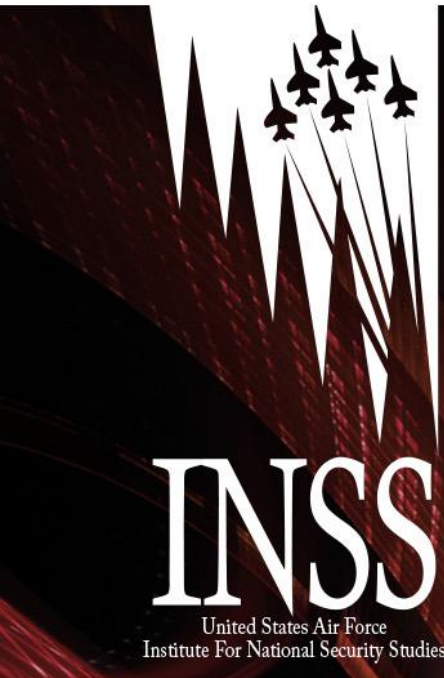
PROSPECTS FOR AN INTERNATIONAL CYBERSECURITY REGIME

Polly M. Holdorf, Toeroek Associates, Inc.



2015

INSS STRATEGIC PAPER

US AIR FORCE
INSTITUTE FOR NATIONAL SECURITY STUDIES
USAF ACADEMY, COLORADO

PROSPECTS FOR AN INTERNATIONAL CYBERSECURITY REGIME

By Polly M. Holdorf[*]
2015

INTRODUCTION

Cybersecurity represents a unique and evolving challenge to US national security planners and practitioners. Global interconnectedness facilitated by the internet has created unprecedented opportunities for international commerce and communication. The evolution of cyber technology provides many positive benefits, but significant security risks come along with it. The United States must be prepared to meet a range of cyber challenges such as cyber-crime, cyber-espionage, and cyber-sabotage.

Cyberspace is a domain unlike any other. There are no physical boundaries in cyberspace; actions taken by a group or an individual on one continent can precipitate an immediate effect on a target located on the other side of the world. There are no physical walls, security fences or border checkpoints to prevent malicious cyber activity from crossing international borders. The cyber domain is a virtual domain that allows for anonymity in addition to the ease and low cost of operating within it. Cyber-attacks may be perpetrated by states, non-state actors, or individuals and attribution of such attacks can be exceedingly difficult. Damage sustained by cyber-attacks is generally intangible, or non-physical, and yet such attacks can have disastrous effects. Both the public and private sectors are vulnerable to cyber-attack.

This paper considers the potential for the establishment of an international cybersecurity treaty, order, or regime. It begins by reviewing existing international treaties and polices relating to cybersecurity – specifically the Budapest Convention on Cybercrime and the cyber-related policies of the United States and NATO. The second section looks at the proposed International Code of Conduct in Information Security and discusses the Chinese viewpoint regarding cybersecurity. The third, and final, section examines two alternate forecasts on the probability of the establishment of a viable international cybersecurity agreement.

EXISTING TREATIES AND POLICIES

At the present time there is only one cyber-related international treaty in existence. This section provides a brief overview of the Budapest Convention on Cybercrime and addresses the cybersecurity-related policies of the United States and NATO. Two US policy documents, the International Strategy for Cyberspace and Executive Oder 13636, are reviewed and the roles and responsibilities of US agencies

[*] The views expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

regarding cybersecurity are discussed. The section concludes with an overview of NATO's cyber defense policy.

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime is the first international treaty to address internet and computer crime, and it is the only legal instrument designed to facilitate international cooperation against cybercrime. It provides common definitions and criminal prohibitions, unified procedures and rules to ensure the preservation of evidence, and a streamlined legal process to facilitate international cooperation.[1] The Convention, drawn up by the Council of Europe in 2001 and ratified by the United States in 2006, addresses cyber-related crimes such as copyright infringements, computer-related fraud, child pornography, hate crimes, and violations of network security. State signatories to the Convention are required to establish specific types of conduct as criminal offenses in domestic legislation, provide criminal justice authorities with effective means for investigations, and engage in efficient international cooperation.[2] To be clear, while the Budapest Convention is the only cyber treaty currently in existence, its focus is on criminal justice – not cybersecurity in the political-military sense.

US Policy

<u>The International Strategy for Cyberspace</u>

In May 2011 the White House issued its "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." The first of its kind, the Strategy is intended to provide a roadmap for US departments and agencies to define and coordinate their roles in international cyberspace policy, identify specific ways forward, and plan for eventual implementation. The document calls on both civil society and the private sector to "reinforce these efforts through partnership, awareness, and action" and invites other states to join in "realizing this vision of prosperity, security, and openness in our networked world."[3] The key focal points of the Strategy concentrate on the future of cyberspace, building a cyberspace policy, and identifying policy priorities. The document affirms that the United States is committed to preserving and enhancing the benefits of digital networks and will pursue an international cyberspace policy which empowers the innovation that drives the US and global economies. The United States will confront the inevitable challenges brought about by the growth of digital networks while preserving fundamental freedoms, privacy, and the free flow of information.

The "International Strategy for Cyberspace" states that the United States will build and sustain an environment in which "norms of behavior guide state's actions, sustain partnerships, and support the rule of law in cyberspace."[4] Existing principles which will likely support cyberspace norms include: upholding fundamental freedoms, respect for property, valuing privacy, protection against crime, and the right of self-defense. Additionally, emerging norms could include: global interoperability, network stability, realizable access, multi-stakeholder governance, and cybersecurity due diligence. Diplomacy,

defense, and development will all be incorporated into the future US role in cyberspace. The United States will seek to include as many stakeholders as possible, will defend its networks, and will encourage good actors while dissuading and deterring actors who use cyberspace to threaten peace and stability. The United States will work bilaterally and multilaterally to facilitate cyberspace capacity-building abroad and will assist other states in the development of cybersecurity capabilities relevant to their levels of technological development. The enhancement of national-level cybersecurity in developing nations will be of immediate and long-term benefit.

The Strategy identifies seven distinct areas of policy priorities which form the action lines for the strategic framework: 1) Economic – promoting international standards and innovative, open markets; 2) Protection of networks – enhancing security, reliability, and resilience; 3) Law enforcement – extending collaboration and the Rule of Law; 4) Military – preparing for 21st Century security challenges; 5) Internet governance – promoting effective and inclusive structures; 6) International development – building capacity, security, and prosperity; and 7) Internet Freedom – supporting fundamental freedoms and privacy.

Executive Order 13636: Improving Critical Infrastructure Cyber Security

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (E.O. 13636), issued in March 2013, seeks to "enhance security and resilience of CI [critical infrastructure] through voluntary, collaborative efforts involving federal agencies and owners and operators of privately owned CI, as well as use of existing federal regulatory authorities."[5] It utilizes statutory and constitutional authority to expand information sharing and collaboration between the government and the private sector, develop a voluntary framework of cybersecurity standards and best practices for protecting critical infrastructure, establish a consultative process for improving cybersecurity of CI, identify high priority CI for protection, establish a program of incentives for the voluntary adoption of the framework, review cybersecurity regulatory requirements, and incorporate privacy and civil liberties protections in activities under the order.[6]

An important question regarding information sharing is how to balance the requirement for improved cybersecurity with other imperatives such as the protection of privacy, civil rights, and legitimate business and economic interests. Some CI sectors are already subject to federal cybersecurity regulations, but the protection of other sectors is dependent on voluntary regulatory efforts. Proponents of additional mandatory regulation argue that voluntary regulations don't provide sufficient protection; opponents maintain that implementing additional federal requirements would be expensive and ineffective. E.O. 13636 doesn't authorize federal CI regulation other than what is already present under existing law, but it does require the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework, the Secretary of Homeland Security to establish

performance goals for the framework, sector-specific agencies to coordinate review of the framework, develop sector-specific guidance, and report annually on participation by CI sectors, and CI regulatory agencies to engage in a consultative review of the framework and determine if existing requirements are adequate.[7]

Some security observers view E.O. 13636 as a necessary measure in the effort to secure critical assets against cyber threats, but critics have voiced several concerns.[8] Some critics think that the process for developing the framework is too rushed, others think it is too slow. Some worry that the framework risks becoming a form of *de facto* regulation, others are concerned that it will be unenforceable because of its voluntary nature. Detractors claim it does little to improve on existing processes and could actually decrease the likelihood of legislation being enacted. There is also concern that it could lead to over- or under-classification of high-risk infrastructure by DHS.

US Roles and Responsibilities

A recent *Air & Space Power Journal* article titled "Policy for US Cybersecurity" provides an outline of the authorities, roles, and responsibilities of US agencies responsible for cybersecurity and recommends modifications that could improve cybersecurity and protect US national security interests.[9] Because of the ease, low cost, and potential anonymity of cyber operations, authors Roesener, Bottolfson, and Fernandez claim that cyber-attacks are as rampant and as dangerous as attacks in the physical domain. They assert that (because of the interconnectedness of the cyber domain) a successful cyber-attack on the United States could affect all aspects of US society. The serious potential for significantly negative impacts on US national interests compels the authors to call for "government preparation and protection in the virtual domain equal to those in the physical domain."[10]

Multiple US agencies are tasked with cyber security-related responsibilities. The Department of Homeland Security (DHS) is the lead agency for the protection of critical infrastructure, both physical and intangible. The Secretary of Homeland Security is responsible for the crisis management and coordination of response to significant cyber incidents.[11] The Department of Justice (DOJ) is responsible for mitigating domestic terrorist threats, investigating incidents, and prosecuting "actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources."[12] The Federal Bureau of Investigations (FBI) operates the National Cyber Investigative Joint Task Force. The National Institute for Standards and Technology (NIST), a non-regulatory agency under the jurisdiction of the Department of Commerce (DOC), sets the standards for the security of critical infrastructure but lacks the authority to impose or enforce cyber standards on the private sector. The Department of Defense (DOD) is responsible for the security of its own critical infrastructure and "when authorized by the president or Congress, conducts activities in cyberspace to defend the United States and its national interests."[13] Within DOD, US Strategic Command (USSTRATCOM) is responsible for cyber operations, US Cyber

Command (USCYBERCOM) is responsible for most cyber capabilities, and US Northern Command (USNORTHCOM) is responsible for planning, organizing, and executing homeland defense missions.

Roesener, Bottolfson, and Fernandez conclude that the above agencies lack the authorities required to allow them to secure and defend cyberspace and may be incapable of adequately performing their assigned tasks. They recommend three modifications to correct the situation and improve the United States' ability to protect its citizens from cyber threats.[14] First, the companies and corporations that make up the defense industrial base (DIB) must incorporate cybersecurity measures that comply with DOD standards. Second, USCYBERCOM should be activated as a fully functional combatant command and be designated as the principal agency for developing and implementing cybersecurity measures across all US government agencies. USCYBERCOM should also be responsible for defending against cyber threats emanating from state-sponsored foreign intelligence agencies. Third, DHS should retain responsibility for physical critical infrastructure, but DHS and USCYBERCOM should have co-ownership and co-oversight of the National Cybersecurity and Communications Integration Center (NCCIC).

NATO Cyber Defense Policy

At the Wales Summit in September 2014 NATO Allies endorsed an enhanced cyber defense policy and corresponding action plan. The new policy confirms that international law applies in cyberspace, recognizes that cyber defense is part of NATO's core task of collective defense, and strengthens Alliance cooperation with industry. Streamlined cyber defense governance, procedures for assisting Allied countries, and the integration of cyber defense into operational planning are included in the policy. Also addressed are ways to foster improvement in cyber awareness, education, training, and exercises. Protection of NATO owned and operated communications systems is the top cyber defense priority. The Alliance is committed to enhanced information sharing and mutual assistance in the prevention, mitigation and recovery from cyber-attacks. NATO assists member countries by working with national authorities to "develop principles, criteria and mechanisms to ensure an appropriate level of cyber defence for national CIS."[15] The Alliance coordinates the sharing of information and best practices, and conducts regular cyber defense exercises. In addition to its member states, NATO also coordinates with the United Nations (UN), the European Union (EU), the Council of Europe (COE), the Organization for Security and Cooperation in Europe (OSCE), and others. NATO's Cyber Defence Policy is implemented by the Alliance's political, military, and technical authorities, and by individual Allies.

INTERNATIONAL CODE OF CONDUCT IN INFORMATION SECURITY

This section looks at the proposed International Code of Conduct in Information Security which was submitted by Russia, China, Tajikistan and Uzbekistan to the United Nations in September 2011. At

present, this "code of conduct" exists solely as a formal letter which was submitted to the UN secretary general and then distributed to the UN member states; it is not a formal international agreement but a document designed to stimulate dialogue on cyber issues. The overview of the Code of Conduct will be followed by a brief discussion about China's unique perspectives on cyber issues.

International Code of Conduct in Information Security

On September 12, 2011 Russia, China, Tajikistan and Uzbekistan submitted to UN Secretary General Ban Ki-moon a proposed International Code of Conduct for Information Security.[16] The Code of Conduct stipulates that nations ascribing to it shall not use information or telecommunications technologies to conduct hostile or aggressive acts or to threaten international peace and security. It upholds that states have both rights and responsibilities to protect critical information from threats, interference and sabotage. The Code of Conduct advocates a) establishing a multilateral, transparent and democratic international governance mechanism, b) respecting the rights and freedom of information and cyberspace while observing laws, c) helping developing countries to develop information and network technologies, and d) cooperation on fighting cybercrime. The purpose and scope of the Code of Conduct involve identifying the rights and responsibilities of states, enhancing cooperation in addressing common threats and challenges, and ensuring that information and communication technologies (ICTs) be used only to the benefit of social and economic development. The objective of the Code is the maintenance of international stability and security. Adherence to the Code is voluntary and open to all states.

Shortly after the International Code of Conduct for Information Security was submitted to the UN, cybersecurity expert Jeffrey Carr identified four "critical flaws" with it and recommended that it be rejected by the United States and its allies.[17] First, Carr maintained that the Code of Conduct does not appear to support international cross-border law enforcement; sections 1 and 5 uphold the importance of territorial integrity and the sovereign right of states to have jurisdiction over their own information space. Second, he surmised that the Code of Conduct supports cooperation mainly in the face of threats posed by dissident political extremists or terrorists. Third, he claimed that section 6 allows states to continue national policies related to censorship while at the same time promoting the freedoms of speech, acquisition and dissemination of information. Fourth, he pointed out that the Code of Conduct does not address cyber espionage. He described the call for banning "information weapons and related technologies" hypocritical because both Russia and China are pursuing their own information warfare commands which are similar to USCYBERCOM.

In January 2015 an updated version of the International Code of Conduct on Information Security was submitted to the UN Secretary General. The updated Code of Conduct takes into account developments which have occurred since the release of the original document, particularly a 2012-2013 UN report titled "Group of Governmental Experts on Developments in the Field of Information and

Telecommunications in the Context of International Security,"[18] and the UN Human Rights Council's internet freedom resolution.[19] The modifications seem to refer to the GGE report in order to support Moscow and Beijing's positions on the concept of "cyber sovereignty" and the need for international laws governing cyberspace. The updated Code of Conduct doesn't involve any changes that would provide any kind of incentive for the United States or its allies to consider it more seriously; the amendments may be intended to appeal more strongly to developing and middle-income countries.[20]

Chinese Perspectives on Cybersecurity

A 2014 US-China Economic and Security Review Commission Staff Report, "China and International Law in Cyberspace," identifies central themes in the Chinese perspective on cyberspace, discusses China's approach to cyberspace in international agreements, and assesses Chinese thoughts on the applicability of international law to cyberspace.[21] There are two main issues that Beijing is unwilling to compromise on: internet sovereignty and information control. China is concerned about what it perceives as a "digital divide" between developed and developing countries. (China considers itself a developing country.) It considers its own cyber capabilities to be a necessary, defensive response to US efforts to militarize cyberspace with offensive capabilities. Beijing perceives the US International Strategy for Cyberspace to be a hegemonic attempt at the militarization of cyberspace. China strongly supports the extension of state sovereignty and non-interference to the cyber realm; it believes that states should not interfere with each other's sovereignty within cyberspace, and that states should be permitted to impose their own national cyber laws on their own nationals, foreign citizens, and organizations physically located within their borders.

The International Code of Conduct for Information Security, on which China partnered with Russia and others, represents China's most significant multilateral contribution to the effort to create norms for cyberspace. The Code of Conduct continues to be part of China's official position. It is unlikely that China will submit to any international agreement that might constrain its ability to reform the current internet infrastructure, which Beijing views as being dominated by the United States. China did not accede to the Budapest Convention on Cybercrime because the Convention did not conform with China's state-centric approach to international cyberspace agreements.

There is evidence to suggest that China does agree, at least in principle, to the general application of international law to cyberspace, including the Law of State Responsibility, concepts in the UN Convention relating to the use of military force, and the Law of Armed Conflict. At same time, there are indications that cyber espionage techniques are utilized by the Chinese Government, the PLA, and state-owned enterprises. Debate is ongoing within China regarding the specific applicability of the Law of Armed Conflict to cyberspace. In contrast to the US position that existing international treaties and norms governing the Law of Armed Conflict should apply directly to cyberspace, China seems to favor

the development of a separate, cyber-specific regime. It is unlikely that Beijing will diverge from its strongly-held position regarding the importance of state sovereignty in the cyber realm.

PATH FORWARD: PROSPECTS FOR A CYBERSECURITY ORDER

There are pessimists and optimists concerning the potential for a future international cyber security order or treaty. This section will look at both perspectives. First, a review of an essay published by the Hoover Institution discusses three challenges which will come into play during the negotiation of a cybersecurity treaty: the non-alignment of interests among states, the problem of mutual concession, and verification difficulties which will complicate international discussions toward a viable cyber agreement.[22] Second, a recent *Strategic Studies Quarterly* article contends that an international cybersecurity regime will eventually be established and that power politics and the evolving international structure will be key factors in its creation.[23]

A fundamental requirement for the widespread adoption of a treaty is that all parties must benefit from it in some way. Because states have different expectations and concerns regarding cybersecurity, it may be difficult to persuade a diverse range of states to agree to a treaty. There is likely to be international disagreement over what, specifically, the problem is and what types of cyber practices should be restricted or forbidden. Some states (such as China and the United States) may even disagree about the importance of preserving the fundamentals of intellectual property protection, freedom of speech, and free access to information. Some states may be unwilling to accept restrictions on certain cyber activities. US adversaries "might think they gain relatively little from a cybersecurity agreement to refrain from using offensive weapons."[24] In addition to agreeing on the benefits of a cybersecurity agreement, parties must also agree on what does and doesn't count as cooperation with such an agreement. Distinctions regarding what is and isn't permitted must be precisely defined in order to avoid misinterpretations, and the nature of cyber activities may make it difficult to accurately define the characteristics of cyber weapons, effects, and targets.

An ideal cybersecurity treaty, from an American perspective, would benefit and protect the United States by restricting malicious cyber activity perpetrated by US adversaries. The problem, according to author Jack Goldsmith, is that this assumes "(a) the United States is a major victim of the cyber threat rather than a part of the problem, and (b) American cyber activities abroad are legitimate, while those of adversaries in the United States are not."[25] The reality is that other states perceive the United States to be a source of cyber-attacks and exploitation, and therefore a reason to pursue or maintain their own offensive cyber capabilities. A viable cybersecurity treaty would require the United States to make difficult concessions regarding its own cyber activities – which it may not be willing to do.

For instance, a treaty that bans cyber espionage may be unpalatable because the United States depends heavily on electronic means of gathering intelligence.

Reliable means of verification will be indispensable in any cybersecurity treaty. Unfortunately, verification in the cyber realm is extremely difficult. Timely and accurate attribution of offensive cyber activities is exceedingly challenging. Uncertainty regarding the perpetrator of a cyber-attack makes it difficult to hold a specific actor responsible. Goldsmith maintains that an effective cyber verification regime would be both controversial and expensive; it would require extensive government monitoring of activity in private networks and could raise substantial Fourth Amendment concerns.[26] Even with a great investment of capital, no state could reasonably expect to prevent – or even investigate – all malicious cyber activity within its borders. Goldsmith concludes that a practicable cyber security treaty is unfeasible due to the divergence of interests concerning regulation, the deep constraints the United States would have to accept in order to receive reciprocal benefits, and the substantial problems associated with effective verification.

The authors of *Strategic Studies Quarterly* article "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace," provide a more optimistic outlook regarding an eventual establishment of a cybersecurity regime. James Wood Forsyth Jr. and Maj. Billy E. Pope (USAF) contend that international order within cyberspace is inevitable and maintain that power politics and international structure are key factors in the establishment of a cybersecurity regime. The problem, they claim, lies not with the "extraordinary nature of cyberspace" but with the "rather ordinary connection between political structure and order."[27] Structural disagreement at the international level has contributed to the challenges associated with the establishment of a cybersecurity regime. However, the structure of international politics is changing. The current unipolar structure is steadily giving way to a multipolar one and, as this shift occurs, dependencies on sea, air, space and cyber assets and capabilities will intensify. [28] As the world becomes more interconnected, the security and prosperity of each state will be contingent on the security and prosperity of other states, incentivizing great powers to cooperate more closely with each other, particularly regarding cybersecurity.

Two thoughts are offered by Forsyth and Pope regarding the effects that the changing international landscape will have on cyberspace. First, an international order within cyberspace will evolve, but it will not necessarily guarantee harmony. As with other international regimes, there will likely be disagreement, cheating, and some states may even choose to withdraw from the regime. Second, there is no way to predict what the normative nature of the regime will look like. It may be one that promotes democracy or it may resemble a "digital 'Iron Curtain.'"[29] One thing is for certain, activities in cyberspace will continue to affect domestic and international politics in a substantial way, not the least in the realm of economics. With globalized markets for services and goods, the prospect of "living off the

grid" is becoming untenable for developed and developing economies alike.[30] Cyberspace affects *all* states; therefore every state has an interest in cybersecurity. The authors maintain that states will have no choice but to work collectively toward an international cyber order.

Forsyth and Pope reflect on the development of the nuclear arms control regime and draw connections to the eventual establishment of a cybersecurity regime. The concept of mutual vulnerability precipitated the conditions necessary for the nuclear states to develop "rules, norms, and standards of behavior that brought order to what was highly contested and valuable terrain."[31] These rules and norms were not established instantly, but "evolved as global power became more divided among the superpowers and as ideas and practices orbited within the minds and habits of concerned scientists and practitioners."[32] The authors maintain that a similar set of scholars and policymakers is in place today that can set the stage for the establishment of a cybersecurity regime. While a cybersecurity regime would not eliminate all of the risks and challenges associated with cyber activity, it would provide states with some means to mitigate many cyber-related challenges. Like the arms control regime, a cybersecurity regime would create rules and norms which would mitigate uncertainty, strengthen legal liability, and reduce transaction costs related to the use of cyberspace.

CONCLUSION

The establishment of an international regime regulating cybersecurity is important for the future of the international security environment and the security of all states that operate within it. Cybersecurity affects every nation on earth and is integral to the success of global commerce in the modern era. The threats and challenges associated with the cyber domain will not dissipate on their own but will continue to evolve; it is critical that the issue be met head on by a determined international effort to secure cyberspace for the good and prosperity of all involved. The process will certainly be complicated and time consuming. There will be disagreement between states regarding the specific nature of the threat, levels of state authority and responsibility, and the implications for state sovereignty. The problem of establishing viable means of verification of compliance will be challenging. Multiple levels of coordination will need to be established, including interagency coordination within states, coordination between allies and partners, and global coordination and cooperation. Despite the difficulties associated with the formation of a global cybersecurity regime, it is likely that such a regime will ultimately be achieved. International norms do not develop overnight. Progress may be slow and incremental, but eventually the pieces will come together and the international community will unite in support of a mutually beneficial cyber agreement.

ENDNOTES

[1] Gregsby, Alex, "Coming Soon: Another Country to Ratify the Budapest Convention," Council on Foreign Relations, Net Politics Blog, December 11, 2014, http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/.

[2] Seger, Alexander, "The Budapest Convention on Cybercrime 10 Years On: Lessons Learnt or the Web is a Web," Council of Europe, February 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf.

[3] *Ibid*, 25

[4] *Ibid*, 8

[5] "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress," Congressional Research Service.

[6] *Ibid*, 5-6

[7] *Ibid*, 8

[8] *Ibid*, 16-17

[9] Roesener, Lt Col August G., Maj Carl Bottolfson, and DCR Gerry Fernandez, "Policy for US Cybersecurity," *Air & Space Power Journal*, November-December 2014.

[10] *Ibid*, 39

[11] *Ibid*, 42

[12] *Ibid*, 43

[13] *Ibid*, 45

[14] *Ibid*, 46-50

[15] NATO Policy on Cyber Defence, http://www.nato.int/cps/en/natohq/topics_78170.htm.

[16] "International Code of Conduct for Information Security," United Nations. General Assembly. *Letter dated 12 September 2011 from the Permanent Representatives of China the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359. New York: United Nations, 14 Seotenber 2011.

[17] Carr, Jeffrey, "4 Problems with China and Russia's International Code of Conduct for Information Security," Digital Dao, September 22, 2011, http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html.

[18] United Nations, http://www.un.org/ga/search/view_doc.asp?symbol=A%2F68%2F98&Submit=Search&Lang=E.

[19] United Nations, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf.

[20] Grigsby, Alex, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Council on Foreign Relations, Net Politics Blog, January 28, 2015, http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/.

[21] Hsu, Kimberly, and Craig Murray, "China and International Law in Cyberspace," US-China Economic and Security Review Commission Staff Report, May 6, 2014.

[22] Goldsmith, Jack, "Cyber Treaties: A Skeptical View," Hoover Institution, Stanford University, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

[23] Forsyth Jr., James Wood, and Maj Billy E. Pope, "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace," *Strategic Studies Quarterly*, Winter 2014.

[24] Goldsmith, 5.

[25] *Ibid*, 7.

[26] *Ibid*, 8.

[27] Forsyth and Pope, 118.

[28] *Ibid*, 120.

[29] *Ibid*, 121.

[30] *Ibid*, 122.

[31] *Ibid*, 124.

[32] *Ibid*, 124-125.