ORF ISSUE BRIEF

NOVEMBER 2013 ISSUE BRIEF # 62

Rules for Cyberspace: The Evolution of American Policy[i]

Darshana M. Baruah

Introduction

The international community has realised the need for rules to govern cyberspace—a domain which transcends national boundaries and is challenging conventional norms of international relations. At the global level, the discourse on cyberspace governance is divided into two schools of thought, one led by Russia and China and the other led by the US. This divide within the international community is due to differing concerns regarding information security. Moscow and Beijing are concerned about the use of information and communication technology as a political tool to incite violence or dissent within their societies. As a result, these nations have been pressing for greater state control over platforms such as the Internet. The US, on the other hand, opposes state control over cyberspace. American concerns are focused on the security of their cyber infrastructure as well as the protection of their economic and defence secrets.

Currently, the US is actively engaging with the international community by discussing cyber security threats and challenges. However, till 2009 Washington seemed reluctant to engage on cyber issues at a global level and even opposed resolutions put forth by Russia on information security in the United Nations (UN). The UN First Committee[ii] has been discussing the issue of information security since 1998, when Russia introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security" in the General Assembly (GA). Since the adoption of the 1998 resolution, there has been a push for international regulations on information security at the UN. However, while Washington continues to oppose calls for an international treaty to govern cyberspace, post 2009 it has begun engaging with the wider global community on the subject. This Issue Brief traces the American cyber policy changes over the last decade, highlighting the factors

[i] This is an updated and more extensive version of the article "Cyberspace Governance: The American Approach", published by the ORF Cyber Monitor, Vol.1, Issue 3, October 2013.

[ii] The United Nations (UN) First Committee on Disarmament and International Security deals with disarmament, global challenges and threats to peace that affect the international community.

underlying the shift. It also spells out the US approach toward cyberspace governance within the UN, bringing forward the current international debate on the issues and challenges in the cyber domain.

US Policy till 2009

Post the 9/11 attacks, US policies on cyber security were framed to ensure the national priority of protecting its infrastructure from terrorist attacks. Washington's primary aim was to strengthen its digital networks to ensure that its critical infrastructure was not vulnerable to potential attacks. US policy was to "protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States."[1]

At the national level, the US released the *National Strategy to Secure Cyberspace* (NSSC) in February 2003, outlining the strategy to protect its critical infrastructure. The document, underlining Washington's main concern, stated: "A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security".[2] Explaining this initiative undertaken by the US Department of Homeland Security, Tom Ridge[iii] stated that panic followed the 9/11 terrorist attacks and a new debate emerged on "cyber security and its relation to national infrastructure".[3] Furthermore, he added: "At the time[while debating on the NSSC] … we believed–perhaps more than some others did–that information security was critical to operational security and as a government, we had to be very concerned about operational security because we depend on the private sector to provide the fundamental services to keep government running".

However, at the global level, Washington opposed calls for an international convention to govern cyberspace and refuted the notion of regulated internet space. As its concerns were different from those of Russia and China, the US did not find any common interest to collaborate with them. In 2003, Russia proposed "the establishment of the Group of Governmental Experts (GGE) on information security".[4] The idea was to provide a platform to the international community to examine and discuss issues on cyberspace. The first GGE was convened in 2004 but due to disagreements within the 15-member expert group, it failed to reach a consensus on a final report.[5] The differences were primarily over control on trans-border information content and on the "question of the impact of developments in information and communications technologies (ICTs) on national security and military affairs".[6] The US reiterated that an international treaty was unnecessary to govern cyberspace, adding that: "Implicit in these proposals would be the extension to governments of the right to approve or ban information transmitted into national territory from outside its borders should it be deemed disruptive politically, socially or culturally".[7]

American apprehensions about collaborating with the international community on a legally binding agreement stem from concerns that authoritarian regimes would use such a mechanism to control the free flow of information. With respect to military applications of IT, Washington has stated that "the

[iii] Tom Ridge is America's first Homeland Security Secretary and was instrumental in drawing the NSSC along with Howard Schmidt-former cyber security coordinator of the Obama administration

law of the armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies".[8] Even after the failure of the first GGE to come to a consensus, Russia continued to push for an international convention through the GGE and drafted another resolution in 2005. The resolution was adopted by a record vote of 163 to 1.[9] The US was the only country to vote against it and continued to oppose it till 2008. However, by 2006 Russia was no longer the sole sponsor for the resolution—it was co-sponsored by China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan and Uzbekistan. While Russia was gaining support within the UN, the US continued to oppose the proposals brought forth by the group till certain events in cyberspace demanded a change or shift in policy. Equally important was the Obama Administration's critique of American unilateralism during the Bush years and greater commitment to multilateralism in addressing global challenges.

Developments in Information Security

A series of developments exposed the vulnerabilities in cyberspace and simultaneously demonstrated its potential utility in 21st century warfare. At the same time, there was growing recognition that cyberspace can potentially be used for economic espionage and theft of defence secrets. This paved the way for inclusive and elaborative discussions amongst world powers on regulating cyberspace. It also triggered greater US engagement with the international community, including Russia and China.

In April-May of 2007, Estonia faced a barrage of coordinated cyber attacks, crippling government websites and halting internet banking. Estonia accused Russia of the attacks owing to its conflict with Moscow over the removal of the Bronze Soldier Soviet war memorial in central Tallinn. The attacks, which initially started as a nuisance to disrupt daily operations, went on to cripple the state's cyber infrastructure including the banking sector for about a week. It also disrupted the functioning of news organisations and other communication services, which made updating citizens about the situation a challenge. The incident highlighted that disruption in cyberspace could severely impact governance and critical infrastructures, potentially leading to chaos and confusion. These attacks were closely monitored by the western countries and the North Atlantic Treaty Organisation (NATO) stepped in to help Estonia strengthen its electronic defence.[10] Subsequently, the 2008 cyber attack on Georgia, which coincided with the Russian military advance into the country, highlighted the application of cyberspace at the time of a military conflict. Russia denied any involvement in both cases.

The cyber attacks on Estonia and Georgia demonstrated the extent to which cyberspace can be used against a state. It established the role of cyberspace in the military domain beyond the conventional use of such technologies to assist communication, command and control. These incidents also brought up challenges such as the difficulty in accurately identifying the aggressor, given the possibility that third party information systems could be used or of non-state actors mounting an attack. Although experts today believe that attribution is not technologically a severe limitation, the question of what sort of response a state could resort to in such a situation remains. During this period, reports on espionage and theft of US intellectual property from foreign actors using cyberspace began surfacing. This was a concern that had been voiced by Washington in most of its reports since 2007. The "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008" stated that:

> “The threat to the United States from foreign economic intelligence collection and industrial espionage has continued unabated since the publication of the 'Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2007'. Economic espionage cases went up slightly and nearly every day brought reports—in the press and in the classified world—of new cyber attacks against US Government and business entities. Additionally, the increasing use of new modes of communication and social networking has provided uncharted opportunities for transferring information and espionage for enterprising foreign intelligence services”.[11]

The report added that the most targeted sectors were aeronautics, information systems, lasers and optics, sensors, and marine systems. Soon after Barack Obama was elected President, he directed the National Security Council and the Homeland Security Council to conduct a top-to-bottom review of America's information and communications infrastructure. Releasing the report on the review in May 2009, Obama stated that “... [Obama] administration will pursue a new comprehensive approach to securing America's digital infrastructure”.[12] Explaining the need for a change in the cyber policy, Obama stated that there had been increasing attacks on Washington's military networks and that the country's “economic prosperity in the 21st century will depend on cyber security.”[13] He also pointed out the potential use of cyberspace during a military conflict by noting the attacks on Georgian government websites as Russian tanks rolled into Georgia. Citing these developments in information security and emphasising on the need to review America's cyberspace policy, Obama remarked that “we're not as prepared as we should be, as a government or as a country”.[14]

The developments within cyberspace and the growing espionage reports forced Washington to engage actively at the international level. If the attacks as suspected were originating from China and Russia, then the US needed some sort of mechanism to discuss cyber security issues. The beginning of the shift in the US policy came through the convening of the second GGE. Although divided on their respective concerns over information security, the draft resolution (this time co-sponsored by the US) was adopted at the 65th GA session (2010), without a vote.[15] This shift in US policy came after President Barack Obama took charge at the White House. The shift was possibly due to cumulative developments in the cyber domain and the political emphasis on multilateralism. While Washington still debated on the need for an international treaty to govern cyberspace and opposed government control over the Internet, it realised the need to collaborate with the wider global community on the subject.

Shift in US Policy

The shift in US policy can be viewed both from the political and security contexts. To begin with, the cyber attacks on Estonia and Georgia made a compelling case for the leaders of the world to decide on red lines in cyberspace. It was also becoming important for Washington to address the increasing reports of cyber attacks and economic espionage by Russia and China on the US. The US-China Economic and Security Review Commission prepared two reports, submitted to the US Congress, on “Chinese Capabilities for Network Operations and Cyber Espionage” detailing the trends and network intrusion incidents attributed to China. Even though Washington traced the attacks back to China, it never directly accused the Chinese government of these attacks. However, as attacks, sabotage and espionage on American soil originating in China increased, the Pentagon in its 2012 annual report directly linked the attacks to the Chinese government—accusing it of not just disrupting systems but also of stealing security and trade secrets.[16] The report stated that:

> "Numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military... The information targeted could potentially be used to benefit China's defence industry, high technology industries, policymaker interest in US leadership thinking...and military planners building a picture of U.S. network defence networks, logistics, and related military capabilities that could be exploited during a crisis".[17]

Realising its own vulnerabilities in the cyber domain, the Obama Administration ventured to join the international discourse and engage in dialogue with other countries. Washington has since emphasised the need for the international community to understand the risks and engage in dialogue to address cyberspace issues. Analysing the change in policy, Joseph Nye, Harvard Professor and American foreign policy analyst, noted:

> For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that measures banning offense can damage defence against current attacks, and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the internet. Nonetheless, the United States has begun informal discussions with Russia. Even advocates for an international law for information operations are sceptical of a multilateral treaty akin to the Geneva Conventions that could contain precise and detailed rules given future technological volatility, but they argue that likeminded states could announce self governing rules that could form norms for the future.[18]

In 2011, China, Russia, Tajikistan and Uzbekistan submitted a letter to the UN Secretary General requesting him to distribute the International Code of Conduct for Information Security drafted by them as a formal document of the 66th session of the GA. The International Code of Conduct (CoC) was a step forward taken by Russia and China to regulate cyber norms and governance. Explaining the CoC, Beijing stated that:

> The International Code of Conduct for Information Security raises a series of basic principles of maintaining information and network security which cover political, military, economic, social, cultural, technical and other aspects. The principles stipulate that countries shall not use such information and telecom technologies as the network to conduct hostile behaviours and acts of aggression or to threaten international peace and security and stress that countries have the rights and obligations to protect their information and cyberspace as well as key information and network infrastructure from threats, interference and sabotage attacks.[19]

The CoC reflects the major concerns of Moscow and Beijing over the use of technologies and platforms such as the Internet as an information weapon. This view has been opposed by the West led by the US. In response to the CoC, Washington issued a statement stating:

> "... the introduction of a draft Code of Conduct for Information Security presented an alternative view that seeks to establish international justification for government control over Internet resources. At its heart, it calls for multilateral governance of the Internet that would replace the multi-stakeholder approach, where all users have a voice, with top down control and regulation by states. It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights".[20]

As noted earlier, Washington has always maintained that there is no need for an international treaty to govern cyberspace. Provisions which already exist within the UN charter to maintain peace and stability apply in the cyber domain as well. Reiterating this position, Washington noted that,

> "... the draft Code appears to propose replacing existing international law that governs uses of force and relations among states in armed conflict with new, unclear, and ill-defined rules and concepts. Indeed, one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of jus ad bellum and jus in bello that would provide a legal framework for the way that states could use force in cyberspace, have no applicability. This position is not justified in international law and risks creating instability by wrongly suggesting that the internet is an ungoverned space to which existing law does not apply".[21]

While the US changed its position on the need for international collaboration to address challenges in cyberspace, it maintained its stance against governmental control over the internet. Analysing this shift in the American policy, Adam Segal[iv] noted that "after years of dismissing the utility of international negotiations on cyberspace",[22] US officials post 2009 began to engage in talks to develop norms in cyberspace. Further, he added that "the Obama administration's May 2009 Cyberspace Policy Review revealed a shift in US attitudes. [It noted] that 'International norms are critical to establishing a secure and thriving digital infrastructure.' In December 2009 the United States agreed to talk with Russia and a United Nations arms control committee about Internet security."[23]

Despite the differences, the two sides now agree on the need for a joint collaboration at a global level to address cyberspace issues. Different viewpoints led by Russia-China and the US, respectively, present a major challenge in bringing definitional clarity as well as a rule-based agreement in cyberspace. At the global level, this shift was once again visible through the GGE. Acting on the need to discuss the growing challenges in cyberspace, the UNGA adopted a resolution in 2011 to set up a third GGE to "continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them".[24] The official GGE report is yet to come out, but a statement by the US Department of State on "Consensus Achieved by the UN Group of Governmental Experts" provides an insight into the course to be taken by the international community. There are a few significant developments brought in by the third GGE. One critical development was that the "Group affirmed that international law, especially the UN Charter, applies in cyberspace".[25] This time the US was no longer on the sidelines voting against resolutions at the UN. The Obama administration engaged at

[iv] Adam Segal is Ira A. Lipman senior fellow for counterterrorism and national security studies at the Council on Foreign Relations.

bilateral and multilateral levels to present its position and work closely with countries like Russia and China. At the 68th UNGA (2013), US representative Michele G. Markoff addressed Washington's views on the subject, stating: "let me reiterate the United States' unwavering commitment to an Internet governance model that is people-centered, bottom-up, multi-stakeholder, and transparent." Markoff emphasised that "The United States favours international engagement to develop a consensus on appropriate state behaviour in cyberspace, based on existing principles of international law, and we cannot support other approaches that would only serve to legitimize repressive state practices."[26]

Conclusion

Washington's policy on cyberspace governance has undergone a change and towards international engagement on the subject. While the US continues to oppose an international treaty, its policy since 2009 has shifted to engage actively at bilateral and multilateral levels. Prior to 2009, the American policy was primarily concerned with the protection of its critical infrastructure. The main difference between the US, on one side, and Russia and China, on the other, concerns the need for a legally binding international convention and governmental control of the internet. However, while the US remains committed to freedom of action in cyberspace, its policy since the Obama administration took over has been to engage on the issue with the international community. Developments in the information and telecommunications security domains led to a review of the US policy on cyberspace governance.

The US maintains that the existing international law to preserve peace and security applies to cyberspace as well. Hence, a new international treaty is unnecessary. The two sides are likely to remain divided on the issue as their concerns vary. However, the growing number of attacks, espionage and the use of cyberspace for military purposes has forced Washington to re-evaluate its policy on the subject and give emphasis to multilateralism that would lead to cooperation at the global level. It has become important to develop norms and define red lines in cyberspace to avoid any miscalculation and conflict in the fifth domain of warfare. Although Washington's policy has changed with regard to international cooperation, it is unlikely that either side will compromise where a treaty is concerned. The one thing that has been consistent in US policy since the Bush administration is the resistance to an international treaty on cyber space governance. Given the stalemate, it is imperative that both sides continue to address the issue through negotiations and discussions. Cyber related issues are already an important part of US-China and US-Russia bilateral dialogues. Addressing the challenges in cyberspace will help develop America's dialogue with China and Russia, possibly resulting in some form of necessary rules and norms to govern cyberspace.

Endnotes:

1. The White House, "The National Strategy to Secure Cyberspace", US Government, February 2003, available at: http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
2. Ibid
3. "Tom Ridge to Congress: stop partisan bickering and start focusing on common goals to secure cyberspace", Infosecurity Magazine, March 11, 2013, available at: http://www.infosecurity-magazine.com/view/31183/tom-ridge-to-congress-stop-partisan-bickering-and-start-focusing-on-common-goals-to-secure-cyberspace/
4. "Developments in the field of information and telecommunications in the context of international security", Report to the Secretary General, United Nations General Assembly, 58th Session, Addendum, A/58/373, September 17, 2003

5. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", Report to the Secretary General, United Nations General Assembly, 60th Session, Addendum, A/60/202, August 5, 2005
6. United Nations Office for Disarmament Affairs, "Fact Sheet- Developments in the field of information and telecommunications in the context of international security", June 2013, available at: http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf
7. "Developments in the field of information and telecommunications in the context of international security", Report to the Secretary General, United Nations General Assembly, 59th Session, Addendum, A/59/116/Add.1, December 28, 2004
8. Ibid
9. " Developments in the field of information and telecommunications in the context of international security", Report to the First Committee, United Nations General Assembly, 60th Session, A/60/452, November 16, 2005
10. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, May 17, 2007, available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia
11. Office of the National Counterintelligence Executive, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008", US Government, July 2009.
12. Barack Obama, "Securing our Nations Cyber Infrastructure", The White House, Washington D.C., May 29, 2009. Available at: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure
13. Ibid
14. Ibid
15. "Developments in the field of information and telecommunications in the context of international security", Report to the First Committee, United Nations General Assembly, 65th Session, A/65/405, November 9, 2010
16. David E. Sanger, "U.S. Blames China's Military Directly for Cyberattacks", The New York Times, May 6, 2013. available at: http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html
17. Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013", US Department of Defense, 2013
18. Joseph S. Nye Jr, "Cyberpower", Paper, Cambridge, Mass.: Harvard Belfer center for Science and International Affairs, Harvard Kennedy School, May 2010. Available: http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html
19. Foreign Ministry of People's Republic of China, "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations," September 13, 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm
20. Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-seventh Session of the United Nations General Assembly", Statement by Delegation of the United States of America, November 2, 2013, available at: http://www.state.gov/t/avc/rls/200050.htm
21. Ibid
22. Adam Segal, "Cyberspace Governance: The Next Step", Council on Foreign Relations, March 2011. Available at: http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397
23. Ibid
24. "Developments in the field of information and telecommunications in the context of international security", United Nations General Assembly, Resolution, A/RES/66/24, December 2, 2011
25. US Department of State, "Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues", Press Statement, June 7, 2013, available at: http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm
26. Michele G. Markoff, "Sixty-Eighth UNGA First Committee Thematic Discussion on Other Disarmament Measures and International Security", U.S. Department of State, Washington DC, October 30, 2013

ABOUT THE AUTHOR

Darshana M. Baruah is a Research Assistant at Observer Research Foundation, New Delhi. Her research focuses on Cyber Security and Maritime Security in the Asia-Pacific.

Observer Research Foundation,
20, Rouse Avenue, New Delhi-110 002
Phone: +91-11-43520020 Fax: +91-11-43520003
www.orfonline.org email: orf@orfonline.org