as the two greatest culprits of intellectual property theft and corporate espionage against the United States. The current state of cyber espionage has been characterized as the greatest transfer of wealth in human history.

There are international protections for intellectual property and unfair international trade practices that could be potentially applied to industrial espionage carried out through cyberspace, but norm development around their application remains nascent. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which was passed as part of the 1994 Uruguay Round of trade negotiations within the GATT (now the WTO), holds that states must set minimum domestic protections for foreign intellectual property and not act

HACK BACK AND CYBER VIGILANTISM

The increasing number of sophisticated and successful penetrations of corporate networks, coupled with the perceived ineffectiveness of law enforcement in identifying and punishing malicious actors and retrieving stolen property, is causing some companies to consider going on the offensive, including hacking into the computers that are attacking them. Unauthorized penetration, even in "hot pursuit" of a cyber thief, generally violates national computer security laws, though some have argued that common law property rights may allow some activity. Nation-states generally have a problem with individuals or corporations taking the law into their own hands, even when the actors are seeking revenge or even the mere recovery of their stolen property.

Since national laws vary on these concepts and common law is unclear, the entire subject area of "hack back" and counter-measures deserves public discussion to determine if some international norms could be developed. "Cyber vigilantism" raises the risk of the wrong people being punished and of others becoming part of "collateral damage." Unintended consequences could easily develop in a wave of uncoordinated attack and retaliation. However, it may be reasonable for an affected party to develop technical countermeasures that would allow stolen property to communicate home.

in a manner "contrary to honest commercial practices" regarding trade secrets. States are also obliged to offer equal rights to foreign and domestic IP holders. Stealing IP through cyber espionage to benefit domestic companies would likely violate these principles. In a 2011 letter to U.S. Trade Representative Ron Kirk, the leadership of the Senate Judiciary Committee raised concerns about Russian cyber espionage given their accession to the WTO, specifically as it might violate their obligations under the TRIPS Agreement.

4.4.1 Outlook for Norms Development on Cyber Espionage

As grave as the pandemic of cyber espionage is, the topic is unlikely to result in international agreement any time soon. Cyber espionage is a reality that governments will have to manage domestically just as traditional espionage is largely dealt with not through international regimes, but rather national counterintelligence efforts. Just as in other forms of intelligence gathering, successful cyber espionage can help allay states' "worst case scenario" assumptions about each other, but faulty collection and analysis can lead to poor policy decisions.

One area of cyber espionage that is harmful to international cooperation and economic competition is spying by nation-states on private sector corporations, stealing proprietary competitiveness data including research and development, intellectual property, and transactional data for the benefit of competing corporations in the spying nation. However, many states still participate in such practices. Given the belief that such cyber espionage is a valuable element of their economic development, a number of states that engage in such activity are unlikely to agree to any new international norms that would specifically address government-sponsored or government-supported cyber espionage against private sector corporations.

Concerned nations could seek to use existing international mechanisms and norms to cast a light on Chinese and other government-sponsored behavior in the hope that such action might reduce the current, brazen, large-scale government-sponsored cyber espionage on private corporations around the world. For instance, several nations could band together and jointly file a complaint with the WTO against China for its pattern of cyber espionage against private corporations, in violation of existing standards and agreements. However, to date, both governments and targeted private sector companies have been reticent to bring these issues to the WTO for trade, political, and economic reasons. Companies refrain from speaking out publicly when they have been victimized for fear of government-sponsored retaliation as well as financial and reputational damage. Western governments too have been cautious to say anything that could jeopardize sensitive economic relationships with offending states. Thus, even though government cyber espionage against the private sector could be addressed under existing international mechanisms, it is unlikely to be. State-sponsored espionage attacks on the international private sector will, therefore, likely continue unabated.

4.5 Cyber Crime

The use of computer networks to commit financially motivated crime dates back to the 1970s. In an early case, a teller at Union Dime Savings Bank in New York used computer systems controlling accounts to embezzle over $1.5 million. In the 1990s, with the expansion of online business and finance, the popularity, internationalization, and professionalization of cyber crime took off, particularly in Russia and Eastern Europe where legitimate economies were floundering. With the ability of criminals to steal money from anywhere in world, international coordination became critical for national law enforcement agencies. By the late 1980s, countries in the West had largely criminalized cyber offenses domestically, including the United States through the 1986 Computer Fraud and Abuse Act. However, many states around the world still had no laws, weak laws, or lacked the will or technical ability to carry out investigations, offering sanctuary to organized and adept criminals.

In order to combat the issue of sanctuary states and the diversity of domestic laws, groups of like-minded states began to issue recommendations for what should be included in national cyber crime legislation. As early as 1986, the Organization for Economic Cooperation and Development released a report calling for states to criminalize and harmonize computer crime laws. Similar reports were endorsed by the Council of Europe in 1989 and the G-8 in 1997. None of these reports had binding authority, but they did begin the process of creating norms around the need to outlaw criminal activity involving cyberspace and for states not to act as sanctuaries.

The norm that states must outlaw cyber-related offenses reached a level of development in the West great enough to initiate the negotiation of a binding treaty addressing cyber crime. Negotiated within the Council of Europe and signed in 2001, the Budapest Convention on Cyber Crime calls on states to outlaw such online crimes as illegal access to a computer system, interception of data, interfering with data, and committing fraud or forgery using a computer system. The treaty also calls on state parties to provide mutual assistance in the investigation of cyber crimes. Most European nations have signed and ratified the convention with Japan and the United States as the only non-European states to have acceded. Russia, China, Brazil, and other important economic players have neither signed nor ratified. There has been little normative movement since Budapest, but Russia and China have pushed for a potential UN-based global cyber crime convention.

4.5.1 Outlook for Norms Development on Cyber Crime

Cyber crime has been the area where the most significant international norms progress has been made thus far. The Budapest Convention is a constructive first step, a multilateral treaty that establishes norms of cooperation and behavior among the parties. However, problems remain in enforcing cyber crime laws internationally. First, the Convention has not attracted the participation of some major nations such as Russia and China. A number of smaller nations that have become centers of international cyber crime activity are also not adherents to the Convention. Second, the Convention does not fully address the cross-

jurisdictional problems associated with cyber crime. The burden of dealing with crimes continues to fall on individual nation-states, many of which are ill equipped to investigate or apprehend criminals based outside their borders. Cyber crimes frequently leave an evidence trail that runs through many countries and are difficult for a single nation to solve. Cyber criminal enterprises often attack many nations simultaneously, creating the need for multilateral investigative responses. Yet, the Convention has not resulted in the creation of an effective multilateral organization to respond rapidly to criminal activity or to do post-crime forensics. Finally, some nations have become, in effect, cyber crime sanctuary states, allowing cyber criminal enterprises to operate with impunity. While sanctuaries are sometimes a result of the host nation having insufficient capacity to terminate the activity, more often there is complicity on the part of national police and security service authorities. That complicity results both from bribery of authorities by the cyber criminals and from the intentional policy of some nations to permit the cyber criminal enterprises as a form of cyber reserve army, available for "deniable" cyber espionage and potentially cyber war.

In considering normative solutions, the optimal outcome might be the creation of a global cyber crime convention, building on the Budapest Convention, adding additional adherents and an operational organization to assist in investigations. Many nations will not agree to the Convention or an enhanced version of it any time soon. However, rather than do nothing more about international cyber crime, like-minded states might act to build on the Budapest Convention.

4.5.1.1 A Like-Minded Nations Center

To address both the sanctuary problem and the difficulty of dealing with cyber crimes that spread out over many nations, a small organization of like-minded states could create the Cyber Crime International Investigative Center (IIC) to do the following:

- Create, share, and maintain for member states a database of significant cyber crimes, the techniques employed, and the possible suspects;
- Operate a Significant Cyber Crime Response Squad of investigators and forensics experts who could rapidly assist a member state upon request; and,
- Coordinate in real time, or near real time, requests by member sates for assistance in investigating, tracing, and doing forensics on cyber crime attacks.

The IIC would be different than Interpol because unlike Interpol, its membership would not include sanctuary states. It would also differ from traditional Computer Emergency Readiness Teams (CERTs) because its focus would be on solving crimes, identifying criminals, making arrests, and achieving successful prosecutions.

PROPOSED IIC CHARACTERISTICS

Multilateral treaty, like-minded states, closed membership, secretariat, technical assistance and prescribing behaviors, domestic implementation, limited private sector role.

Member states could use the IIC as a forum to note when they believe they have been given inadequate or untimely assistance from other member States. The IIC could create metrics for judging the degree of and speed of assistance a nation provides another nation in such cyber crime investigations. The IIC would address the problem of sanctuary states through coordinated capacity building assistance when a possible recipient nation demonstrates a real interest in complying with international norms concerning prosecuting or extraditing cyber criminals. Members states could deal with recalcitrant or scofflaw sanctuary states by conducting international investigations, publishing "name and shame" reports documenting state complicity with cyber criminals, and engaging in multilateral diplomacy with such states. Ultimately, IIC member states might have to consider multilateral sanctions against sanctuary states, but that would be a last resort and need not be explicitly addressed during the creation of the like-minded group or its IIC.

For the IIC to work successfully, member states would have to agree upon and implement domestically an international norm along the following lines: "When requested through IIC channels, a member state will rapidly assist another member state with an investigation or with cyber crime mitigation, including through the use of court ordered search warrants and cease-and-desist orders." For the United States to achieve that level of cooperation with other like-minded states would require the creation of a central response office with the ability to obtain court orders quickly no matter which U.S. jurisdiction was involved, and teams of cyber crime investigators dedicated to assisting other nations' requests for action in the United States quickly. Currently, other nations' requests for assistance with an on-going cyber crime are often not acted upon with a positive outcome in a timely manner.

Members states could deal with recalcitrant or scofflaw sanctuary states by conducting international investigations, publishing "name and shame" reports documenting state complicity with cyber criminals, and engaging in multilateral diplomacy with such states.

4.6 Cyber War

Norms around how and under what circumstances cyber war can be fought have been grafted onto the existing legal instruments that govern when states may engage in armed conflict and what constitutes a legitimate target. In both jus ad bellum (right to war) and jus in bello (law during war) norms and international legal rules, those applying to air, space, land, and sea are also being applied to cyberspace by states. In jus ad bellum norms, the United Nations Charter prohibits the use of force against another state except in cases in which a country is responding in "self-defense" to an "armed attack" carried out against its territory or when authorized by the UN Security Council. During armed conflict, jus ad bellum, largely made up of the Hague and Geneva Conventions and often referred to as the law of armed conflict (LOAC), guides

how and against whom hostilities may be conducted, attempting to limit the impact of war against civilian populations. A number of states are attempting to take these principles, which were developed in a purely kinetic warfighting era, and create norms around their application to cyber conflict.

During cyber war and in carrying out offensive cyber operations, most nations have accepted that LOAC applies and constrains their actions. China remains the singular major power in cyber conflict to dissent from this norm. Unlike other norms where international consensus has been built through international agreements, norms around the applicability of LOAC have been expressed through state practice and statements of national policy. For example, in presenting the 2011 Strategy for Operating in Cyberspace, former Deputy Secretary of Defense William Lynn made clear that US would be guided by the law of armed conflict when responding to cyber attacks. The United Kingdom has also explicitly stated that the law of armed conflict applies in cyberspace. The International Committee of the Red Cross, an influential non-state norm promoter on international humanitarian law, has consistently held that the law of armed conflict must guide offensive cyber operations. However, while there is largely acceptance of LOAC, how to apply the key principles of distinction between civilians and military objectives, military necessity, and proportionality of attacks is difficult and has not been well articulated in the international normative environment.

In terms of the right to go to war, most countries have accepted that the United Nations Charter applies to international cyber relations. However, there remain challenges in applying the Charter to cyber conflict. Under Article 2(4) of the UN Charter, the "threat or use of force against the territorial integrity or political independence" of any state is outlawed. Article 51 of the Charter then sets a higher bar for the invocation of the inherent right to self-defense, holding that a state must be victim of an "armed attack." Countries have made few statements about how to apply these standards in cyberspace, but there is momentum within the United States towards a norm whereby cyber attacks would be judged by their equivalent kinetic effects in order to determine whether they constitute force or an armed attack. In a September 2012 speech, US State Department Legal Advisor Harold Koh stated, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." He cites the triggering of a nuclear power plant meltdown, the opening of dam flood gates, or attacking air traffic control networks and causing plane crashes as clear uses of force through cyber means. However, Koh also notes that there are many cases of cyber conflict that would not be so clear and that other countries see a wider gap between a use of force and armed attack than does the United States in both kinetic conflict and cyber war. The United States traditionally and in cyberspace sees very little to no space between a use of force and armed attack. Also, attributing cyber events to a particular state, which is critical for striking back in self-defense, can be technically difficult in cyberspace. It has been suggested by some that the ability to carry out attribution is improving, however.

China is one of the key states that have reservations about US-advanced jus ad bellum norms. They have expressed support for the applicability of the UN Charter, but have

focused on issues of territorial integrity and non-interference rather than cyberspace as a new avenue for armed attacks. In their 2011 Code of Conduct for Information Security, China, Russia, Uzbekistan, and Tajikistan state that all countries must comply with the UN Charter, citing issues of territorial integrity and sovereignty, and call on states not to carry out hostile activities or acts of aggression, but make no mention of potential armed attacks or the right of self-defense. The right of self-defense when victim of an armed attack is critically important to the overall acceptance of the applicability of current jus ad bellum principles and the UN Charter as a whole to cyber war. However, the fact that the illegality of the threat or use of force, as expressed in Article 2(4), is included in the Code of Conduct could indicate that there is potentially some space for discussion on the acceptance of the traditional "use of force" and "armed attack" jus ad bellum framework.

Along with jus ad bellum and jus in bello norm propagation, there have been state efforts at limiting cyber "weapons." Russia has long supported a binding international arms control treaty for cyberspace that would ban information warfare capabilities. The United States, as the dominant offensive cyber power, has rejected such an idea because it would be unenforceable and constrain its offensive superiority. However, Russia has had more success in normatively presenting the idea that the use of ICT against the maintenance of international stability and security is of international concern. This sentiment was first expressed in 1999 in UN General Assembly Resolution 53/70, and the UN Secretary-General has presented a report with member state opinions on the issue annually.

4.6.1 Outlook for Norms Development on Cyber War

Potential ideas for cyber war control and limitation are numerous, including confidence building measures (CBMs), tacit or unilateral declaratory norms, and ultimately a multilateral cyber war treaty. The negotiating history of other agreements (LTBT, NPT, SALT, START, INF, CFE, CWC, BWC) is instructive as we begin to think about cyber war control. Many of those agreements began with small steps such as CBMs or tacit unilateral declarations and evolved into treaties.

> Every significant area of arms control in the last forty years has also posed major verification problems, but they were overcome, and the resulting agreements enhanced security.

There are unique difficulties in cyber war control stemming from the difficulty of attribution and verification. The verification hurdle was initially viewed as an insurmountable barrier in the arms control of nuclear weapons development and testing, nuclear-armed missiles, conventional land forces, chemical weapons, and biological weapons, but over time, functioning norms regimes and verification systems were able to be constructed. Whether verification and attribution improve in cyberspace or not, advancement can still be made on international norms governing cyber war.

4.6.1.1 Confidence Building Measures

In 2010, the UN Group of Government Experts on Issues of Information Security (GGE) found consensus on the need for confidence building and risk reduction measures, along with information exchange on national strategies, policies, and practices. States hope that such

measures will reduce the risk of cyber conflict by increasing transparency about the actions of other states and provide avenues for building trust between cyber powers. However, even with this international consensus on the need for confidence building measures, no strong, institutionalized practices and procedures have yet been built.

The creation of CBMs between states would be an important and practical first step in the creation of norms of state behavior intended to limit the risk of cyber war. CBMs ban some kinds of activities, limit others, create channels for discussion, and add transparency measures designed to reduce suspicion and tension among militaries. Such CBMs create norms about expected state behavior during certain situations and can proliferate those norms as these processes mature. Starting with simple CBMs about sharing information about threats and during crises, which states have experience with in other areas of interstate relations, and then working towards more controversial or involved CBMs would be a good course to pursue.

PROPOSED CYBER RISK REDUCTION CENTER CHARACTERISTICS

Multilateral international agreement, like-minded states, open membership, small institution, confidence building through information exchange, no domestic implementation, minimal private sector involvement.

A group of nations, perhaps through the Organization on Security and Cooperation in Europe (OSCE), could agree to the creation of a multilateral Cyber Risk Reduction Center. Risk reduction centers are a known phenomenon, small organizations designated as the point of contact when one nation has questions or concerns about perceived activities of another nation, which might appear threatening or destabilizing. Russia and the US have agreed to use existing bilateral risk reduction centers for cybersecurity risk discussions. The United Kingdom is also establishing bilateral risk reduction center agreements. Thus, creating a channel for multilateral risk reduction should be relatively easy and an important first step in the creation of CBMs.

In parallel, an OSCE working group on CBMs in cyberspace has been convened under the chairmanship of the United States to discuss a basic, but important, set of initial CBMs. While progress in these discussions is somewhat difficult to assess from the outside, multilateral agreement at the OSCE on a particular subject is often held hostage over disagreement on other issues, often between the United States and Russia. Exploring what types of confidence building measures might be created to apply to activities in cyberspace, however, is an important avenue that OSCE member states should continue to pursue. As with other international discussions on cybersecurity, these OSCE discussions would benefit from the involvement and participation of key private sector stakeholders. Inviting such an open discussion about cyber CBMs might produce creative ideas, some of which might be negotiable in the near term.

4.6.1.2 Declaratory Policy on Key Private Sector Target Avoidance

In most wars, private corporations' facilities are damaged. Certainly, corporations engaged in the manufacture of arms are thought to be fair game to be attacked. Hospitals, however, have long been ruled off limits by international law. Prior

to the negotiation of rules of the road for cyber war, nations might consider unilateral declaratory policies stating their intentions to avoid certain classes of targets. Such unilateral articulation of policies does not raise verification issues because the policies only affect the declaring nation itself. Nonetheless, the declarations begin to shape international conduct and may lead to later negotiated norms.

Among the classes of targets that might be considered to be designated safe havens from cyber war are financial institutions, electrical power systems, and the infrastructure of cyberspace itself. Many of those types of facilities are frequently private sector owned and operated.

The Financial Sector

In most major nations, the financial sector has become inherently international and interconnected. The international financial system is based to a large degree on trust, a belief that assets recorded in databases do in fact exist in the type, amount, and ownership recorded. Altering and falsifying those databases, or engaging in unauthorized ownership transfer, would significantly undermine the international financial system.

Thus, nation-states have a major incentive to refrain from altering data in or disrupting the communications system of the international financial system. The United States reportedly considered and rejected a cyber attack on the Iraqi banking system in 2003 precisely because of a fear that such an attack would be a precedent that would be used by others to justify similar attacks, which would undermine the essential trust in the international financial system. Arms control often begins with nations promising not to do things that they never had any intentions of doing anyway. Thus, a first step to a cyber war norm might be a series of unilateral declarations that financial sector targets will be avoided.

The Electric Power System

Power generation and distribution systems are often "dual use," in that they usually support both government (including military) and private sector facilities. Thus, targeting a generator or a transformer for cyber attack could bring down a grid that supported both a military base and a civilian hospital. While nations might foreswear attacks on hospitals, they are likely to target military bases by using cyber weapons. Indeed, attacking a power grid may be one of the best ways in which to debilitate a nation's military capability.

Thus, while it might be desirable to have nations declare their intentions to avoid cyber war targeting of power grids, such declarations may lack credibility.

The international financial system is based to a large degree on trust, a belief that assets recorded in data bases do in fact exist in the types, amounts, and ownership recorded. Altering and falsifying those databases, or engaging in unauthorized ownership transfer, would significantly undermine the international financial system... A first step to a cyber war norm might be a series of unilateral declarations that financial targets will be avoided.

Cyberspace-Enabling ICT

The infrastructure that enables cyberspace, including domain name servers, cables, switches, routers, public key infrastructure, certificate authorities (CAs), and data centers, as well as software and applications that manage these functions, is so critical to modern society that it is occasionally referred to as a "global commons," a precious societal resource valued like the sea, air, and space. Offensive cyber operations targeting the cyberspace commons itself are distinct from those that target specific civilian or military infrastructure; both can have harmful effects, but attacks against the underlying infrastructure of the commons have broader and fundamental societal implications. For instance, cyber operations targeting root servers, the Domain Name System, certificate authorities, and other elements that constitute the cyberspace commons can cause widespread disruption of the functioning of the commons, as well as undermine the trust in and reliability of the systems. On the other hand, cyber operations against specific targets can have significant and destructive impacts on systems without disrupting or affecting the broader commons.

Nation-states should consider developing international cybersecurity norms banning the destruction or disruption of cyberspace-enabling infrastructure. States should articulate their intentions not to disrupt or destroying cyberspace-enabling ICT, as such technology is fundamental to modern life and the smooth functioning of the global economic system. Without a functioning and available Internet, modern commerce comes to a halt. During a conflict, destroying or disrupting the underlying Internet architecture would not only harm other belligerent parties, but the international system as a whole.

STUXNET AND FLAME: EXPLOITATION OF CERTIFICATE AUTHORITIES

The Stuxnet worm exploited four zero day vulnerabilities and compromised multiple certificate authorities in order to physically damage approximately 1,000 Iranian nuclear centrifuges. It used two legitimate, signed digital certificates from Taiwanese companies. The first certificate was from RealTek Semiconductor, a small hardware firm. While the RealTek certificate was quickly revoked, a second stolen certificate from JMicron Technology was later discovered.

Flame was a sophisticated espionage tool that spied on infected machines by logging keystrokes, taking screenshots, and remotely and surreptitiously activating computer microphones to record conversations of users. The malware exploited a cryptography algorithm associated with the Microsoft Terminal Licensing Service that issued certificates with the ability to sign code binaries as if the code had come from Microsoft. This allowed Flame's operators to hijack the Terminal Licensing Service certificate authority to assign Flame a Microsoft imprimatur, which would lead any targeted machine to accept the malware as if it were coming directly from Microsoft. The creators of Flame had discovered a way to make, theoretically, anything appear as though it was from Microsoft.

As most major players in cyber conflict rely heavily on the global Internet for economic growth and the quality of life of their populations, finding a significant number of states willing to enact such a declaratory policy should be possible. Disrupting or destroying cyberspace-enabling infrastructure runs in direct conflict to the national interests of most states in the international community. The International Telecommunications Union has estimated that one third of the total world population uses the Internet. The majority of these users are in the developing world. Both rich and poorer states should have an interest in keeping cyberspace functioning for their domestic development and economic expansion. The trust and expectation that the Internet will operate properly empowers innovation worldwide.

It would also be beneficial for like-minded states to declare that they will not exploit cyber commons technology. Just as directly attacking underlying infrastructure hinders the global benefits of cyberspace, so too does exploiting the trust mechanisms that enable its smooth operation. For example, in both the Stuxnet and Flame malware, attackers exploited certificate authorities to gain trusted access to networks. While neither Flame nor Stuxnet directly disrupted or destroyed the certificate systems themselves, the exploitation of the trust that end users place in ICT companies that issue certificates arguably does equivalent harm to the global cyber commons as a direct attack on the architecture. Exploiting cyberspace-enabling technology stifles innovation and the economic benefits of cyberspace by breaking down the expectation that these mechanisms are secure. Without this expectation, users will be less likely to put more advanced and potentially risky services online.

Unlike with disruption or destruction of the underlying Internet architecture, finding broad-based international support for a norm against the exploitation of such infrastructure is likely to be more difficult, as it can be used as a method for then carrying out espionage or offensive cyber operations against more enticing strategic targets. As was seen with the Flame espionage software, exploiting underlying cyberspace technology can give intelligence collectors trusted access to key systems, allowing easy exfiltration of potentially valuable information housed on networks. As previously discussed, strong, universal norms limiting cyber espionage are not likely to emerge, and espionage is a common part of interstate relations. While states will likely be reluctant to abandon the advanced capabilities necessary to quietly exploit such technology, declarations by like-minded states – as outlined above – could evolve into a strong norm adhered to by the international community, which would in turn be beneficial to the entire global Internet user base.

Before a government creates collateral damage through attacks on the underlying trust mechanisms of the Internet, there should be a serious review of the need to do so. The national leadership should conduct this review, and decisions should not be made solely by intelligence officials.

4.6.2 Cyberspace Commons Arbitration

While a series of unilateral declaratory statements by nations regarding the inviolability of the ICT commons would be welcome, it would also be insufficient. Nations have already ex-

ploited, damaged, and disrupted the international ICT commons infrastructure. Thus, such declarations would take on added significance if backed up by a system to financially compensate the private sector corporations that are damaged by nation-states activities. In no other domain is the private sector given the role of creating and maintaining a global commons, which suggests that such companies deserve special international protections.

States must take responsibility for the costs they place onto the private sector when exploiting, disrupting, or destroying cyberspace-enabling ICT and deviating from these proposed norms. When cyberspace-enabling ICT is exploited, disrupted, or destroyed, the private sector currently bears the costs. In 2011, RSA's SecurID token system, which is used for secure, remote connectivity by many large organizations, was compromised. RSA put the cost of remediating the attack at $66 million. In the case of the Flame attack, which exploited its certificate authority, Microsoft shouldered the burden of repairing the systems at a significant but unknown cost. The Stuxnet attack against the Iranian nuclear facility at Natanz compromised the digital certificates of Realtek Semiconductor and JMicron Technologies, Taiwanese ICT companies. While it is possible for states to make payments to private sector actors quietly and out of the public eye, an international arbitration panel, created by like-minded states who have explicitly affirmed through international agreement that they will not exploit, disrupt, or destroy cyberspace-enabling ICT, would offer a better mechanism for enforcing norms that support the stability and security of the global cyber commons. Arbitration is a common method for resolving international disputes, including through the Permanent Court of Arbitration.

Such an arbitration mechanism, called the Cyberspace Commons Arbitration Panel, would be empowered by states to name offending member and non-member states and order member countries to pay restitution to private sector companies that are part of the global commons should evidence become available that a member state was responsible for an attack. The arbitration panel would see evidence presented by independent forensics specialists and affected companies to identify the malicious actor and determine their relationship to a nation-state. While attribution might not always be possible, attempting to hold attacking states responsible shifts the financial burden of remediation back onto offending nations as well as names and shames them as bad actors in the international community. Such a burden for states would give norms against harming the cyber commons greater teeth.

PROPOSED CYBERSPACE COMMONS ARBITRATION PANEL CHARACTERISTICS

Multilateral treaty, like-minded nations, open membership, secretariat and formal institution, dispute resolution, no domestic implementation, large private sector role.

Even in cases when attribution could not be achieved or a non-member state or non-state group was responsible for the harm caused to the privately constructed global commons, a global fund, financed by the like-minded states, could help provide compensation to private actors for their damages. Such a system might put a financial strain on states that were not

involved in actually causing harm, but it would allow these countries to show a commitment to the global cyber commons that could not be questioned. Demonstrating a willingness to reimburse harmed private actors for losses not caused by ones own state in very specific circumstances would demonstrate a real commitment to the preservation of an open, innovative, and safe Internet.

Companies seeking to utilize the arbitration mechanism should show attributes about both their operations and the attack. First, companies must be able to prove that their products or services are cyberspace-enabling ICT and contribute directly to the operation of the global commons. If they are unable to do so, exploitation or attack against them would not reach the same level of international concern and would not be open to arbitration. Second, they must show harm and be able to quantify that harm. Without being able to specifically show their losses, the panel would be unable to provide them with restitution. Finally, companies must present any forensics evidence they have collected or third-party forensics firms have found in order to assist with the attribution process.

Such a system presents the best possible hope for adding enforcement behind the proposed norm against attacks on cyberspace-enabling ICT. While states may be unwilling to enter such an arbitration system, it does offer a potential option for moving the responsibility for remediating harm inflicted upon the cyber commons from the private sector to states. Ultimately, it is not an acceptable status quo for the private sector to continue to suffer financially for the harm done to the global Internet commons by nation-states acting for their own strategic gain.

5 A Call to Arms: The Private Sector and International Cyber Norms

While nation-states, intergovernmental organizations, and non-governmental organizations are traditionally powerful "norm entrepreneurs" in the international system, throughout the centuries, private actors have taken leadership roles in the development of international norms in a variety of areas. In the 17th century, Hugo Grotius wrote *Mare Liberum* while counsel to the Dutch East India Company, formulating a theory that the high seas should be open and free for all to use. In the early 20th century, government, labor, and business working together created the International Labor Organization and its associated standards. In the late 20th century, DuPont and other chemical and bio-chemical companies were key to the development of both the Chemical Weapons Convention and the biological weapons ban. Private sector experts assisted in the development of US government positions and acted as consultants to US arms control negotiating teams. Without their expertise,

THE PRIVATE SECTOR: A TARGET IN CYBERSPACE

There are certain circumstances under which private sector companies may be legally targeted by national militaries both in kinetic and cyber conflict. Under the law of armed conflict and the principle of distinction, civilian infrastructure is generally considered to be separate from military objects, with military installations always targetable during international armed conflict and civilian infrastructure off limits from direct attack. However, even in the physical realm, there is often ambiguity about what constitutes civilian infrastructure. The 1977 Additional Protocol I to the Geneva Convention attempts to set out a standard under which normally civilian infrastructure could become a military objective. Under Article 52(2) of Additional Protocol I, military objectives are defined as "objects which by their nature, location, purpose, or use make an effective contribution to military action" and on which an attack would provide a "definitive military advantage." Article 52 implies that if traditionally civilian infrastructure, often held by the private sector, is being used for military purposes and damaging, neutralizing, or destroying such infrastructure would serve a military goal, it is defined as a military object and thus open to attack. While key global players in cyberspace such as the United States, Israel, and Iran have not signed Protocol I, Article 52 is considered customary international law by the international community and thus binding on all states.

the verification systems of those two treaties could not have been successfully formulated, nor could either treaty have been ratified by the United States Senate absent their support. Previously mentioned normative systems like the IMO (maritime security), ICAO (aviation security), and FATF (money laundering) also include significant private sector participation.

If any area of international norms or arms control ever required such corporate involvement it is cyberspace. Almost all of the world's fiber optic communications cables, Internet backbone routing and switching systems, and data storage centers are privately owned and operated. Almost all software and hardware is the creations of the private sector. Although there are pockets of expertise in some intelligence agencies and military units, the leading minds in the development and operation of cyber systems are in universities, laboratories, and corporations.

Without extensive private sector involvement, governments would not be able to devise international cyber norms that would work or be accepted. Beyond the need for their expertise, private sector cyber corporations also have equities in the conduct of governments in cyberspace. Private actors must participate in the development of international norms related to cyber war if for no other reason than they are potential targets for attack. As most of the international community has accepted that existing international law and norms can be applied to cyberspace including the law of armed conflict, private sector companies of all types (including but not limited to critical infrastructure) must understand and prepare for the consequences that the existing normative framework potentially has on their operations. The private sector often wants to think of itself as separated from military operations, immune and segregated from acts of warfare. This clean separation of the private sector as only civilian in nature from legitimate military targets is not a reality under existing international law should that private infrastructure be acting to support military action.

All private sector actors potentially involved in cyber war, in particular potential targets including information and communication technologies companies and private critical infrastructure owners and operators, should be involved in the norms creation process concerning targeting in cyberspace. This large private sector community can play a key role by pooling their collective voices to influence conversations on the legitimacy of certain military targets, even as such conversations have traditionally been dominated by nation-states. This voice could help governments better understand the risks of targeting certain types of infrastructure, including the potential for serious and unintended cascading effects resulting from cyber attacks, even as such attacks might be legal in certain circumstances under the law of armed conflict.

6 Conclusion and Recommendations

Given the dependence much of the world has on cyberspace, it is surprising that few international norms have emerged concerning it. Those that have been created, such as the Internet Engineering Task Force and its Request for Comments-based standards, have been largely the work of the private sector. Governments have more often been involved in intractable disputes with each other about whether, where, and how to create standards for their own behavior in cyberspace.

The pandemics of cyber crime and cyber espionage as well as the building of cyber offensive capabilities by over thirty countries to date suggest a need for a renewed attempt at creating international cyber norms to limit the damage being caused. The prospect of destructive cyber war adds a new urgency to the creation of cyber war control regimes. Yet governments have not created the public-private partnerships necessary to shape such limitation regimes. Some government officials seem to think that they are better off without new norms, better able to operate without constraints and unlikely to be hurt as much by malicious cyber activity as benefited by it. Others persist with notions about the impossibility of cyber norms due to preconceptions about nations' motives or the inherent difficulty of issues such as attribution and verification. Such thinking is shortsighted and ultimately dangerous. The proliferation of knowledge about how to conduct malicious cyber activity means that such wisdom is no longer held only by people who will act for the good of humanity. That fact combined with the inherent advantage of cyber offense over cyber defense means that the absence of international norms and controls puts vital national and global systems at risk.

Some government officials seem to think that they are better off without new norms, better able to operate without constraints and unlikely to be hurt as much by malicious cyber activity as benefited by it. Others persist with notions about the impossibility of cyber norms due to preconceptions about nations' motives or the inherent difficulty of issues such as attribution and verification. Such thinking is shortsighted and ultimately dangerous.

A global treaty meaningfully limiting malicious cyber activity would be difficult to achieve today. Indeed, it may never be possible, but first steps in that direction are feasible now. Those steps may create the atmosphere and understanding necessary for a meaningful global agreement someday, but even if they do not, the steps that can be taken today have inherent value.

The initial multilateral step most likely to succeed would focus on cyber crime and

would be conducted by a membership-limited group of like-minded nations. Their efforts would try to deal with the problems created by cyber crime sanctuary states and the current weakness of timely mutual assistance in the international investigation of cyber crime cases.

While cyber espionage norms are likely to remain weak and the theft of intellectual property will continue, nations that do not participate in industrial espionage should attempt to use existing international enforcement mechanisms to change the status quo. A WTO case against offending states offers the only reasonable hope for ending the impunity with which cyber espionage against private sector actors is currently carried out. However, with the lack of political and economic will shown by states for such a confrontational approach, it appears to be an unlikely avenue in the short-term.

Some steps might also be taken to begin to address cyber war control. Bilateral risk reduction efforts along with the formulation of declaratory policies and "politically binding" norms would be the best course of action for initial progress and could lay the foundation for subsequent multilateral agreements. The private sector has a substantial role to play in this process.

Just as in other areas of international relations, movement towards deep international cooperation is often slow and requires sustained diplomatic action with significant private sector support. This paper has suggested the following normative starting point:

6.1 Like-minded nations should form the Cyber Crime International Investigative Center to deal with criminal cartels and cyber crime sanctuary states.

6.2 States should cooperate in a timely manner with mutual assistance requests on cyber crime, including through the use of court ordered search warrants and cease-and-desist orders.

6.3 States should participate in bilateral and multilateral Cyber Risk Reduction Centers by responding to inquiries about potential malicious action by other states and sharing information on potential threats.

6.4 Like-minded nations should coordinate on a joint presentation to the WTO concerning rampant state-sponsored or state-condoned cyber espionage in support of industrial competitiveness of corporations.

6.5 States should declare their intentions not to target financial institutions, including banks and stock exchanges, with attacks that alter data, move money, or disrupt markets.

6.6 States should declare their intent not to exploit, disrupt, or destroy cyberspace-enabling ICT infrastructure.

6.7 Should states exploit, disrupt, or destroy privately controlled cyberspace-enabling ICT infrastructure, those private sector firms should be reimbursed for the harm caused to them by offending states through an international investigative and arbitration mechanism called the Cyberspace Commons Arbitration Panel.

6.8 States should involve and consult closely with private sector ICT companies on the creation of international cyber norms and confidence building measures.

Good Harbor Security Risk Management, LLC
Washington D.C.
703-812-9199
contact@goodharbor.net
www.goodharbor.net