acknowledging the need for intervention. Further, the UN had a chronicled history and bureaucratic culture of incremental action. The abrogation of the principle of sovereignty was therefore, operationally, not likely to have a pernicious effect on them, reserved instead, they were constantly told, for the most extreme of cases.

The same principle that would abrogate sovereignty in the name of preventive intervention would, however, do the same for preemptive intervention. In contrast, American behavior seemed capricious, narrowly self-interested, and arbitrarily driven by populist and nativist domestic American sentiments, even among some of America's traditional European allies, such as France. Efforts to institutionalize change at the UN along these lines were therefore throttled.

Ironically, having failed in their efforts to locate the purported weapons of mass destruction in Iraq, the Bush Administration subsequently resorted (as a second line of defense for their actions) to justifying the invasion on the basis of humanitarian intervention. As Ken Roth points out, the claim seemed less than credible.

> [T]he United States-led coalition forces justified the invasion of Iraq on a variety of grounds, only one of which–a comparatively minor one–was humanitarian. The Security Council did not approve the invasion, and the Iraqi government, its existence on the line, violently opposed it ... To justify the extraordinary remedy of military force for preventive humanitarian purposes, there must be evidence that large-scale slaughter is in preparation and about to begin unless militarily stopped. But no one seriously claimed before the war that the Saddam Hussein government was planning imminent mass killing, and no evidence has emerged that it was.[92]

Nonetheless, in the end, the Bush Administration came full circle in support of the doctrine of intervention, resorting (however incredibly) to the same humanitarian principle as that advocated by the NGOs and Kofi Annan. Only the UN body stood in the way of its institutionalization and acceptance as a global norm.

[92] Ken Roth (2004), "War in Iraq: Not a Humanitarian Intervention", *Human Rights Watch World Report 2004*, January, http://www.hrw.org/legacy/wr2k4/3.htm#_Toc58744952

5
Cyberspace, the New Frontier – and the Same Old Multilateralism

Panayotis A. Yannakogeorgos

in Simon Reich, Global Norms, American Sponsorship and the Emerging Patterns of World Politics. Palgrave Macmillan, 2011.

> Speaking at the Newseum, Washington D.C. on Internet Freedom, US Secretary of State Hillary Rodham Clinton said "countries or individuals that engage in cyber attacks should face consequences and international condemnation."[1]
>
> Responding to reporters, Mr. Burton said "As the President has said, he continues to be troubled by the cyber security breach that Google attributes to China. His view, and as he said even in China, he thinks that unfettered Internet access is an important value."[2]

The term "cyberspace" still elicits a sense of fundamental departure from business as usual. Depicted in the popular press as being a metaphor for a medium without geographic boundaries, the dynamic new applications using computer networking technology are the epitome of a global project that, although barely visible, has an extensive geography consisting of terrestrial, maritime, outer space, and electromagnetic elements.[3] The processes of negotiation and bargaining, as well as the endemic politics of cyberspace, are surprisingly familiar.

[1] Hillary Rodham Clinton (2010), "Remarks on Internet Freedom", 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm

[2] White House Briefing Room (2010), "Gaggle by Deputy Press Secretary Bill Burton Aboard Air Force One en route Cleveland, Ohio", 22 January 2010, http://www.whitehouse.gov/the-press-office/gaggle-deputy-press-secretary-bill-burton-aboard-air-force-one-en-route-cleveland-o

[3] Elihu Zimet and Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace", in *Cyberpower and National Security* (Washington, DC:

For the most part, however, details of the case look like ineffectual multilateralism as usual, as the US strives to lead and others fail to follow. American technological innovation in the development and maintenance of the Internet's backbone is unquestioned. But a global effort to promote regulatory reform, including the inclusion of global stakeholders in the governance of the domain name system (DNS), is a tense political issue closely linked with national cybersecurity. In sum, American "leadership" as first among equals has led to a succession of dead ends.

In this chapter we examine these processes – the competition between multinational corporations, other norm entrepreneurs and the US to dictate the terms of global cybersecurity norms; the efforts to institutionalize them at a global level; and the predictable failures in attempts at enforcement. Ironically – to use some of the jargon of the social sciences – an inability to generate a suitable global norm has only enhanced insecurity for all actors, as has the failure to agree over how to protect a non-excludable global public good. This has therefore led to a negative-sum outcome. In other words, American attempts to lead have resulted in everyone being worse off. Creating the Internet, and policing it, are two very different problems.

Conflict in cyberspace is a growing problem. Russian hacker-networks indirectly linked to the Kremlin opened a devastating cyber-front against Estonia in 2007. During Russia's 2008 war against Georgia, Russian hackers opened a front in cyberspace the night before conventional forces began their operations. The US is not exempt from this problem. Over the years, Chinese-based hacker networks alone have managed to extract 40 terabytes of information critical to US national security.[4] Many military analysts believe cyber defense and attack will be vital to future military efforts. Indeed, according to Lani Kass, director of the Air Force Cyber Task Force, "We are already at war in cyberspace," as both countries and terrorist organizations currently attempt to carry out cyber-attacks on US interests. Kass points out that "Chinese attacks on DOD (Department of Defense) networks are on the upswing,

National Defense University Press, 2009), pp. 91–112. See also Aharon Kelerman (1993), *Telecommunications and Geography* (New York: Belhaven Press), p. 14.

[4] Economic and Security Review Commission (2007), *Report to Congress of the U.S.-China Economic and Security Review Community*, November, http://www.uscc.gov/annual_report/2007/report_to_congress.pdf

and China is now the United States' peer competitor in cyberspace."[5] In early 2010 it was revealed that unauthorized users attributed to the Chinese government had hacked into 33 US companies, including Google e-mail accounts belonging to Chinese dissidents. The spat between Washington and Beijing brought into public view the accusations that had commonly stayed behind closed doors, rarely making material for public diplomacy.

Challenges to cyberspace security go beyond preventing the corruption of information systems and the promotion of Internet freedom. Well-executed cyber-attacks are not limited to data theft. Using the same techniques, hackers can inject false information into a system, with a number of serious consequences.[6] Recently, the CIA warned that, "cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities."[7] There is circumstantial evidence that Chinese hackers may have been responsible for past power blackouts in the United States, including the notable "Northeast Blackout" of 2003. During this event, over 100 power plants were shut down, in part due to the disruption of communication lines used to manage the power grid. This disruption was attributed to a then circulating computer virus.[8] It has been noted by "one security analyst in the private sector with close ties to the intelligence community... that some senior intelligence officials believe that China played

[5] Levon Anderson (2006), "Countering State-Sponsored Cyber Attacks: Who Should Lead?" in Jeffrey L. Groh, David J. Smith, Cynthia E. Ayers and William O. Waddell (eds), *Information as Power: An Anthology of Selected United States Army War College Student Papers* (Carlisle Barracks, PA: US Army War College), pp. 105–122, 106, available online at http://www.csl.army.mil/usacsl/Publications/infoaspowervol2/IAP2%20-%20Section%20Two%20(Anderson).pdf

[6] The threat to the US power grid is tangible. During a DHS exercise, hackers were given the task of breaking into the information system of a power generator. They were able to physically destroy the generators by gaining remote access to those in the SCADA control system. The Aurora vulnerability, as this exploit is labeled, lends credence to the suggestion that the manipulation of computer code can be just as effective in destroying critical infrastructure as a missile would be.

[7] Ellen Nakashima and Steven Mufson (2008), "Hackers Have Attacked Foreign Utilities, CIA Analyst Says", *Washington Post*, 19 January, A04.

[8] Shane Harris (2008), "Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May be Responsible for Two Major U.S. Power Blackouts", *National Journal Magazine*, 31 May 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

a role in the 2003 blackout that is still not fully understood."[9] Further investigation of China's role is impossible due to data limitations.

Responding to any cyber-incident requires being able to attribute the origins of the attack, which is a complex task, and is often impossible if military or intelligence services are involved in the attack. Nationally based efforts are insufficient in ensuring that global cybersecurity is maintained. Collectively, the international community recognizes the dimension of this problem and has, in response, articulated the need for a global norm intended to secure cyberspace. Although the US disagrees, the majority of global stakeholders have identified the ITU as the appropriate institution through which to organize global cybersecurity efforts. Since 2002, there has been a flurry of activity under the auspices of the ITU designed to emphasize the importance of cybersecurity for maintaining the free flow of information and democratic governance structures for the Internet. Furthermore, discussions of the militarization of cyberspace and how to regulate conflict in this domain within the context of global cybersecurity have remained absent from the agenda, in part due to a US focus on cybersecurity as a criminal issue.

Cybersecurity is crucial for the success of the "Information Society" in which e-commerce, e-governance and e-learning can take place in a regulated manner. The negotiation processes of cyberpolitics generally take place at the ITU, the UN General Assembly (UNGA) and the World Summit on the Information Society (WSIS). The UNGA has recognized the importance of cyberspace as an enabling environment for the Information Society, and that international cooperation is required to assure the peaceful use of Information and Communication Technologies (ICT).[10] The WSIS *Declaration of Principles* and the *Plan of Action*, *Tunis Commitment* and the *Tunis Agenda* reaffirm a global willingness to secure the cyber-commons in order to stimulate a digital Information Society. These embryonic global protocols have sought to shift the position from one where the US has complete technical oversight into one that includes non-US representatives. The US, until recently, blocked all such related efforts.

[9] Shane Harris (2008), "Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May be Responsible for Two Major U.S. Power Blackouts", *National Journal Magazine*, 31 May 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

[10] UN General Assembly (2002), "Developments in the field of information and telecommunications in the context of international security", *Resolution No. A/RES/56/19, PP7*, 7 January, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement

After years of maintaining its position, in September 2009, the US National Telecommunications and Information Administration (NTIA), a bureau of the US Department of Commerce, made what appears superficially as a first step towards internationalizing the DNS. The US, however, retains the ability to shut down the Internet because of its command of network technology.[11]

US businesses currently dominate global networks as a result of their research, development, management and production of ICT, which are part of the Internet's core. This command of global network infrastructure reinforces the view that any global movement to internationalize the core technologies of the information revolution is contrary to broad US security interests, thereby leading to friction on other issues related to global cybersecurity between the US and the rest of the world. Thus, while cybersecurity norms are emerging, and are being codified and institutionalized, US support for them is lukewarm – and they are therefore weakly implemented.

Cyberspace is considered a global commonage, much like land, sea, air, and outer space.[12] The basic environmental platform of cyberspace – the electromagnetic spectrum – has existed as long as the other commons. Recent technological progress, however, has resulted in the harnessing of the spectrum's potential to facilitate social, economic,

[11] United States Code §606 section 47 (d) *War Powers of the President*, wherein it states: "Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication, or any device capable of emitting electromagnetic radiations between 10 kilocycles and 100,000 megacycles, which is suitable for use as a navigational aid beyond five miles, and the removal there from of its apparatus and equipment, or he may authorize the use or control of any such station or device and/or its apparatus and equipment, by any department of the Government under such regulations as he may prescribe upon just compensation to the owners."

[12] Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons", in *Contested Commons: The Future of American Power in a Multipolar World*, Abraham M. Denmark and Dr James Mulvenon (eds), Center for a New American Security, 2010, pp. 137–76; Ahmad Kamal (2005), *The Law of Cyber-Space: An Invitation to the Table of Negotiations* (Geneva, Switzerland: United Nations Institute for Training and Research), http://www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf

political, and military activities. Definitions of cyberspace are numerous, and fall into two categories: strategic and metaphorical.

The strategic definition is the one that is parsimonious and coherent, and has the greatest field utility. Arguably, the strategic definition as coined by the US DOD is one that will best serve the global community in international negotiations aiming to govern cyberspace. That is:

> A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and, exchange data via networked systems and associated physical infrastructure[13]

Overall, this definition may have the greatest analytical utility for the study of how this domain will be governed by a regime of global character. The strategic conceptualization is precise, internally coherent, and parsimonious, thereby offering a greater field utility and contextual range for such a study. De-emphasizing or ignoring the physical character of cyberspace does not contribute to the effort of governing this commonage.

Popular metaphorical definitions of cyberspace argue that cyberspace is nongeographical. Instead, they suggest, it is a highly malleable social construct to which the laws of physics do not apply.[14] Robert Keohane and Joseph Nye have suggested that:

> The contemporary information revolution, however, is inherently global since "cyberspace" is divided on a nongeographical basis. The addresses "edu," "org," and "com" are not geographical.[15]

Such conceptualizations define cyberspace as a social construct outside the realm of physical environment. Keohane and Nye's analysis is particularly problematic because the domain names they mention do have geographical coordinates. The Internet Corporation for Assigned Names and Numbers (ICANN) – a US-based corporation

[13] US Department of Defense, *The National Military Strategy for Cyberspace Operations*, November 2006, p. 3.

[14] Martin Libicki (2007), *Conquest in Cyberspace* (New York: Cambridge University Press).

[15] Robert O. Keohane and Joseph S. Nye (1999), "Power and Interdependence in the Information Age", *Democracy.com? Governance in a Networked World* (Hollis, NH: Hollis Publishing Company), pp. 197–214, especially p. 199.

whose servers are located in the US and operated under agreement with the Department of Commerce – is responsible for the administration of top-level domains such as *.com* and *.org*. The physical location of the administration is in fact the crux of the issue in global cybersecurity negotiations.

Technologically, the DNS is the element that makes the Internet user-friendly. It allows the use of Uniform Resource Locators (URLs) to communicate with other machines on the Internet. Instead of having to type in the numeric IP address of a website, a person can simply type what has become a standard address into a web browser in order to connect with the corresponding location.[16] The major domain names, such as ".com" or ".net," are maintained and updated by ICANN. The US therefore sustains (and from every indication clearly wishes to maintain) a critical hold on this technology.

Cybersecurity norm entrepreneurs

The key social actors are generally a function of the issue areas in which they operate. On most issues, however, private sector corporations and representatives of civil or social organizations tend to clash. This is evident in the case of cybersecurity, where corporate interest in control (for the sake of profit) conflicts with the goals of social norm entrepreneurs seeking to use the Internet as a democratizing tool.

Within the ITU, multinational corporations contribute to the formulation of international standards and policies regulating global information flows, including those broadcast over the Internet. The trend of forming public–private partnerships in order to strengthen the critical information infrastructure, and thereby secure cyberspace, rests on the cooperation of private companies with the state. Thus, at first glance it would appear that the most influential actors in any global cyberspace regime would be corporations such as AT&T, CISCO, and Microsoft. Yet, in international telecommunications negotiations, a state and its ICT firms share a symbiotic relationship – evident in the behavior of the state–business relationship in telecommunications meetings at the

[16] IP addresses thus reside on DNS databases on root servers that allow the translation of URLs into IP addresses. See Robert E. Molyneux (2003), *The Internet Under the Hood: An Introduction to Network Technologies for Information Professionals* (Westport, CT: Libraries Unlimited), pp. 85–6.

ITU.[17] This has been the case ever since the International Telegraph Union, the ITU's predecessor, was formed in the mid-nineteenth century with the intent of regulating telegraph policies.[18]

Some ICT corporations, such as CISCO or Ros Telecom, having earned the trust of ITU members over time as a result of their ownership of the physical telecommunications infrastructure and their proactive contributions to the ITU's program of work, are viewed as more legitimate actors than civil society representatives.[19] This can be attributed to the practice of the ITU in including such business entities in its program of work. Although they did not have voting rights at the WSIS, some states may have served as the mouthpiece of the businesses headquartered within their borders.

In contrast, global civil society representatives decisively lack the corporate advantage at global conferences because they do not research, develop, and deploy the enabling environment of the Information Society. Rather, they focus on ethical issues, ensuring that policymakers embrace democratic principles in implementing cybersecurity measures. It is notable, however, that (originating with the international negotiations that began at the WSIS) global civil society representatives have emerged as active participants, invited by the United Nations to contribute to the drafting of political statements (such as the outcome documents from the WSIS).

Marc Raboy and Normand Landry provide a comprehensive account of the WSIS process from the perspective of global civil society. Noting that the global media did not give the two summits prime coverage, they emphasize the importance of the WSIS, because it:

> ...has placed the governance of global communication on the world agenda, sparking a long overdue discussion that has, in turn, become the spearhead of a larger re-conceptualization of the manner in which global decisions are made.[20]

[17] For further information on the symbiotic relationship between the US Department of State and MNCs, see Edward A. Comor (1994), "Communication Technology and International Capitalism: The Case of DBS and U.S. Foreign Policy", in Edward A. Comor (ed.), *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy* (New York: St Martin's Press), pp. 83–102.

[18] Jill Hills (2002), *The Struggle for Control of Global Communications: The Formative Century* (Chicago, Ill: University of Illinois Press).

[19] Marc Raboy and Normand Landry (2005), *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society* (New York: Peter Lang Publishing), p. 26.

Although their work does detail the Summit's structure, it focuses on the participation of global civil society and its interaction with the UN system, nation-states, and the multitude of constituent actors. They acknowledge that states were the predominant actors in negotiations taking place during the preparatory phase leading up to the actual WSIS summits. Raboy and Landry further note that the WSIS representation led to "a UN summit (that) has been given an organizational structure consisting of a number of components which bring together representatives of member states, the private sector, civil society and various UN agencies."[21] It is further noted that "the clearly expressed desire of the Summit organizer to include these actors from the beginning of the preparatory process is something new at the United Nations."[22] Their study however, focuses on civil society actors – the element that had the least overall access and impact on the outcomes of the WSIS process.[23] It appears, therefore, that NGOs had the greater number of participants but, arguably, were the least influential actors.

Indeed, closed and informal intergovernmental consultations during the preparatory phase – leading to the WSIS Geneva and Tunis phases – occurred without non-governmental actors taking a meaningful part in the decision-making process at all, despite constituting the majority of total participants. Members of civil society organizations or business entities did act, however, as advisers to national governments during the process.[24]

In relegating the participation of non-state entities to the sidelines, states effectively monopolized all authoritative decision-making through their voting rights on key decisions and texts during the Summit itself, complicating the process. Raboy and Landry contend that civil society organizations have a lot to contribute and deserve a greater role in the Internet governance debate. They have not yet, however, been trusted with voting privileges.

[20] Marc Raboy and Normand Landry (2005), *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society* (New York: Peter Lang Publishing), p. 1.

[21] Ibid., p. 30.

[22] Ibid.

[23] Ibid., p. 17.

[24] Ibid.

Articulating and institutionalizing a global culture of cybersecurity: the UNGA, ITU, WSIS and beyond

The importance of organizing and expanding the Information Society was recognized early by the UNGA, in that the establishment of a "global culture of cybersecurity" is key in creating a secure environment for the information society. Initiated at the UNGA with its resolution 57/239 in 2003, the processes have now been institutionalized through the global community meeting at the ITU, which is mandated as the main global institution responsible for the global culture of cybersecurity.[25]

At the UNGA, member states declared their awareness that "effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society."[26] By identifying the provisioning of cybercrime as an activity separate from government or law enforcement, they essentially created a broader cybersecurity framework in which private actors were given the task of preventing cybercrime. The UNGA stated that "technology alone cannot ensure cybersecurity," specifically "in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for, and take steps to enhance the security of these information technologies."[27] The trend towards a broad number of actors (including governments) all of whom are responsible for securing ICT and preventing its misuse was therefore established in a manner that relieves them of the primary responsibility for national security in the cyber-domain. Hence, a global cybersecurity norm emphasizes the role of private actors in providing cybersecurity to society writ broadly, rather than signifying their importance in *supporting* government and law enforcement efforts.

A significant component of the resolution in which global cybersecurity norms are read is the annex of resolution 57/239. This specifies nine elements that form the foundation of the global culture of cybersecurity, as summarized in Table 5.1 below.[28]

[25] United Nations General Assembly (2003), "Creation of a Global Culture of Cybersecurity", *Resolution No. A/RES/57/239*, 31 January, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[26] Ibid., Preliminary Paragraph 5.

[27] Ibid., Preliminary Paragraph 7.

[28] Ibid., Operational Paragraph 3.

Table 5.1 Foundations of the global culture of cybersecurity

Element	Intended outcome
Awareness	All Information Society stakeholders, including individuals, should sustain a level of awareness regarding the importance of having secure information systems.
Responsibility	Stakeholders are responsible for securing their own information systems, and reviewing the policies, practices, measures, and procedures pertaining to their own cyberspace.
Response	Timely and cooperative response is achieved with stakeholders sharing information about threats, vulnerabilities, and security incidents in order to facilitate the detection of and response to the misuse of information systems. Cross-border information sharing may be required.
Ethics	The ethical basis of the GCC is founded on utilitarian grounds in that each participant is expected to respect the interests of others and to act or avoid inaction that will harm others.
Democracy	Cybersecurity regimes are guided by democratic principles, identified as the freedom of thoughts and ideas, free flow of information, confidentiality of information and communication, protection of personal information, openness and transparency.
Risk assessment	Periodic broad-based risk assessments of the security implications of technological, physical and human factors, policies, and services should be conducted in order to determine what an appropriate level of risk is, and how best to manage the risk of potential harm to information systems according to a scale based on the importance of information to the information system being assessed.
Security design and implementation	Security should be incorporated during the planning, design, development, operation, and use of an information system.
Security management	It is on the basis of dynamic risk assessment that security management occurs.
Reassessment	Given the dynamic nature of the information insecurity, in order to assure that all the above elements remain relevant, a periodic reassessment of security protocols and procedures is required.

This global culture of cybersecurity grew out of a prior process within the UNGA whereby Resolution 56/19, entitled "Developments in the field of Information and Telecommunications in the Context of International Security," highlighted several key issues pertaining to the Information

Society and the provision of its security in cyberspace. UNGA acknowledged the potential misuse of ICT in ways that will "adversely affect the security of states in both civil and military fields."[29] Member States were encouraged to prevent the use of information technology for criminal or terrorist use while concurrently promoting its peaceful use. In the operational paragraphs of resolution 56/19, the UNGA called on Member States to support and contribute to multilateral efforts whose task was to identify and develop appropriate countermeasures to current and future threats to international security resulting from the misuse of information technology. Cybersecurity solutions, it noted, must be "consistent with the need to preserve the free flow of information"[30] – a challenging objective, since security measures tend to impede the flow of information.[31]

In 2004, the UNGA addressed the importance of protecting critical information infrastructures,[32] identified as "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operations."[33] This included the DNS. Eleven elements for the enhancement of the protection of critical information infrastructures were proposed in the annex of this resolution. First, it was urged that emergency warning networks should be established to identify and warn of cyber-vulnerabilities, threats, and incidents. Secondly, general awareness must be raised in order to facilitate an understanding of the role that stakeholders play in developing critical infrastructures. The resolution further encouraged

[29] Op. cit., Preliminary paragraph 8.

[30] Ibid., Operational paragraph 1.

[31] For example, when a firewall is installed on a computer network and set to the most secure setting, the firewall makes the use of Internet applications more difficult than beforehand. Free flow of information is preserved when the firewall is adjusted to fit the patterns of an individual's usage. Analogous problems exist when implementing cybersecurity solutions on a larger scale. A corporate firewall may block applications that are useful for some users, but present a security risk for most users. However, if firewalls and anti-virus software are too expensive, an attacker can exploit the lack of security and likewise prevent the free flow of information. Both these examples indicate pitfalls of holding the private sector and individuals responsible for cybersecurity.

[32] United Nations General Assembly (2003), "Creation of a global culture of cybersecurity and the protection of critical information infrastructures", *Resolution No. A/RES/59/199*, 30 January, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[33] Ibid., Preliminary paragraph 3.

the formation of partnerships between private and public stakeholders to better prevent, investigate, and respond to threats on critical information infrastructures. Communication networks, for example, should be in place and regularly tested to assure their effective operation during a crisis situation. Correspondingly, the resolution urged States to develop adequate domestic laws and policies allowing for the investigation and prosecution of cybercrimes, as well as training personnel who would enable the investigation and prosecution of such abuses. Moreover, the annex noted that states are primarily responsible for identifying the perpetrators of an attack against critical information infrastructure, and the sharing of this information with affected states. Appropriate international cooperation should thus accord with properly crafted domestic laws to assure that critical information infrastructures are secure.

As mandated by the ITU, the WSIS and the Global Cybersecurity Agenda are the main summits where governments and all interested stakeholders debate issues and determine the objectives and principles surrounding the structure of the Global Information Society. Although the WSIS Summits in Geneva and Tunis received limited media attention, the foundational work occurring in the preparatory committees and other conferences related to the WSIS received even less attention. These conferences were the venues where the foundation for a common understanding of the Information Society at the WSIS was laid out.[34] The preparatory phases (hereafter PrepCom) were the most important, because this is where states voted on items on the Summit's agenda, on the processes and procedures of the Summit, and where the wording of the final outcome documents was finalized and presented at the Summit itself during interaction with global civil society representatives. Regional meetings were held to supplement the work during the PrepCom phases, and assure that each region could design and define its own needs and expectations regarding the Information Society.[35] By the end of the process, when the Summit's two phases commenced, the international community was willing to finalize the principles of the Information Society.

In 2002, during the lead-up preparatory phase of the WSIS, the United Nations Economic Commission for Europe reported on the challenges to the WSIS process. It noted that complexities and con-

[34] Marc Raboy and Normand Landry (2005), *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society*, op. cit., p. 19.

[35] Ibid., p. 20.

troversies arising from the process were not only due to technological development issues, but were also because of several key questions, including the issue of security.[36] Furthermore, it was then noted that "there is a growing sense of fatigue with global conferences and processes, and that there is no global architecture for international dialogue on knowledge of information technologies" including the Internet.[37] The WSIS emerged out of such concerns at the behest of the ITU, the main institution of global governance given the task of organizing the WSIS. A High-level Summit Organizing Committee was formed to "coordinate the efforts of the United Nations family in the preparation, organization and holding of WSIS."[38] The ITU Secretary-General served as the committee chairman and as the WSIS Executive Secretary; the ITU was led by senior ITU officials and was given the task of ensuring that the contributions of the actors participating in various conferences were comprehensively merged with the contributions from the Preparatory Committee and regional meetings, in a consensus document that would serve as the basis for the *Declaration of Principles* and *Plan of Action* of the WSIS.[39]

The Geneva Summit of the WSIS, held between 10 and 12 December 2003, gave all the relevant parties the opportunity to initiate a formal process of developing the Information Society based on trust and security. The priorities established by UNGA resolutions, notably 56/121 and 57/239, were discussed. The meeting resulted in the drafting and adoption of the *Declaration of Principles* and *Plan of Action* by "the representatives of the peoples of the world."[40] The *Declaration of Principles* decrees that the Information Society should be organized around:

> [A] common desire and commitment to build a people-centered, inclusive and development oriented Information Society, where everyone can create, access, utilize and share information and knowledge,

[36] United Nations Economic Commission for Europe (2002), *The Information Society in Europe and North America: Contributions from the UNECE to the WSIS Prep Com 2*, December, p. 3.

[37] Ibid.

[38] World Summit on the Information Society, *Roles of HLSOC, WSIS-ES, Host country Executive Secretariats, and ITU*, http://www.itu.int/wsis/basic/roles.html

[39] Marc Raboy and Normand Landry (2005), *Civil Society Communication and Global Governance: Issues from the World Summit on the Information Society*, op. cit., p. 21.

[40] World Summit on the Information Society (2003), *Declaration of Principles WSIS-03/GENEVA/DOC/0004*, Paragraph 1.

> enabling individuals, communities and peoples to achieve their full potential in promoting sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.[41]

The Information Society should, therefore, be based on democratic principles, according to which individuals would be guaranteed the right to freely create and transmit information and knowledge, as long as their objectives did not conflict with the principles of the *UN Charter* and the *Universal Declaration of Human Rights*.

Security forms the cornerstone of the Information Society. Paragraph Five of the *Geneva Declaration* states that users must have confidence in the Information Society. A framework of trust that includes "information security and network security, authentication, privacy and consumer protection" must be established to assure that data, privacy, access, and trade are protected.[42] Additionally, the WSIS recommends that appropriate actions at the national and international levels should be taken to secure cyberspace, so that ICT is not used "for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within states."[43] In this regard, the *Declaration of Principles* calls for all interested stakeholders to have a strong commitment to the concept of "digital solidarity" with governments at the national and international level, and recognizes that new forms of partnership will be required in order to meet the goals set out in the *Declaration*.

In addition to the *Declaration of Principles*, participants at the Geneva session of the WSIS agreed upon a negotiated *Plan of Action* for achieving the goals set out. In section C5.12, the WSIS defined what actions must be taken to fulfill the objectives contained in Paragraph Five of the *Declaration of Principles*.[44] Reiterating the importance of security and its role in developing user confidence in ICT, the *Plan of Action* recommended that private–public partnerships address the prevention of, the

[41] World Summit on the Information Society (2003), *Declaration of Principles WSIS-03/GENEVA/DOC/0004*, Paragraph 1.

[42] Ibid., Paragraph 5.35.

[43] Ibid., Paragraph 5.36.

[44] World Summit on the Information Society (2003), *Plan of Action WSIS-03/GENEVA/DOC/0005*, Section C5.12.

detection of, and the response to cybercrime and other forms of ICT misuse. For their role, governments were mandated with the task of developing guidelines taking into account the ongoing efforts in these areas.

The main outcome of the second WSIS summit on the Information Society was the adoption of the *Tunis Commitment* and the *Tunis Agenda for the Information Society*. Significantly, the *Tunis Agenda* called on the Information Society to establish the "requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities."[45] Internet governance was there defined as "the development and application by government, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[46] It did not clearly define the role of each stakeholder, governments in particular, in Internet governance, thereby allowing private actors a strong role in governing the Internet. Given that the core operators of the Internet are US based, the global consensus is that this US control is a threat to their own cybersecurity.

Furthermore, the *Tunis Agenda* stated that "the existing arrangements for Internet governance have worked effectively to make the Internet the highly robust, dynamic and geographically diverse medium that it is today, with the private sector taking the lead in day-to-day operations, and with innovation and value creation at the edges."[47] It stressed that there is:

> [A] need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.[48]

The private sector's role is therefore clearly defined by the *Tunis Agenda* as being responsible for the day-to-day operations of the Internet, and governments should play no role in these technical and operational

[45] World Summit on the Information Society (2003), *Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6*, Paragraph 31.
[46] Ibid.
[47] Ibid., Paragraph 55.
[48] Ibid., Paragraph 69.

aspects. The governmental role remains unclear, other than that it should be significant in policymaking. As will be shown in the diplomatic dispatches (in the next section), the language relating to cybercrime and Internet governance was shaped by the US insistence that ICANN was, and continues to be, a suitable mechanism regulating the day-to-day operations of the Internet. As the Internet expanded globally, the international community has come to disagree with the US position, maintaining that Internet governance mechanisms should be internationalized, a move ICANN itself made in late 2009.

The US response in the process of negotiation

Despite the domestic rhetoric within the United States, the US avoids any discussion of international law to regulate the militarization of cyberspace, focusing instead on issues of cybercrime, bridging the digital divide, promoting public–private partnerships, market liberalization, and the creation of independent regulatory agencies.[49] The US position on the freedom of information flows was apparent in its suggestions that issues such as content regulation should not be discussed since it "infringes on the right of all to freedom of expression as set forth in Article 19 of the Universal Declaration of Human Rights."[50] The focus of the EU was on clusters of e-government, e-learning and e-inclusion, and within each cluster it was "implied that security, privacy protection, and general trust are underlying conditions in order to build people's confidence on the information society."[51] Russia raised challenges to the Information Society, such as "national sovereignty and security in the information space, non-interference in internal affairs and freedom of information, and the safeguarding of human rights in global

[49] World Summit on the Information Society (2005), *United States Contribution document WSIS/PC-1/CONTR/9-E*, http://www.itu.int/dms_pub/itu-s/md/02/wsispc1/c/S02-WSISPC1-C-0009!!MSW-E.doc, Annex 2. It should be noted here that the US is beginning to alter its public position on issues pertaining to intra-state cyberwar. Nonetheless, fundamental differences exist between the US and Russia and resolution will be a long process. For more information on issue this see: John Markof and Andrew E. Kramer, "In Shift, US Talks to Russia on Internet Security" *The New York Times*, December 12, 2009, p.A1.
[50] Ibid.
[51] World Summit on the Information Society, *Denmark, speech on behalf of the European Union*, http://www.itu.int/wsis/docs/pc1/statements_general/denmark.doc. See also World Summit on the Information Society, *Denmark, speech on behalf of the European Union Content and Themes for the World Summit on the Information Society (WSIS)*.

telecommunication."[52] Likewise, the PRC identified security as the key to information and communications networks, arguing that:

> Communications security is directly related to the risks and losses in communications. Security guarantees may improve consumer confidence and further promote the applications of infocom technologies and networks. Security of infocom networks involves technologies as well as laws and regulations and requires international cooperation.[53]

Fighting cybercrime, they suggested, is of utmost importance in ensuring the security of communications networks. International organizations and mechanisms were essential for this purpose. They identified research and development initiatives intended to develop security technologies and "strengthening control of network security and protection of communications networks through application of laws and regulations" as areas the Summit should consider.[54] However, one Council of Europe (COE) transmission note to heads of missions to the COE described the PRC's views as "being inclined to show understanding for views expressed by developing countries."[55]

All parties supported initiatives attempting to wrestle technical control of the DNS away from the US. The EU, Russia, China and the developing world prioritized security concerns, whereas the US appeared to place the emphasis on issues pertaining to the development of the Information Society. As the WSIS process progressed, the preliminary remarks on the importance of securing cyberspace and governing the Internet were soon supplanted by the US resistance to the internationalization of the ICANN. They refused to delegate command of the network, not allowing its control of day-to-day operations

[52] World Summit on the Information Society (2003), *First Deputy Minister of the Russian Federation for Communications and Informatization of the Preparatory Committee for the World Summit on the Information Society, Opening Ceremony*, 10 December.

[53] World Summit on the Information Society (2002), *Statement by Chinese Ambassador Sha Zukang at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society*, 1 July, http://www.itu.int/wsis/docs/pc1/statements_general/china.doc

[54] Ibid.

[55] Council of the European Union General Secretariat (2002), "Main Items raised at the Working Lunch at Ambassador Level between the Troika and China", 5 December, p. 3.

of the domain name system to be handed over to a more diverse group of actors possibly opposed to US interests.

The Pan-European Regional Conference, hosted by Romania on 7–9 November 2002, intended to help the Western European and Others Group (including the United States and Russia) coordinate member states' participation in the WSIS. Preparatory meetings took place leading up to the November meeting. Although other regional conferences took place prior to the second PrepCom, the Pan-European conference included a diverse number of participants from 55 countries.[56] The main outcome of the Pan-European conference was the *Final Declaration of the Pan European Regional Conference*. Principle Six eventually read:

> To realize fully the benefits of ICTs, networks and information systems should be sufficiently robust to prevent, detect and to respond appropriately to security incidents. However, effective security of information systems is not merely a matter of government and law enforcement practices, nor of technology. A global culture of cybersecurity needs to be developed – security must be addressed through prevention and supported throughout society, and be consistent with the need to preserve free flow of information. ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security in both civil and military fields, as well as in relation to the functioning of their economies. It is also necessary to prevent the use of information resources or technologies for criminal or terrorist purposes. In order to build confidence and security in the use of ICTs, Governments should promote awareness in their societies of cyber security risks and seek to strengthen international co-operation, including with the private sector.[57]

This language echoed the UNGA resolutions on the establishment of a global culture of cybersecurity, that would not expand beyond

[56] Other regional conferences held in preparation of the second PrepCom were held in Bamako for Africa (28–30 May 2002), Tokyo for Asia (13–15 January 2002), Santo Domingo for Latin America and Caribbean countries (29–31 January 2003), and Cairo for Middle Eastern countries (June 2003).

[57] World Summit on the Information Society (2002), *Final Declaration of the Pan European Regional Conference*, 7–9 November, http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf

preexisting diplomatic language. The text of Principle Six is straightforward – effective security of information systems extends beyond the responsibility of government and law enforcement practices.[58] The militarization of cyberspace, however, was not included as an item of concern.

The process of negotiating this final draft, however, was conflictual. Comparing the final version of Principle Six with the revisions suggested by the US, EU and Russia indicates that the US preferred to exclude its mention. To safeguard their position, the US led a coalition against the Russians, who were concerned with the issue of cyberspace militarization. The contrast is informative. The Russians proposed the following language for Principle Six:

> Development of ICTs should take into account new challenges and threats in the field of security. There is concern that ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of states in both civil and military fields... It is also considered necessary to prevent the use of information resources or technologies for criminal or terrorist purposes... This suggests the need for a greater awareness and understanding of security issues and the need to develop a "culture of security"... One key element of protection of ICTs against illegal use is the strengthening of information and communication networks security.[59]

The US disagreed with some of the Russians' language, and offered the following revisions:

> Development of ICTs should take into account the need to defend against the wide variety and increasing number of threats to information systems and networks ~~offer new challenges and threats in the field of security. There is concern that~~ ICTs can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the infrastructure of states to the detriment of their security in ~~security of states in~~ both civil and military fields... It is also considered necessary to prevent the use of information resources or technologies for criminal or terrorist purposes... This suggests the need for a greater awareness and understanding of security issues and the need to develop a "culture of security"... One key element of protection of ICTs against unauthorized ~~illegal~~ use is the strengthening of information and communication networks security.[60]

The US revisions were guided by the global norms set out in the UNGA resolution on the *Global Culture of Cybersecurity*, which the US also wanted the EU to reflect in its declaration on Principle Six.[61] Furthermore, the US argued that the language the Russians proposed was "too narrow" and not inclusive of the wide variety of threats to computer systems,[62] focusing on the security of civil and military cyber *infrastructures* of states. The securitization of the issue was thus diluted. The US maintained that its proposed language more precisely reflected the true nature of the threat – suggesting that the US believed, as a core operator of the global cyber-infrastructure, it better understood the nature of the problem. Furthermore, the removal of the word *illegal*, and replacement with the word *unauthorized*, was an attempt to avoid the inclusion of language that would challenge any US intelligence or military activities in cyberspace as illegal. The word *unauthorized*, rather, implies that the US is simply acting without the authority of the operator of an information system. Much open source documentation provides evidence that the US successfully uses cyberspace as a medium for espionage, targeting several countries, including Russia. Branding such activity as "illegal" would therefore put both the US government and business entities cooperating with US intelligence in such operations at risk. One factor, therefore, clearly motivating the US in its refusal to accept language constraining state behavior in cyberspace was its ability to collect information traveling through network infrastructures created by CISCO Systems, IDT, and Microsoft – US-based multinational corporations with close ties to the intelligence community.[63]

[58] World Summit on the Information Society (2002), *Final Declaration of the Pan European Regional Conference*, 7–9 November, http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-E.pdf

[59] Russian Federation proposal for the text of Principle VI.

[60] United States Revision to the Russian Proposal. Markings duplicated here as they appear on the original document.

[61] US comments on the Russian text for Principle VI, received October 29.

[62] Ibid.

[63] James Bamford (2009), *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York, Anchor Books, 2009).

While noting the importance of private enterprises and civil society to the Information Society, the Economic Commission for Latin America and the Caribbean (ECLAC) countries indicated that states should lead the process.[64] Furthermore, they declared that the strengthening of international cooperation in all aspects of the Information Society was important, given the global nature of the problem.[65] In the field of cybersecurity, consistent with the general framework of the other declarations, the *Bavaro Declaration* noted the importance of the priority issues of:

> Establishing appropriate national legislative frameworks that safeguard the public and general interest and intellectual property and that foster electronic communications and transactions. Protection from civil and criminal offences ("cybercrime"), settlement and clearance issues, network security and assurance of the confidentiality of personal information are essential in order to build trust in information networks. Multilateral, transparent and democratic Internet governance should form part of this effort, taking into account the needs of the public and private sectors, as well as those of civil society.[66]

Latin America, led by Brazil, implicitly criticized the US dominance of ICANN with the inclusion of language emphasizing the importance of making Internet governance mechanisms transparent and open to more actors, as a critical component of securing cyberspace. Throughout the ensuing WSIS process, and continuing in other forums discussing Internet governance and global cybersecurity, Brazil has continued to be a vocal opponent to the US position on ICANN. In the period immediately prior to PrepCom 2 in Geneva, in February 2003, the WSIS President suggested that a legally binding *Charter for the Information Society* be instituted in the Tunis phase – an idea attractive to the representatives. However, it was made clear that "a legally binding document would be a non-starter",[67] reflective of a US hesitancy to adopt a formal body of international law governing the Information Society and cyberspace.

[64] World Summit on the Information Society (2003), *Bavaro Declaration*, Paragraph 1.h, http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0007!!PDF-E.pdf

[65] World Summit on the Information Society Asia-Pacific Regional Conference, *The Tokyo Declaration- The Asia-Pacific Perspective to the WSIS*, Paragraph 1.i, p. 3.

[66] World Summit on the Information Society (2003), *Bavaro Declaration*, op. cit., Paragraph 2.g.

The main objective of PrepCom-2 was participant agreement on the substance of the text of the Geneva *Declaration* and *Plan of Action*. While disagreement prevailed, participants did compile a draft declaration of principles and plan of action based on input from the regional conferences:

> Recognizing that confidence, trust and security are essential to the full functioning of the Information Society, guarantees should be provided to users of media, communication and information networks against cybercrime and child pornography as well as protection of privacy and confidentiality.[68]

As a result of slow momentum during PrepCom-2, the WSIS called for an intercessional meeting, subsequently held in Paris from 15 to 18 July 2003. This meeting was called to discuss the *Plan of Action* in order to align it with the text of the draft *Declaration of Principles*.[69] The deliberations of the ad hoc group dealing with confidence and security issues of the Information Society noted that the US, Brazil, Iran, and India agreed on the part of the draft text prepared by the EU. Russia, however, insisted on the inclusion of language on the security of civil and military cyber-infrastructures, and on the inclusion of clauses on cybercrime and terrorism. Others, however, rejected these clauses.[70] Furthermore, other areas of controversy arose during ad hoc committee discussions on Internet governance. Although there was general agreement on the role of the private sector (mainly ICANN) in governing the Internet, some countries, including China, argued for the transformation of this Internet governance mechanism from a private entity to an international governance mechanism.[71] The US strongly opposed this position.

[67] World Summit on Information Society, Transcript of Ambassadorial meeting in Geneva regarding latest developments on the WSIS process.

[68] World Summit on Information Society (2003), *Report of the Second Meeting of the Preparatory Committee*, 17–28 February, http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0012!R1!PDF-E.pdf, Paragraph B.20.

[69] World Summit on the Information Society (2003), *Note by the President*, 18 July.

[70] Diplomatic note on the theme of the Paris intercessional meeting.

[71] Ibid.

In the lead-up to the intercessional panel, disagreements emerged within the EU delegation regarding how the Internet should be governed. France, in particular, diverged from the common EU stance, arguing that the issues of management of Internet governance, "notably, those concerning the integrity and the coherence of the system (standardization and subsidiarity), as well as the sovereignty of states in their management of national domain names, must be entrusted to an inter-governmental organization"[72] – a view in support of the position that the US should internationalize ICANN.[73] Russia and the US, meanwhile, continued to disagree over the language of the *Draft Declaration of Principles* in the area of building confidence, trust, and security in the use of ICT at the third PrepCom.[74] Although Russia had been isolated in meetings prior to PrepCom-3, over its insistence on the use of language "in both civil and military fields" when referring to cybersecurity threats, the PRC supported Russia on the inclusion of this language in exchange for Russian support on two items – "consistent with the need to preserve the free flow of information" and "in accordance with the legal system of each country" in reference to cybersecurity issues.[75] This language, however, remained unchanged in other drafts prepared during PrepCom-3.[76]

The issue of Internet governance, therefore, proved to be one of the most contentious issues during PrepCom-3. The US insistence that language referring to the coordination of the international management of the Internet should be removed from the draft was the main sticking point on this issue. In paragraph 40, the US objected to language referring to a "technical level" of private sector involvement in the Internet:

> The management of the Internet encompasses both technical and policy issues. The private sector has had and will continue to have an important role in the development of the Internet at the technical level.[77]

[72] Draft Declaration of Principles refined in April 22/23, Paragraph 18.

[73] However, the dispute between France and other EU members was resolved prior to the intercessional mechanism during negotiations at the Deputy Representative level in the Committee of Permanent Representatives (COREPER-1). (Diplomatic dispatch dated 16 May 2003 on the results of the EU Commissions meeting at the level of delegate–expert).

[74] World Summit on the Information Society (2003), *Draft Declaration of Principles WSIS/PC-3/DT/1-E*, 19 September.

[75] Ibid., Paragraph 28.

[76] World Summit on the Information Society (2003), *Draft Declaration of Principles WSIS/PC-3/DT/1(rev.2B)-E*, 26 September, Paragraph 28.

The US did agree to the addition of a new paragraph (42) in which "Internet issues of an international nature related to public policies should be coordinated between government and other interested parties."[78] However, less developed countries preferred alternative language referring to coordination "through/by appropriate intergovernmental organization under the UN framework" or "as appropriate on an intergovernmental basis."[79] Thus, it is clear that the US remained hesitant to relinquish its informal control over ICANN, while other participants were resolute that ICANN should be transferred to an intergovernmental organization, preferably within the UN framework. In a second draft prepared during PrepCom-3, an alternative paragraph 40 was introduced, which included language regarding the important role the private sector should play at "the technical and commercial levels."[80] With only a few months until the WSIS's main event in Geneva, the international community continued to wrangle over the text of the document in an effort to bridge the North–South divide, including the issue of US dominance over ICANN.[81]

The second phase of the WSIS focused on the practical issues of implementing the *Geneva Plan of Action*, addressing two significant open questions that remained unanswered after the Geneva phase of the WSIS. These questions centered on how the Internet was to be governed, and how the *Plan of Action* would be financed.[82] Both of these were major areas of contention between North and South. To resolve them, the UN Secretary General established two working groups. In an effort to avoid the pitfalls of intergovernmental negotiations, these

[77] World Summit on the Information Society, *Draft Declaration of Principles*, 19 September, op. cit., Paragraph 40.

[78] Ibid., Paragraph 42.

[79] Ibid., Paragraph. 42, Alternatives b and c.

[80] World Summit on the Information Society (2003), *Draft Declaration of Principles WSIS/PC-3/DT/1(rev.2B)-E*, 26 September, Alternative Paragraph 40.

[81] The main issues of contention were not related to cybersecurity, but rather to human security and human rights. In an effort to bridge this divide with Southern concerns, see Office of the United Nations High Commissioner for Human Rights (2003), *"Background Note on the Information Society and Human Rights"*, October.

[82] European Commission Working Party on Telecommunications and Information Society (2004), *Preparation of the Transport/Telecommunications and Energy Council of 1/10* (6423/04 TELECOM 30 DEVGEN 37 CONUN 6).

working groups included multiple stakeholders under the independent auspices of the UN. The working definition and scope of Internet governance was generally agreed to be:

> ...the global coordination of the Internet's Domain Name System, consisting of the technical management of core resources of the Internet, namely domain names and IP addresses, and the root server system. The WGIG [Working Group on Internet Governance] should firstly concentrate on these issues. A second focal point of WGIG's work should be issues with direct impact on the Internet's stability, dependability and robustness, in particular spam.[83]

WGIG deliberations sought to resolve political issues prior to the main Summit meeting in Tunisia. These deliberations contributed largely to the Internet governance section of the *Tunis Commitment* and *Tunis Agenda for the Information Society.*

Prior to the commencement of the WGIG's program of work, the UN's ICT Task Force hosted a Global Forum on Internet Governance in March 2004.[84] At the forum, the clashes dating from the first phase of the WSIS reemerged. Marc Furrer, Director of the Swiss Federal Office of Communications, representing Switzerland at the meeting, noted that the issue of adjusting or replacing ICANN – a system that is working and improving – deflected attention from more important issues related to cybersecurity that were of greater concern to the Information Society.[85] In contrast, Brazilian and South African delegates opposed this argument. Brazilian delegate Maria Luiza Viotti claimed that Internet governance needed to be reformed, since it excluded developing countries, and appeared to be under the ownership of one group of stakeholders.[86] Lyndall Shope-Mafole, Chairperson of South Africa's National Commission, spoke

[83] European Commission Working Party on Telecommunications and Information Society (2004), *World Summit on Information Society (WSIS): Internet Governance-Guidelines for Discussions in the WSIS Framework*, 7 October, Paragraph 4.2.

[84] (2004) "U.N. ICT Task Force Global Forum on Internet Governance to be Held in March", http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html

[85] United Nations Press Release (2004), "Global Internet Governance System is Working But Needs to Be More Inclusive, U.N. Forum on Internet Governance Told", 26 March, PI/1568, http://www.un.org/News/Press/docs/2004/pi1568.doc.htm

[86] Ibid.

along similar lines, arguing that the legitimacy of ICANN's processes, rather than its functions, was of greatest concern to developing countries.[87] After rigorous talks, it was concluded, on the basis of concerns from the developing world, that ICANN required further reform.

An assessment of the WSIS process at the conclusion of its first phase was presented at a meeting between ITU Secretary General Yoshio Utsumi and EU Heads of Mission.[88] Utsumi stressed the importance of making the current Internet governance structure more democratic, adding that this was more of a technical problem, which had been transformed into a political issue during the Geneva phase of the Summit.[89] His expectation was that all the problems of Internet governance, especially top-level domain names, would not be resolved in Tunisia, and that discussions there should be viewed as part of a longer process.

The EU identified security as an area where horizontal cooperation would be useful in addressing the issues of cybersecurity.[90] It advocated closer global cooperation, while recognizing that many initiatives would require fine-tuning at the local level. The role of the WSIS, as envisioned by the EU, was of raising awareness of the need for effective legislation, international cooperation on enforcement and the need for best technical practices by industry, and user-level awareness of security issues.[91] Finally, the EU suggested that ICANN could improve its performance and structure through a process of internationalizing itself by opening participation to non-American companies and stakeholders.[92]

[87] Ibid.

[88] Transmission Note for the Attention of EU Heads of Mission (2004), *WSIS: Information Exchange of Views Between E.U. Heads of Mission and the ITU Secretary General, Mr. Utsumi*, 17 November. See also World Summit on the Information Society, Tunis Phase, 16–18 November (2004), *Letter from Yoshio Utsumi*, 2 June.

[89] Transmission Note for the Attention of EU Heads of Mission (2004), op. cit.

[90] Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions (2004), "Toward a Global Partnership in the Information Society: Translating the Geneva Principles into Actions: Commission Proposals for the Second Phase of the World Summit on Information Society (WSIS)", 13 July 2004.

[91] Ibid. Toward a Global Partnership in the Information Society.

[92] Council of the European Union Working Party on Telecommunication and Information Society (2004), *World Summit on Information Society (WSIS): Internet Governance- Guidelines for Discussions in the WSIS Framework*, 7 October, Paragraph 4.4.

The US position at the first PrepCom was indicative of its strategy in dealing with the ICANN issue. In its published comments, the US focused on its efforts to bridge the digital divide, an issue far more important to the developing world than Internet governance.[93] Although cybersecurity was mentioned, it was not within the context of Internet governance. This position starkly contrasted with the position of the EU, which noted its intention to actively contribute to the dialogue on Internet governance as well as issues aiming at bridging the digital divide during the Tunis phase of the WSIS.[94] Thus, the fact that the US refrained from mentioning Internet governance in its position paper is indicative of its attitude toward this issue throughout this and other international discussions and negotiations.

PrepCom-2 took place in February 2005 in Geneva, Switzerland. Between the two PrepComs, Europe continued its trend of working on issues of Internet governance in order to better inform the WGIG. Internal debates included a suggestion by France that:

> The new cooperation model should be based on a combination of the current bottom-up public-private partnership, with a light, fast-reacting and flexible oversight entity. This entity would provide a platform for policy dialogue in the interest of all governments.[95]

A suggestion that a formal entity should be established (implicitly replacing ICANN) went beyond the EU's language, which stuck to the WSIS position of creating a transparent multi-stakeholder framework based on democratic principles. In its final report, the EU argued that existing mechanisms and institutions should not be replaced, but should be built on the current structures of Internet governance, whereby public-policy issues of Internet governance could be dealt with in a multilateral environment.[96]

[93] *United States Position on Phase II of the World Summit on the Information Society*, http://www.itu.int/wsis/docs2/pc1/contributions/us.pdf

[94] *Preliminary E.U. Views on the Preparatory Process for the Tunis Phase of the Summit*, http://www.itu.int/wsis/docs2/pc1/contributions/eutext.pdf

[95] Presidency of the Council of the European Union (2005), *World Summit for the Information Society- Guidelines for the Exchange of Views at the Council*, 20 June.

[96] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions (2005), *Towards a Global Partnership in the Information Society: The Contribution of the European Union to the Second Phase of the World Summit on the Information Society (WSIS)*, 6 February.

Subsequent to this declaration, the US National Telecommunications and Information Administration (NTIA) issued a statement affirming its position that the US would not relinquish command and control of ICANN and the DNS system. While recognizing that country-level domain names should be controlled at the national level, the US reiterated the principle that:

> ICANN is the appropriate technical manager of the Internet DNS. The United States continues to support the ongoing work of ICANN as the technical manager of the DNS and related technical operations and recognizes the progress it has made to date. The United States will continue to provide oversight so that ICANN maintains its focus and meets its core technical mission.[97]

The statement concluded by emphasizing that the "United States will continue to support market-based approaches and private sector leadership in Internet development broadly."[98] Thus, the US then – as today – refused to relinquish its control of ICANN, and, as part of its negotiating tactic, shifted its attention to the issue of bridging the digital divide.

On 26 June 2008, the High Level Experts Group (HLEG) for the Global Cybersecurity Agenda (GCA) met at ITU headquarters in Geneva to discuss its recommendations for the ITU Secretary General in the group's five work areas. The GCA is important, since the ITU institutionalized and operationalized this concept at the International Multilateral Partnership against Cyber Threats (IMPACT) hosted in Cyberjaya, Malaysia.

The working group on legal issues was unable to reach an agreement on the contentious issue of the DNS. The US, Canada, and the corporations based in these countries (i.e., Cisco Systems, AT&T, and Microsoft) contended that the ITU was not mandated to regulate and manage systems such as DNS. They argued that the recommendation that included language specific to DNS and identity management should be omitted from any recommendations submitted to the ITU Secretary General.

[97] National Telecommunications and Information Administration (2005), *Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System*, 30 June, http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

[98] Ibid.

Syria, Saudi Arabia, and Brazil opposed this view. They felt that their country-level top-level domain names (ccTLD, e.g., .gr) would not be guaranteed protection, given that ICANN, which is controlled by the US, could delete the ccTLD at any time. Despite the intervention of the ITU Secretary General, who advised meeting participants that they were there in a personal capacity and not as representatives of their respective nation-states, no compromise could be found. In the end, the members agreed to submit their recommendations to the Secretary General via the HLEG Chairman in the form of a "Chairman's report." This report would describe the opposing positions of the two parties.

The remaining points mainly centered on the objections of the US government and US corporate representatives that certain aspects of the recommendations were not part of the ITU's mandate. These elements include the ITU conducting a study of the structure of the Internet, including DNS, and organizing international conferences on cybersecurity. The main response, voiced mainly by Saudi Arabia and Syria, was that, if the ITU's mandate were conservatively interpreted, there should be no HLEG or other cybersecurity talk within ITU, since it is primarily a telecommunications organization. The United States and Canada were constantly reminded that it is the job of Member States, and not HLEG, to review the ITU mandate.

Conclusion

The US currently maintains control of a large percentage of the Internet and other elements of cyberspace. Evolving Internet patterns, however, indicate an incremental decrease in traffic passing through the US.[99] The advanced level of Russian radio-electronic warfare capabilities is clearly an emergent challenge to US national security, partially explaining the US stance at international conferences, where they object to discussions on the use of cyberspace for military or espionage purposes. Decisions have been made on the importance of raising awareness of the cybersecurity policy issue, the need to harmonize domestic laws, and the need for cooperation between private industry and government in securing information infrastructures. The main areas of disagreement are between the US and most of the rest of the world on the issue of Internet governance, specifically as it relates to the expansion of authority of DNS and ICANN to a group of international stakeholders.

[99] John Markoff (2008), "Internet traffic begins to bypass the U.S.", *New York Times*, 31 August.

The US objected to this until 2009 on the grounds that the configuration system was highly functional. Even with the apparent shift in this policy, however, the US still retains the technical control that other states maintain breaches their own cybersecurity. Furthermore, the US objects to the inclusion of certain legalistic language, as well as to the idea of drafting an international convention for regulating conflict in cyberspace. Rather than focusing on cyber-weapons, the US focuses on criminal misuse of this domain. The Russians, on the other hand, are eager to bring the world to the negotiating table for a treaty on cyberspace.

Overall, cyber-attacks and cyber-espionage linked to either US, Russian, or Chinese interests will continue their upward trend. As more and more people gain access to advanced ICT and enter the digital Information Society, the consequences of how states direct and respond to cyber-attacks targeting their national critical information infrastructures and other systems are unclear due to the lack of an international law regulating information warfare in cyberspace. US technical control of the global networks, and the Internet in particular, gives it a distinct advantage over other countries, albeit likely a temporary one. Its decade-long reluctance to treat the security concerns of states relating to US control of the domain name system, and hesitation to discuss the military uses of cyberspace, continue to create a sense of cyber-anarchy. This information dominance may have a long-term cost: an international convention for cyberspace addressing the militarization of cyberspace is likely necessary to protect US networks from attacks originating in private-computer networks that are not under US technical control, but, as potential competitors increase their cyber-warfare capabilities, they may no longer be as willing to negotiate as they are today. The short-term cost is more apparent: the self-interested focus of the US position, even if pursued through a multilateral strategy, has stifled the development of a global norm.