MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

# Perspectives on Cybersecurity:
# A Collaborative Study

Massachusetts Institute of Technology:

Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz


Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

# PERSPECTIVES on CYBERSECURITY

## A Collaborative Study

**Authors**

*Chrisma Jackson*

*Lyla Fischer*

*Brooke Gier*

*Vivian Peron*

*Ben Ze Yuan*

*Liu Yangyue*

*Glenn Voelz*

**Editors**

*Nazli Choucri*

*Chrisma Jackson*

**Department of Political Science**

**MIT**

**2015**

# Table of Contents

# 3. The Conceptual Underpinning of Cyber Security Studies

## Liu Yangyue

Technology is often a driving force in the transformation of the international system. Over the past two decades, such transformative power has been best manifested in the development of information technologies, which are adjusting and reshaping the "interaction capacity" of human society.[6] An important part of this change occurs in the security domain. Development of the Internet and related technologies has empowered new political actors, fostered new patterns of interactions, and also opened up new venues for threats and conflicts. This security aspect of cyber politics becomes even more salient, as human reliance upon cyberspace intensifies. How the advent of cyberspace influences the meaning and conduct of security practices has sparked increasing academic interest and increasing discussion since 2007 (Figure 1).

There are abundant discussions in security studies and international relations about the emerging risks and challenges associated with cyberspace. However, partly due to the complexity of the new socio-technological system, little consensus has been reached on what constitutes cyber security. On this score, Hansen and Nissenbaum pointedly remarked that "in spite of the widespread references to cyber insecurities in policy, media, and Computer Science discourses, there has been surprisingly little explicit discussion within Security Studies of what hyphenating 'security' with 'cyber' might imply".[7]

Therefore, this review attempts to examine the burgeoning literature on cyber security, mainly from an international security study (ISS) perspective. ISS represents a research field that concerns different types of actors, as well as different levels of policy responses, in international politics. The emergence of cyber security issues adds a new, yet important, dimension to this field. But, it also raises a serious question of how this unprecedented cyber phenomenon should be conceptualized and measured.

[6] Barry Buzan, Charles Jones, and Richard Little, *The Logic of Anarchy: Neorealism to Structural Realism* (New York: Columbia University Press, 2009)
[7] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (2009): 1156.

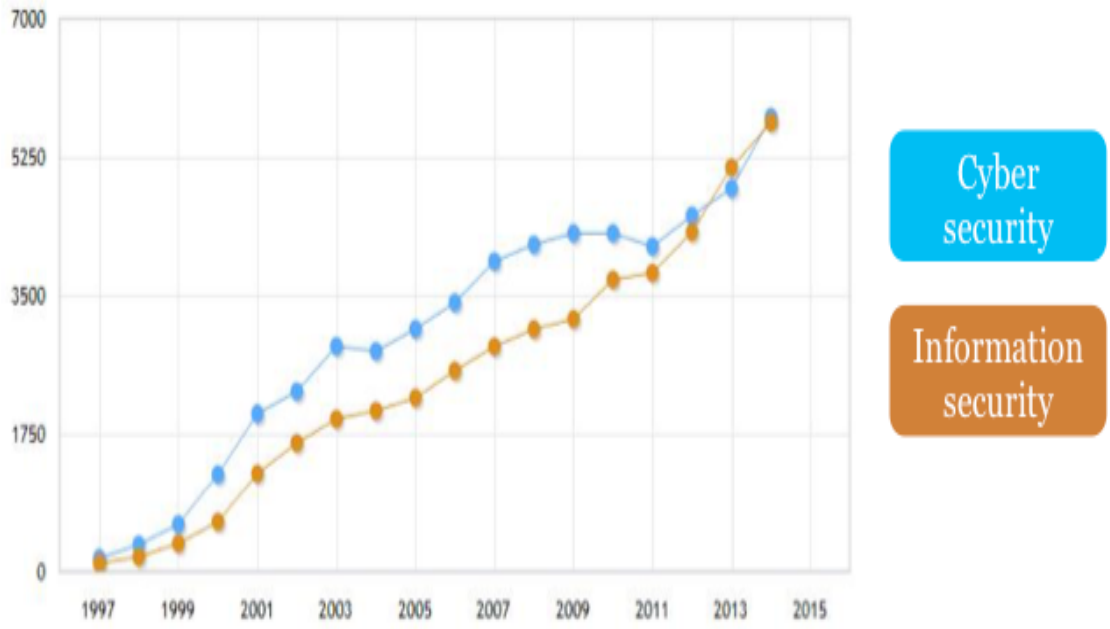


**Figure 3.1**
**Burgeoning Discussions on Cyber Security**

## 3.1 Cyber Security in the Broad Context of International Security Studies

Starting from the later years of the Cold War, the discipline of international security studies has experienced a dual shift on its agenda.[8] On the one hand, the previously narrow focus on military-political security is expanded to include other sectors such as economic security and environment security. The 1994 *Human Development Report* published by the United Nations Development Programme suggested that the scope of global security should be extended to threats from economic, food, health, environmental, personal, community and political areas.[9] It also identified the significant linkage between development and security, thus broadening the conceptual boundary and policy orientations of security studies.[10] Accompanying these "widening" efforts is a growing list of non-traditional threats and risks such as terrorism and global pandemics. Security problems caused by the use of computers and digital networks make their appearance on that list, too.

Although these problems were considered purely technical at the beginning, the increasingly intertwining relationship between cyber domain and other sources of threats – both traditional and non-traditional – has attached much greater significance to cyber security.[11] Meanwhile, the constructed notion of cyberspace, with an imagined resemblance to other geographic space (sea, air,

[8] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009).
[9] United Nations Development Programme, *Human Development Report* (New York: Oxford University Press, 1994).
[10] Caroline Thomas, "Global Governance, Development and Human Security: Exploring the Links," *Third World Quarterly* 22 (2001): 159-175; Pauline Ewan, "Deepening the Human Security Debate: Beyond the Politics of Conceptual Clarification," *Politics* 27 (October) 182-189.
[11] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?," *International Political Science Review* 27 (2006): 221-244.

outer space etc.), implicates a perceivable domain that can be both target and source of security risks.[12] As noted by Buzan and Hansen, technological changes and key events are among the major driving forces of security studies.[13] Similar mechanisms may also apply to cyber security. In this sense, the meaning of security in cyberspace would not remain static, subject, instead, to the dynamics of technological development and unforeseen circumstances.

On the other hand, "wideners" of international security studies are joined by "deepeners" who stress the need to move beyond the nation-state as the sole "referent object" of security. The critical question of "security for whom" highlights vulnerabilities of non-state entities – individuals, groups, communities – who suffer violence from various levels of threats. By extending security objects vertically, it should be regarded as an integral part of the human security narrative as well as the security-development nexus.[14] In addition, this approach indicates that providers of security services become multiplied and security is not a public good offered and realized only by the state apparatus.[15] Again, discussions on cyber security parallel and exemplify these "deepening" efforts. As interactions in and through cyberspace effectively connect all levels of actors and systems, it is difficult to speak of security without referring to users, corporations, organizations, processes, and systems, all of which, alongside states, are essential components, and thus security objects, of cyberspace. New modes of security governance also take shape, delegating power from traditional, hierarchical structure to networked, decentralized collaboration.[16]

Therefore, the perceptions of cyber security issues have, in general, conformed to the evolution of international security studies. But it also means that the process of knowledge generation on cyber security would be influenced by existing vocabularies, theories, frameworks and mindsets of international security studies, yet leaving the validity of such "concept travelling" unexplored.[17] Typical examples can be found in the coined terms such as "cyber war" and "cyber weapon", or in the biological analogies of computer viruses and worms.[18] Still under debate is to what extent these metaphors can deliver accurate connotations to cyber-related phenomenon.

## 3.2 Sources of Cyber Threats

Despite its various meanings, security is foremost understood as the status or value of being free from threats.[19] As Ullman put it, "we may not realize what it (security) is or how important it is until we are threatened with losing it".[20] As a result, defining security often pertains to identifying and describing threats that challenge it.

---

[12] Ronald Deibert and Rafal Rohozinski, "Risking Security: The Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4 (2010): 15-32.
[13] Buzan and Hansen, *The Evolution of International*, 53-57.
[14] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 2009); Gary King and Christopher Murray, "Rethinking Human Security," *Political Science Quarterly* 116 4 (2001): 585-610; Maria Stern and Joakim Öjendal, "Mapping the Security-Development Nexus: Conflict, Complexity, Cacophony, Convergence?," *Security Dialogue* 41 (2010): 5-29.
[15] Lucia Zedner, *Security*, (London: Routledge, 2009).
[16] Milton Mueller, Andreas Schmidt, and Brenden Kuerbis, "Internet Security and networked Governance in International Relations," *International Studies Review* 15 (2013): 86-104.
[17] Giovanni Sartori, "Concept Misformation in Comparative Politics," *American Political Science Review* 4 (1970): 1033-1053.
[18] Thomas Rid, *Cyber War Will Not Take Place*, (Oxford: Oxford University Press, 2013); David J. Betz and Tim Stevens, "Analogical reasoning and cyber security," *Security Dialogue* 44 (2013): 147-164.
[19] Arnold Wolfers, ""National Security" as an Ambiguous Symbol," *Political Science Quarterly* 67 (1952): 481-502; Richard H. Ullman, "Redefining Security," *International Security* 8 (1983): 129-153.
[20] Ullman, "Redefining Security," 133.

The understanding of cyber security starts with a similar pattern. When the earliest known computer virus (codenamed Morris Worm after its programmer) infected thousands of computers in the United States and overseas, a report by US General Accounting Office (1989) several months later warned the government of the security vulnerabilities exposed by the Internet virus and other intrusions. The first Computer Emergency Response Team was established immediately after the incident, with one of its major functions being the provision of "mechanisms for coordinating community response in emergencies, such as virus attacks or rumors of attacks".[21] During those early days, the primary concern of cyber-related security centered on the potential loopholes of computer systems, which might lead to loss or leakage of computer data and problems of computer crime.[22] The same vulnerability that permitted a virus attack by malicious individuals was thought to be likely exploited by terrorists and foreign nations. In this regard, the US National Academy of Sciences cautioned in 1991 that "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".[23] Though visionary, these accounts fell short of presenting any detailed scenario of a future threat.

The National Institute of Standards and Technology, in its 1995 *Introduction to Computer Security*, further specified nine types of security threats, including errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage, malicious code, foreign government espionage, and threats to personal privacy. It mainly underscored the risk of interception of, or illegal access to, digitized data, while pointing to various kinds of perpetrators.[24] As the development of information technologies fosters greater penetration of the Internet into human society, perceptions of cyber threats naturally expand, and the relatively narrow sense of computer security evolves into a more inclusive notion of cyber security.

Accordingly, sources of security threats proliferate. Now cyber security is seen as encompassing a host of problems, such as spamming and phishing, unauthorized intrusions, denial-of-service attacks, website defacements, online surveillance, unintended bugs in protocols and systems, as well as the intersection with military and political threats.[25] The list of cyber threats is largely expandable, especially as new threats emerge from the increasingly digitalized and interconnected physical domain. Examples include security concerns to the cyber-physical systems, supervisory control and data acquisition (SCADA) networks, and even unmanned aerial vehicles (UAVs).[26] Some

---

[21] Jason Healey and Karl Grindal, eds., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013.

[22] Myriam Dunn Cavelty, "Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology and Politics* 1 (2007): 24.

[23] National Academy of Sciences, *Computers at risk: Safe computing in the information age* (Washington, DC: National Academy Press, 1991).

[24] Barbara Guttman and Edward Roback, *An Introduction to Computer Security: The NIST Handbook* (Gaithersburg, MD: U.S. Department of Commerce, 1995).

[25] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 97-108; Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010); Ronald Deibert, "The Growing Dark Side of Cyberspace(…and What To Do About It)," *Penn State Journal of Law and International Affairs* 1 (2012): 260-274; Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 11-12; Brandon Valeriano and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research* 51 (2014): 353-354.

[26] Md E. Karim and Vir V. Phoha, "Cyber-physical Systems Security," in *Applied Cyber-Physical Systems*, ed. Sang C. Suh, U. John Tanik, John N. Carbone, and Abdullah Eroglu (Switzerland: Springer, 2014); Eric Knapp and Joel T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Gride, SCADA, and Other Industrial Control Systems*, (Rockland, MD: Syngress Publishing, 2011); Kim Hartmann and Christoph Setup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," in *5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013).

studies contribute to the threat list by identifying specific means or tools used in particular incidents.[27] These threats appear to be progressively advanced and persistent, as they employ complicated techniques and operate in a long-term, systematic manner.[28] Myriam Dunn Cavelty further distinguished among three clusters of cyber threats: a technical cluster that concentrates on malware, a socio-political cluster that captures various human wrongdoings, and a human-machine cluster that produces threats through complex interactions.[29] But, the problem of overlap (especially between the socio-political cluster and the human-machine cluster) that this classification intends to address remains, to some extent, unabated.

A key difference among these various forms of cyber threats lies in their levels of severity (or intensity). It often argues that cyber threats can be classified according to the damage incurred, methods and actors involved, and motivations behind.[30] Thus, the mapping of cyber threats usually points to a spectrum with unintentional failures (such as software or system errors) – assumed as the least dangerous – at one end, and full-blown, strategic cyber warfare – perceived as the most destructive and destabilizing – at the other. In between the extremes are malicious activities initiated by criminals (in the name of cyber crime), spies (cyber espionage), terrorist groups (cyber terrorism), or other political organizations (cyber conflict)[31]. Though not articulated as direct security threat, cyber conflict also exists in political contention over the designing and management of cyberspace and its resources.[32] The gradual politicization of such contention would likely produce security implications for the relevant actors. On the military side of the cyber-threat continuum, differentiation can still be made among enabling operations (activities relating mostly to reconnaissance and intelligence collection), disruptive operations, and outright cyber attacks.[33]

The internal logic common in these efforts shares great similarities with Charles Tilly's seminal work on collective violence, which highlights (a) damage caused by and (b) degree of organized coordination among violent participants.[34] That said, classifying cyber threats by mapping a spectrum suffers several drawbacks. Firstly, threats and conflicts in a cyber context often involve a mixture of stakeholders.[35] It is difficult, for instance, to properly place attacks initiated by state actors against non-state actors (and vice versa) on a continuum, let alone those initiated by a combination of actors or involving ambiguous, mysterious cyber militias. The proliferation of political actors in cyberspace and the problem of attribution have, to some extent, blurred the division of cyber crime, terror, and

---

[27] James P. Farwell and Rafa Rohozinski, "Stuxnet and the Future of cyber War," Survival 53 (2011): 23-40; Christopher R. Hughes, "Google and the Great Firewall," *Survival* 52 (2010): 19-26.
[28] Mandiant, APT1: Exposing One of China's Cyber Espionage Units (2013): http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; James A. Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage," Center for Strategic & International Studies Report (2014).
[29] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15 (2013) 108-109.
[30] Jan-Frederik and Benedikt Müller, "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik and Benedikt Müller (Switzerland: Spring 2014) 45-51.
[31] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008) 20; Paul Cornish, Rex Hughes, and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (London: Chatham House, 2009); Nicholas Thomas, "Cyber Security in East Asia: Governing Anarchy," *Asian Security* 5 (2009): 3-23; Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012); M.A. Gregory and David Glance, *Security and the Networked Society* (Switzerland: Spring, 2013).
[32] Laura DeNardis, *Protocol Politics: The globalization of Internet governance* (Cambridge, MA: The MIT Press, 2009); Choucri, *Cyberpolitics*, 126.
[33] Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operatins," *Small Wars Journal* December 11 (2012) http://smallwarsjournal.com/print/13595.
[34] Charles Tilly, *The Politics of Collective Violence* (Cambridge: Cambridge University Press, 2003).
[35] Kremer and Müller, "SAM", 44.

war. Secondly, while war represents the most destructive form of violence, current exercises of "cyber war" may qualify, more precisely, as forms of sabotage, espionage and subversion.[36] Meanwhile, cyber crimes inflict, so far, heaviest and most immediate harm on businesses and customers.[37] This calls into question the order of severity used as the criteria of a cyber threat spectrum. Last but not least, even among cyber threats involving distinctive clusters of actors and motives, methods and tools may still overlap. For instance, distributed denial-of-service (DDoS) attacks are found in all levels of cyber conflict, with botnets and other toolkits widely available in an underground economy.[38] Therefore, although pointing out the mounting sources of cyber threats would help to illustrate the diverse scenarios of security risks, it is still inadequate for a comprehensive understanding of the nature and characteristics of cyber security. A linear spectrum of cyber threats is problematic since it often relies on only one or two dimensions of threats (e.g. actors or severity), while leaving other dimensions (e.g. targets and intentions) and the intertwining effects among them unaddressed.

## 3.3 Boundary of Cyber Security

The notion of security often connotes a target at stake, be it a nation, a community, an individual, an asset, or anything else perceptible. The principal referent object – as securitization theory phrases it – of cyber security points to an artificial and imagined aggregation that connects human, information and machine through digital networks.[39] The coinage of cyberspace gives the collective objects a sense of reality and spatiality, albeit still virtual in nature, thus bringing it closer to the defense and protection narratives.[40] "When thinking about warfare, hackers, pornography, fraud, and other threats to the rule of law that pass through the internet", as Graham argues, "it is challenging to fully understand the complex geographies of these processes and practices.[41] It is much easier to imagine that they simply happen 'out there' in Carl Bildt's dark spaces of the internet". In this sense, the "consensual hallucination" of cyberspace is indeed a fundamental component of cyber security conceptualizations.[42]

However, when referring to cyberspace, studies on cyber security do not always share an identical, unambiguous definition. It is seldom a question that the ecological structure of cyber security consists of different levels (layers) of interactive dimensions. But disagreement arises, explicitly or implicitly, as to the exact composition of that structure. A dichotomous approach emphasizes the virtual-physical distinction of cyberspace, and the different (or even contradictory) security implications that result from its dual properties.[43] When cyberspace is used as the referent object of security, it primarily centers on the material domain – especially critical infrastructure – that suffers security risk and necessitates protection. Deibert and Rohozinski made a step forward by identifying "risks through cyberspace", which underscores the political challenges generated by activities in cyberspace.[44] These risks, composed of "resistance networks" and "dark nets", expand the

[36] Rid, *Cyber War*.
[37] Symantec, *Internet Security*.
[38] Jaideep Chandrashekar, Steve Orrin, Carl Livadas, and Eve Schooler, "The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware," *Intel Technology Journal* 13 (2009) 130-147; Farwell and Rohozinski, "Stuxnet", 23-40.
[39] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security*.
[40] Julie E. Cohen, "Cyberspace as/and Space," *Columbia Law Review* 107 (2007): 210-256.
[41] Mark Graham, "Geography/Internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities?," *The Geographical Journal* 179 (2013): 179.
[42] William Gibson, *Neuromancer* (New York: Ace Books, 1984).
[43] Deibert and Rohozinski, "Risking Security," 15-32; Joseph S. Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5 (2011): 18-38.
[44] Deibert and Rohozinski, "Risking Security," 21-24.

referent objects of security from cyberspace to the broad socio-political order outside the cyber domain.

Other studies focus on cyberspace per se by dividing it into functional layers, but they still differ in how far these layers stretch. For instance, Libicki's trichotomy model of cyberspace posits a structure of the "physical" layer (primarily interconnected computers), the "syntactic" layer (software and protocols) and the "semantic" layer (information).[45] This structure would be both narrow and extensive when compared with other conceptions. Some of them regard cyberspace mainly as a technical system, thus merely focusing on the hardware and logical layers.[46] It is also narrow, since a broader structure of cyberspace may include the human/people dimension pertaining to the users of cyberspace, and the physical layer may not be restricted to digitally-connected computer systems.[47] Even air-gapped systems could be vulnerable to cyber attacks, and thus be considered as part of the cyber domain.[48] Moreover, in regard to the information layer, it would be crucial to distinguish between code and content of information. The latter often points to the perceptual aspect of human brain. It largely stretches the boundary of cyberspace to cover the subjective dimension associated with ideas, beliefs, and values.[49]

In general, there are two separate lines of boundary that govern the divergent conceptualizations of cyber security. One axis moves along the distinction between globalized space and imagined national boundary. The national side of this line of thinking does not necessarily end up with asserting national sovereignty over cyberspace, but it implicitly or explicitly portrays nation-states as the core referent object. Crucial factors that sustain the national image of cyber security point to the physical infrastructure of cyberspace which still operates within national borders, as well as the fundamental roles of territorial government that persist in the cyber domain.[50] The tendency to confine cyber security analysis within a state-centric framework is prevalent in studies from a strategic perspective, and evident in the documentation of national cyber security strategies outlined by a growing number of countries. On the other hand, cyber security represents a novel global issue that occurs in a new arena of interactions.[51] Norms, practices, and institutions that manage security problems in the cyber domain have been fundamentally transformed due to the globalized feature of the cyber system.[52] In this sense, confining discussions on cyber security within a national framework would be counterproductive, and the global governance of cyberspace indicates the de facto elimination of cyber security boundary. Meanwhile, the other line of conceptual boundary moves along the distinction between code and value that transmit in and through cyberspace. In general, stress on the code tends to highlight the technical system of cyberspace, while stress on the value tends to

[45] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007).
[46] Kelce S. Wilson and Muge Ayse Kiy, "Some Fundamental Cybersecurity Concepts," *IEEE Access* 2 (2014): 116-124.
[47] Nazli Choucri and David Clark, Cyberspace and International Relations: Toward an Integrated System," Paper presented at Massachusetts Institute of Technology, Cambridge, MA: August 25, 2011; Shmuel Even and David Siman-Tov, "Cyber Warfare: Concepts and Strategic Trends," *The Institute for National Security Studies Memorandum* 117 (2012).
[48] Scott Applegate, "The Dawn of Kinetic Cyber," Presented at the *5th International Conference on Cyber Conflict*, Tallinn June 4-7, 2013.
[49] Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *4th International Conference on Cyber Conflict,* ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2012), 63-77.
[50] David Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119 (2004): 477-498; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006).
[51] Choucri, *Cyberpolitics*.
[52] John Mathiason, *Internet Governance: The New Frontier of Global Institutions* (London: Routledge, 2008); Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development* (2013): DOI: 10.1080/02681102.2013.836699.; Mueller, Schmidt, and Kuerbis, "Internet Security".

underscore the social and political interactions embedded in the various processes that underpin cyber domain. Accordingly, four approaches to cyber security can be differentiated (Figure-2)

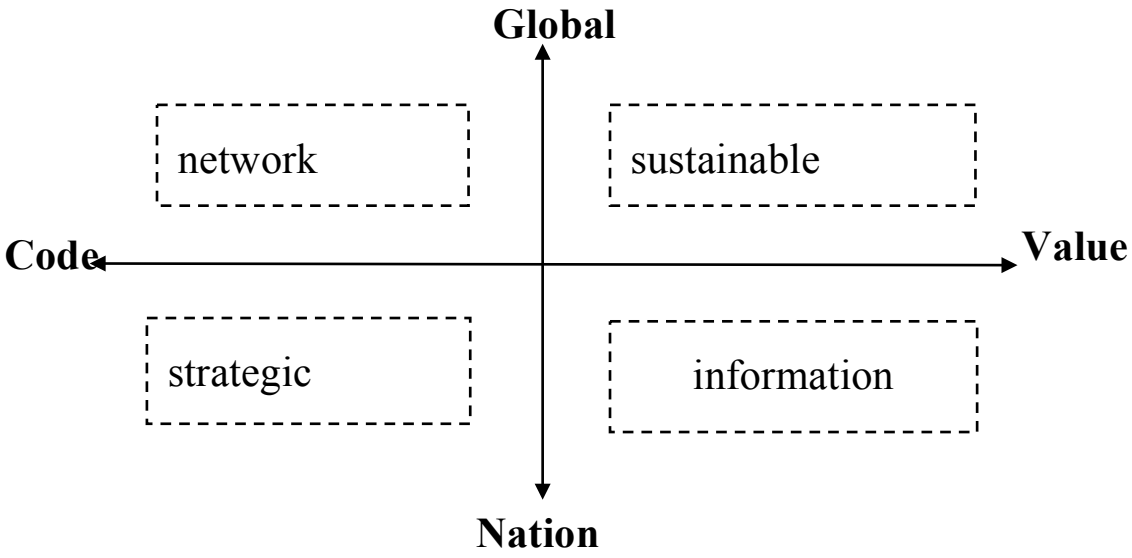


**Figure 3.2**
**Approaches to cyber security**

*Network security* in the upper left quadrant stresses the connectivity of cyberspace which is created through networked terminals and enabling technologies. The core for protection is a globalized network (global commons), which often calls for a horizontal (bottom-up) approach of security governance. By contrast, *strategic security* also underscores the connectedness of cyberspace, but at stake are national assets connected to the cyber domain. In this narrative, the foremost threat is malicious code used by state or non-state actors with strategic and political objectives. It pays special attention to the expanding intersection between cyberspace and military/strategic affairs. In the upper right quadrant, *sustainable security* focuses on the global system of cyberspace, but from a perspective highlighting distribution and development. The developmental objectives of human society are seen as being associated with the development and management of information sphere. This perspective is concerned with how cyber interactions are shaped by and regenerating, in return, human values. In this sense, management of cyber security should mitigate risks resulting from collisions between different values and interests. In *information security*, people and society within a nation-state define the boundary of cyberspace. It is focused primarily on the content and values embedded in information flows. The proposed response to cyber security often calls for regulations and norms on information content and human behavior. The existence of two separating lines (national-global and code-value) used to delineate cyberspace has, in some measure, enriched but also complicated our understanding and conceptualization of cyber security.

Moreover, the boundary of cyber security becomes further clouded as the result of international

power politics. It was observed in 2013 that the number of countries with more-or-less militarized cyber security programs had risen to 47.[53] Six of them publicly released their military cyber strategies, while another 30 expressed cyber security concerns in various national defense documents. However, these national strategies and policies diverge in their conceptualizations of cyberspace and cyber security. The most obvious contention can be found between Euro-Atlantic countries on the one hand, and countries such as Russia and China on the other.

The US Department of Defense defines cyberspace mainly by its technological (hardware) components, which describes the cyber domain as "the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[54] By contrast, Russia and China regard cyberspace as an integrated part of information space, where human cognitive processes interact with all kinds of information. Therefore, cyber security should not be separated from information security that deals with information systems as well as human minds.[55] It should also be noted that even within the West, definitions of cyber security might still vary. For example, while the UK's cyber security strategy "places the logical layer (of cyberspace) at its center", the German counterpart adopts a narrow focus on "the virtual space of all IT systems linked at data level on a global scale".[56]

The unnerving implication is that these divergent national perspectives on cyber security may get entangled with political contention at the international level, which could in turn inhibit conceptual harmonization (academic and diplomatic alike) across different settings.[57] On this score, scholars from the US and Russia have engaged in a track-two effort to clarify cyber-security-related terminology and build a common perceptual foundation.[58] However, the outcome so far is not as promising as it aims. Giles and Hagestad critically pointed out that "the agreed definitions in each language did not actually match up with each other, leaving each side under the impression that consensus had been achieved but in fact remaining as far apart as ever".[59]

With regard to international organizations, the issue of cyber security has been on the agenda of the UN's General Assembly (both the First and the Second Committee) as early as 1998. But none of the resolutions approved as the result of these discussions offered clear definition of cyber security.[60] By contrast, the International Telecommunications Union (ITU) issued in 2008 an "Overview of Cybersecurity". It conceptualized cyber security as the combination of instruments, policies, norms, practices, institutions and technologies "that can be used to protect the cyber environment and

---

[53] James A. Lewis, "Cybersecurity and cyberwarfare: assessment of national doctrine and organization," in *UNIDIR: The Cyber Index: International Security Trends and Realities* (New York: United Nations, 2013).
[54] U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms* (2010): http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
[55] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013) https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf
[56] Even and Siman-Tov, "Cyber Warfare," 12.
[57] Alexander Klimburg, "The Internet Yalta," *Center for a New American Security Commentary* (2013): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf
[58] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher, and Valery Yaschenko, eds. 2011. *Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2*. New York: East West Institute and the Information Security Institute of Moscow State University. http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf
[59] Giles and Hagestad, "Divided by a Common".
[60] Roxana Radu, "Power Technology and Powerful Technologies – Global Governmentality and Security in the Cyberspace," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Switzerland: Springer, 2013).

organization and user's assets".[61] In addition to its ambiguous wording, this definition could be too inclusive to maintain any operational value. In fact, both the absence and the ambiguity of cyber security concepts in the above-mentioned documentation have probably reflected the politicization of framing cyber security within the international society.

## 3.4 Cyber Security as a Social Construct

Although the issue of cyber security has become a hot topic in security studies, discussions above demonstrate that a consensus has not been reached on precise meanings of relevant terms. It has been argued that current conceptualizations of cyber security are excessively broad and obscure in terms of the targets of cyber threats and the threats per se.[62] The conceptual basis of cyber security is further influenced by global political dynamics, since the framing of cyberspace and security problems has direct implications for the principles and institutions of global governance architecture.[63]

This point suggests the importance of the way in which security is constructed by socially interactive perceptions and debates. In this sense, security should be understood not only as an objective condition, but also as an intersubjective product of social construction.[64] Instead of focusing on the material aspects that constitute security, the constructive approach, especially the securitization theory, examines the process that specific "securitizing actors" effectively frame and present a security threat to their audience.[65] Meanwhile, the trajectory of that process is not randomly determined. Rather, different security sectors may involve particular threat agenda and feature distinct patterns of securitization.

Against this backdrop, the framework of securitization theory also sheds light on the discursive (intersubjective) dynamic that constructs cyber security. Accordingly, a number of studies have examined the internal mechanisms that shape cyber threat images, the alarming policy implications due to exaggerated cyber threat rhetoric, as well as perceptual foundations for international cyber security cooperation.[66] Although the primary objective of these studies is not to build a coherent definition for cyber security, they greatly contribute to our understanding of cyber security concept in at least two aspects. Firstly, they highlight the fact that discussions on cyber security are embedded in a web of threat discourse. Distinct strains of discourse can be identified by different actors who hold particular perspectives on cyber security and different models of reasoning used to portray and project cyber threats in particular manners. For instance, actors from a technical background may be more likely to depict cyber security problems as incidents stemming from the internal complexity of

[61] International Telecommunication Union, *Overview of Cybersecurity RecommendationX.1205*, https://www.itu.int/rec/T-REC-X.1205-200804-I.
[62] Dunn Cavelty, "Cyber-Terror-Looming Threat," 28.
[63] David Drissel, "Internet Governance in a Multipolar World: Challenging American Hegemony," *Cambridge Review of International Affairs* 19 (2006): 105-120; Klimburg, "The Internet Yalta".
[64] Michael C. Williams, "Words, Images, Enemies: Securitization and International Politics," *International Studies Quarterly* 47 (2003): 513.
[65] Buzan et al., "Security: A New Framework".
[66] Ronald Deibert, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, ed. J.P. Singh and james N. Rosenau (New York: Suny Press, 2002), 115-142; Dunn Cavelty, "Cyber-Terror-Looming Threat"; Hansen and Nissenbaum, "Digital Disaster"; Betz and Stevens, "Analogical reasoning"; Dunn Cavelty, "From Cyber-Bombs"; Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011): 39-84; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10 (2013): 86-103; Nicholas Thomas, "Cyber Security"; Agnes Kasper, "The Fragmented Securitization of Cyber Threats," in *Regulating eTechnologies in the European Union: Normative Realtities and Trends*, ed. Tanel Kerikmäe (Switzerland: Springer, 2014), 157-187.

networked systems, thus implicating actions that would de-politicize security issues.[67] In contrast, strategic discourse may pay much attention to, and articulate on, unforeseen risks that could lead to political instability and even a cyber catastrophe. Due to the existence of "multi-discursivity" and competing threat images of cyber security, it would be rather difficult to achieve a precise, parsimonious and undisputable concept for all cyber stakeholders.[68] But, it would be also important to find a way to bridge the gap among divergent discourses and practices, and build a knowledge platform where discourses and conceptualizations of cyber security could converge.

This leads to the second aspect: studies on cyber securitization can be seen as a collective effort to systematically explore and establish the linkages among actors, targets and threats of cyber security. The multiple pathways to, and outcomes of, cyber threat representations, identified by securitization framework, have undoubtedly enhanced our understanding of the complex reality of cyber security. Nonetheless, the restricted focus of securitization studies on speech-acts means that other important elements of cyber security, such as instruments and motivations of cyber attacks, and specific context of cyber threats, may not be adequately addressed. This, again, necessitates an even more systematic and comprehensive approach to understand cyber security.

## 3.5 Bridging Diverse Discourses: From Taxonomy to Ontology

The conceptual underpinning of cyber security, as discussed above, is constructed by different discourses and approaches. But several observations can be made in regard to the common features of these studies.

To begin with, it is noteworthy that cyber security represents a collection of constantly changing phenomena. In this sense, a strictly defined cyber security concept may risk over-simplification and being static, especially given that information technologies are evolving dramatically. Lawson has remarked on this difficult and even paradoxical task "to acknowledge their (cyber threats) complexity and to work toward the clearest, most precise definitions possible, even when absolute clarity and precision are unattainable".[69]

Secondly, cyber security issues are found across different domains and penetrate different dimensions of human security. This indicates a holistic approach that can best illustrate the almost ubiquitous character of cyber in human activities. Efforts to conceptualize cyber security should thus encompass a wide spectrum of attributes rather than center on any single indicator of them.

Moreover, the relational aspect of cyber security should be taken into account in any conceptual framework. Unilateral investment in cyber security is often inadequate in enhancing the totality of security.[70] And actors, issues and systems in and through cyberspace become increasingly inter-dependent and intertwined that their connections could be as important as their properties. As a result, methods need to be identified that allow for simultaneously the demonstration of cyber security

[67] Dunn Cavelty, "From Cyber-Bombs."
[68] Hansen and Nissenbaum, "Digital Disaster," 1163.
[69] Lawson, "Beyond Cyber-Doom."
[70] Xingan Li, "Cybersecurity as a relative concept," *Information & Security: An International Journal* 18 (2006): 11-24.

attributes and the relationship among them.

In response to this need, some studies have attempted to establish organized formal models to better present the dynamic interactions within cyber security issues. On this score, a number of taxonomies have been built to classify cyber threats and attacks in a systemic way.[71] These models adopt different combinations of cyber threat attributes (categories), mostly including attackers, tools, actions, objectives, impacts, and defensive methods. This approach enables security practitioners to analyze patterns of threat behavior and linkages among different aspects of security incidents. For instance, when datasets are input into the proposed models, it is possible, and would be valuable, to locate a particular actor or a specific attack instrument, and identify all the security events associated with that actor/tool.[72] It contributes to revealing commonalities and regularities among cyber threats. However, there are still weaknesses firstly in that most studies in this regard focus on technical cyber attacks, which represent a narrow conceptualization that does not necessarily cover the full spectrum of cyber security.

The problem exists, probably because the proposed taxonomies are pragmatically designed to provide guidance for governmental (and organizational) defensive doctrines or strategies. Moreover, as Applegate and Stavrou acknowledged, taxonomy models are often bound to hierarchical categorizations, which may be incapable of capturing all possible relationships and mechanisms among different attributes.[73]

An ontological approach suggested by them, meanwhile, may alleviate or overcome both deficiencies mentioned above. Defined as an "explicit specification of conceptualization", ontology is often used as a means to facilitate knowledge sharing and reusability.[74] Using Web Ontology Language (OWL), it enables formalized representations of categories, attributes and relations involved in a specific domain. More importantly, it becomes possible to bridge the diversified meanings and expressions of a referent object, thus providing a common platform for different discourses. Nonetheless, current efforts to construct ontologies of cyber security are mainly made by technical communities that intend to understand malware and malicious activities more thoroughly.[75] They do not necessarily facilitate collaboration and knowledge-exchange with political and strategic communities concerned about cyber conflicts or political challenges in general.

In fact, a review on information security ontologies has remarked that a complete security ontology has not been developed that can provide "reusability, communication and knowledge

---

[71] John D. Howard, "An Analysis of Security Incidents on the Internet 1989-1995," PhD diss., (Carnegie Mellon University, 1997); Simon Hansman and Ray Hunt, "A taxonomy of network and computer attacks," *Computers & Security* 24 (2004): 31-43; Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu, "AVOIDIT: A Cyber Attack Taxonomy," *Technical Report CS-09-003 University of Memphis* (2009): http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf; Scott Applegate and Angelos Stavrou, "Towards a Cyber Conflict Taxonomy," presented at the 5th International Conference on Cyber Conflict, Tallin (2013); Kremer and Müller, "SAM".

[72] Applegate and Stavrou, "Towards a Cyber".

[73] Applegate and Stavrou, "Towards a Cyber".

[74] Thomas Gruber, "Toward principles for the design of ontologies used for knowledge sharing," *International Journal of Human-Computer Studies* 43 (1993): 907-928.

[75] Takeshi Takahashi, , Youki Kadobayashi, and Hiroyuki Fujiwara, "Ontological Approach toward Cybersecurity in Cloud Computing," in *Proceedings of the 3rd international conference on Security of Information and Networks,* ed. Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings (2010): 100-109; Leo Obrsta, Penny Chase, and Richard Markeloff., "Developing an Ontology of the Cyber Security Domain, ed.ed. Paulo C. G. Costa and Kathryn B. Laskey, *Proceedings of Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS)*, (2012): 49-56.

sharing".[76] To achieve this objective, development of cyber security knowledge models should not be confined to any single community and, instead, serve as an enabling factor that brings together divergent cyber security discourses. For example, the Global System for Sustainable Development (GSSD) has been constructed by researchers in MIT, which offers an interactive knowledge-networking platform that diversified technologies, instruments, ideas and policies related to sustainable development can easily communicate.[77] With similar logic, the Cyber System for Strategic Decisions (CSSD) is currently under construction that would allow for comprehensive knowledge sharing and generation in the cyber domain.

Cyber security has become an influential aspect of international security studies in the twenty-first century. But our review on the conceptual underpinning of cyber security suggests that different discourses coexist and have divergent views on what constitutes cyber security and threats. Organized formal models, such as taxonomy and ontology, represent a systematic way of conceptualization that has potential for bridging multi-discursivity in current cyber security studies. How to fully engage and include the heterogeneous stakeholders of cyber security into this process, meanwhile, remains an important question for future research.

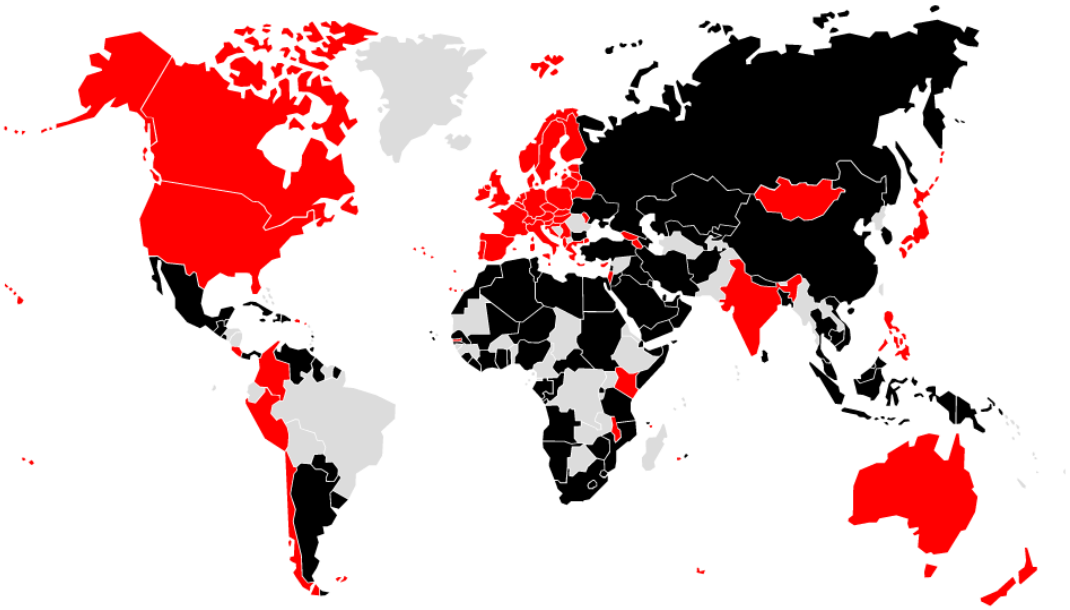

**Figure 3.3**
**Map depicting Final Signatories at WCIT 2012**
(countries in black are signatories of the Final Acts, while red indicates non-signatories)

[76] Carlos Blanco, Joaquin Lasheras, Rafael Valencia-Garcia, Eduardo Fernandez-Medina, Ambrosio Toval, and Mario Piattini, "A Systematic Review and Comparison of Security Ontologies," presented at *The Third International Conference on Availability, Reliability and Security*, Barcelona, Spain,, (2008): March 4-7,
[77] Nazli Choucri, "Mapping Sustainability," MIT Global System for Sustainable Development Working Paper (2003).

**References**


Applegate, Scott. 2013. The Dawn of Kinetic Cyber. Presented at the 5th International Conference on Cyber Conflict, Tallinn, June 4-7, 2013.

Applegate, Scott and Angelos Stavrou. 2013. Towards a Cyber Conflict Taxonomy. Presented at the 5th International Conference on Cyber Conflict, Tallinn, June 4-7, 2013.

Betz, David J. and Tim Stevens. 2013. Analogical reasoning and cyber security. *Security Dialogue* 44 (April): 147-164.

Blanco, Carlos, Joaquin Lasheras, Rafael Valencia-Garcia, Eduardo Fernandez-Medina, Ambrosio Toval, and Mario Piattini. 2008. A Systematic Review and Comparison of Security Ontologies. Presented at The Third International Conference on Availability, Reliability and Security, Barcelona, Spain, March 4-7, 2008.

Brito, Jerry and Tate Watkins. 2011. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. *Harvard National Security Journal* 3 (1): 39-84.

Brown, Gary D. and Owen W. Tullos. 2012. On the Spectrum of Cyberspace Operations. *Small Wars Journal*. (December 11): http://smallwarsjournal.com/print/13595.

Buzan, Barry, Charles Jones, and Richard Little. 1993. *The Logic of Anarchy: Neorealism to Structural Realism.* New York: Columbia University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Buzan, Barry and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Chandrashekar, Jaideep, Steve Orrin, Carl Livadas, and Eve Schooler. 2009. The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware. *Intel Technology Journal* 13 (August): 130-147.

Choucri, Nazli. 2003. "Mapping Sustainability". MIT Global System for Sustainable Development Working Paper.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Choucri, Nazli and David Clark. 2011. Cyberspace and International Relations: Toward an Integrated System. Paper presented at Massachusetts Institute of Technology, Cambridge, Massachusetts, August 25, 2011.

Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2013. Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*. DOI: 10.1080/02681102.2013.836699.

Cohen, Julie E. 2007. Cyberspace as/and Space. *Columbia Law Review* 107 (January): 210-256.

Cornish, Paul, Rex Hughes, and David Livingstone. 2009. *Cyberspace and the National Security of the United Kingdom: Threats and Responses*. London: Chatham House.

Deibert, Ronald. 2002. "Circuits of Power: Security in the Internet Environment." In J.P. Singh and James N. Rosenau, eds., *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, 115-142, New York: Suny Press.

Deibert, Ronald and Rafal Rohozinski. 2010. Risking Security: The Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4 (March): 15-32.

Deibert, Ronald. 2012. The Growing Dark Side of Cyberspace ( … and What To Do About It). *Penn State Journal of Law & International Affairs* 1 (November): 260-274.

DeNardis, Laura. 2009. *Protocol Politics: The globalization of Internet governance*. Cambridge, MA: The MIT Press.

Drezner, Daniel. 2004. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly* 119 (February): 477-498.

Drissel, David. 2006. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs* 19 (1): 105-120.

Dunn Cavelty, Myriam. 2007. Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics* 1 (4): 19-36

Dunn Cavelty, Myriam. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15 (March): 105-122.

Eriksson, Johan and Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review* 27 (July): 221-244.

Even, Shmuel and David Siman-Tov. 2012. Cyber Warfare: Concepts and Strategic Trends. *The Institute for National Security Studies Memorandum* 117.

http://www.inss.org.il/upload/(FILE)1337837176.pdf

Ewan, Pauline. 2007. Deepening the Human Security Debate: Beyond the Politics of Conceptual Clarification. *Politics* 27 (October): 182-189.

Farwell, James P. and Rafal Rohozinski. 2011. Stuxnet and the Future of Cyber War. *Survival* 53 (February): 23–40.

Gibson, William. 1984. *Neuromancer*. New York: Ace Books.

Giles, Keir. 2012. Russia's Public Stance on Cyberspace Issues. In C. Czosseck, R. Ottis, K. Ziolkowski eds., 4th International Conference on Cyber Conflict, 63-77, Tallinn: NATO CCD COE Publications.

Giles, Keir and William Hagestad II. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, and M. Maybaum eds., *5th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf

Goldsmith, Jack L. and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press.

Godwin III, James B., Andrey Kulpin Karl Frederick Rauscher, and Valery Yaschenko, eds. 2011. *Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2*. New York: East West Institute and the Information Security Institute of Moscow State University. http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf

Graham, Mark. 2013. Geography/Internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal* 179 (2): 177-182.

Gregory, M.A. and David Glance. 2013. *Security and the Networked Society*. Switzerland: Springer.

Gruber, Thomas. 1995. Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies* 43 (November/December): 907-928.

Guttman, Barbara and Edward Roback. 1995. *An Introduction to Computer Security: The NIST Handbook*. Gaithersburg, MD: U.S. Department of Commerce.

Hansen, Lene and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53 (December): 1155-1175.

Hansman, Simon and Ray Hunt. 2004. A taxonomy of network and computer attacks. *Computers &*

*Security* 24 (February): 31-43.

Hartmann, Kim and Christoph Steup. 2013. The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. In K. Podins, J. Stinissen, and M. Maybaum eds., *5th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf

Healey, Jason and Karl Grindal, eds. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association.

Howard, John D. 1997. "An Analysis of Security Incidents on the Internet 1989-1995." PhD diss., Carnegie Mellon University.

Hughes, Christopher R. 2010. Google and the Great Firewall. *Survival* 52 (2): 19–26.

International Telecommunication Union. 2008. Overview of Cybersecurity. Recommendation X.1205. https://www.itu.int/rec/T-REC-X.1205-200804-I.

Karim, Md E. and Vir V. Phoha. 2013. Cyber-physical Systems Security. In *Applied Cyber-Physical Systems*, ed. Sang C. Suh, U. John Tanik, John N. Carbone, and Abdullah Eroglu, 75-83. Switzerland: Springer.

Kasper, Agnes. 2014. The Fragmented Securitization of Cyber Threats. In *Regulating eTechnologies in the European Union: Normative Realities and Trends*, ed. Tanel Kerikmäe, 157-187. Switzerland: Springer.

King, Gary and Christopher Murray. 2001. Rethinking Human Security. *Political Science Quarterly* 116 (4): 585-610.

Klimburg, Alexander. 2013. The Internet Yalta. *Center for a New American Security Commentary*. (February): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf

Knapp, Eric and Joel T. Langill. 2011. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Rockland, MD: Syngress Publishing.

Kremer, Jan-Frederik and Benedikt Müller. 2014. SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik and Benedikt Müller, 41-58. Switzerland: Springer.

Lawson, Sean. 2013. Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics* 10 (February): 86-103.

Lewis, James A. 2013. Cybersecurity and cyberwarfare: assessment of national doctrine and organization. In *UNIDIR: The Cyber Index: International Security Trends and Realities*. New York: United Nations.

Lewis, James A. 2014. Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage. *Center for Strategic & International Studies Report* (March).

Li, Xingan. 2006. Cybersecurity as a relative concept. *Information & Security: An International Journal* 18 (January): 11-24.

Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Lynn III, William J. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* 89 (September/October): 97-108.

Mandiant. 2013. APT1: Exposing One of China's Cyber Espionage Units. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. London: Routledge.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. Internet Security and Networked Governance in International Relations. *International Studies Review* 15 (March): 86-104.

National Academy of Sciences. 1991. *Computers at risk: Safe computing in the information age*. Washington, D.C.: National Academy Press.

Nye, Joseph S. 2010. Cyber Power. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (May).

Nye, Joseph S. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5 (Winter): 18-38.

Obrsta, Leo, Penny Chase, and Richard Markeloff. 2012. Developing an Ontology of the Cyber Security Domain. In ed. Paulo C. G. Costa and Kathryn B. Laskey, *Proceedings of Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS)*, 49-56.

Radu, Roxana. 2014. Power Technology and Powerful Technologies - Global Governmentality and Security in the Cyberspace. In *Cyberspace and International Relations: Theory, Prospects and*

*Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller, 3-21. Switzerland: Springer.

Reveron, Derek S. 2012. An Introduction to National Security and Cyberspace. In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, 3-20. Washington, D.C.: Georgetown University Press.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Sartori, Giovanni. 1970. Concept Misformation in Comparative Politics. *American Political Science Review* 4 (1970): 1033-1053.

Simmons, Chris, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. 2009. AVOIDIT: A Cyber Attack Taxonomy. Technical Report CS-09-003, University of Memphis. http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf.

Stern, Maria and Joakim Öjendal. 2010. Mapping the Security–Development Nexus: Conflict, Complexity, Cacophony, Convergence? *Security Dialogue* 41 (February): 5-29.

Symantec. 2014. Internet Security Threat Report 19 (April): http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-19

Takahashi, Takeshi, Youki Kadobayashi, and Hiroyuki Fujiwara. 2010. Ontological Approach toward Cybersecurity in Cloud Computing. In ed. Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings, *Proceedings of the 3rd international Conference on Security of Information and Networks*, 100-109.

Thomas, Caroline. 2001. Global Governance, Development and Human Security: Exploring the Links. *Third World Quarterly* 22 (April): 159-175

Thomas, Nicholas. 2009. Cyber Security in East Asia: Governing Anarchy. *Asian Security* 5 (1): 3-23.

Tilly, Charles. 2003. *The Politics of Collective Violence*. Cambridge: Cambridge University Press.

U.S. Department of Defense. 2010. *Department of Defense Dictionary of Military and Associated Term*s. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Ullman, Richard H. 1983. Redefining Security. *International Security* 8 (Summer): 129-153.

United Nations Development Programme. 1994. *Human Development Report*. New York: Oxford University Press.

Valeriano, Brandon and Ryan C. Maness. 2014. The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research* 51 (May): 347-360.

Williams, Michael C. 2003. Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly* 47 (December): 511-531.

Wilson, Kelce S. and Muge Ayse Kiy. 2014. Some Fundamental Cybersecurity Concepts. *IEEE Access* 2 (February): 116-124.

Wolfers, Arnold. 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly* 67 (December): 481-502.

Zedner, Lucia. 2009. *Security*. London: Routledge.