Centre for Air Power Studies

APPLICABILITY OF 'WESTPHALIAN SOVEREIGNTY' CONCEPT IN CYBERSPACE

Wg Cdr Ashish Gupta
Research Fellow, CAPS

The 'Peace of Westphalia' is a watershed in modern history, resulting in provincial readjustments, geographical arrangements and establishing territorial sovereignty demarcated by borders. Under the 'Peace of Westphalia', a series of peace treaties were signed in the year 1648 in Osnabrück and Münster in Germany, ending the Eighty Years' War between Spain and the Dutch Republic and Thirty Years' War in the Holy Roman Empire. In the later centuries, the concept of sovereignty as enshrined in the treaty, became the basis of guiding principles for nation states. However, the fluidity of the geopolitical landscape has been exacerbated by the political, strategic and economic compulsions redrawing the boundaries among neighbors. Nonetheless, the current world-order ensures sovereign control of a nation over its territory.

But thirty years ago, the birth of the Internet shook the very foundation of sovereignty as propagated by the dominant Westphalian conceptions. This Internet was wild, unhindered and unencumbered by anyone or anything, transcending the physical boundaries with impunity and hubris. The virtual space used by the Internet and operatives became so well recognized that it was even christened with an appropriate name: Cyberspace. There is a growing clamour to identify it as one of the 'Global Commons' at par with the High Seas; the Atmosphere; Antarctica and, Outer Space, outside of the political reach of any one nation state. Independence was the structural yarn used for weaving the fabric of Internet as we know it today. The agnostic nature of the used

standards and protocols do not differentiate between creed, culture or countries. An attempt to block the Internet traffic is treated as a technology hitch and the traffic is rerouted through seemingly infinite networks. "The Net interprets censorship as damage and routes around it."[1] There is a widely held view that it "is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a short-hand term that refers to the environment created by the confluence of co-operative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[2]

The transformation of cyber weapons as an instrument of mass annoyance to an instrument of destruction, with the arrival of Stuxnet on the scene, forced the world to seek order in the disorderly world of cyberspace. The success of Stuxnet changed the perception about cyber warfare, with realisation that serious strategic harm could be inflicted by a determined adversary leveraging cyber weapons. The acts of cyber spying or cyber espionage or even theft through malwares, backdoors or betrayals suddenly start appearing minor irritants in comparison to the possession of devastating and deadly power, which could be yielded with unscrupulous skills remotely. Stuxnet also discredited the fallacy that being disconnected from the Internet is a guarantee of security. All the electronic devices, irrespective of their use in aircraft, plants, factories, production units or system, internally or externally connected to other devices, are highly vulnerable to exploitation to number of inimical elements. In cyberspace, a network of networks spans the planet linking a nation with the rest of the world. Borders in cyberspace are not a definable physical entity but an abstract construct. The lack of sovereign control over cyberspace is a worrisome proposition for all the state nations. Caught in the dichotomous dilemma, the countries are debating, whether to control what comes on Internet over the territories under their sovereign control or to give way to freedom of internet.

The process of erecting virtual fences to regulate flow of information and to prevent acts detrimental to the national interest in cyberspace has already begun. A 'Westphalian age' in cyberspace is slowly but surely emerging, a direct ramification of nation's resolve to exercise sovereign control over cyberspace affecting its national interests. Some of the nations like Russia and China have already initiated the process to have precincts in

cyberspace to protect their national interest, economies and citizens. Other countries have jumped on to the bandwagon demanding control over unhindered flow of data, content and information through the electronic medium, even if it entails restricting the rights of their own citizens.

The concept of borders in cyberspace, akin to physical borders, is taking shape, albeit slowly, a result of efforts by many states to exercise the right of sovereignty over their part of the cyberspace. These efforts are crystallising with the use of technological, institutional and psychological tools and techniques. China is leading the way in its efforts to control the flow of information from outside as well as the information emanating and circulating within its border. The Internet made its appearance in China in the year 1994 primarily with an aim to bring in new technology to provide China with competitive edge to bolster its economy. The event was analogous to enactment of 'Open Door policy' of 1979 to open the country to foreign trade and investment[3]. However, as the open door policy also saw the influx of western ideas, with Internet came a multitude of diversified ideas including the concept of democracy. While the Internet is indispensable in fueling the Chinese economy, its reach and impact on Chinese people is seen as a destabilizing factor to the current political setup. In order to balance between these two ends, the project 'The Great Firewall of China', formally known as the 'Golden Shield Project', was initiated, developed and operated. Initially, under the 'Golden Shield Project', it was envisioned to build a comprehensive database-driven surveillance system capable of accessing every citizen's record as well as linking national, regional, and local security together. The booming numbers of Internet users necessitated various modifications and adjustments to its initial avatar. China has also been working on Project 'Next Generation Internet (CNGI)' for developing an indigenous version of Internet.

Some of the other measures for borders in cyberspace, such as safety against social disharmony, flow of false or fabricated information, attempts of fraud and protection to right to privacy and against social ills such as pornography, may not be as controversial, regressive or authoritative as adopted by China. The vociferous demand for multilateral control over the Internet under one of the agency operating within UN apparatus is already gaining momentum. Several democratic nations, with a goal to curb malicious activities in

cyberspace have put in place a regulating mechanism to prevent social disharmony, misuse or abuse of personal information of its citizens and to protect the economic assets of their countries. States, as cybered entities with sovereign boundaries will be able to defend themselves successfully against threats to their national interests. This will also witness the emergence of less chaotic and relatively safe web.

India, as a tolerant, democratic and pluralistic society, has always stood for the right of freedom of expression. It has been reiterated at various forums that "India is committed to protecting, preserving and safeguarding freedom of expression and Internet freedom and to strengthening them."[4] However, India has taken justifiable measures for removing contents on the Internet that endangers social harmony, public order or national interest. The section 69 A of 'The Information Technology ACT, 2008'[5] vests power with the Government, if it feels necessary or expedient in the interest of sovereignty and integrity of India, defense and security of the State or public order, to initiate actions to block access by the public any information generated, transmitted, received, stored or hosted in any computer resource. Similarly, under many sections of the IT act, various offences such as sending offensive messages through communication service, generation of electronic mail for the purpose of causing annoyance or inconvenience, identity theft, cheating by impersonation by using computer resource, violation of privacy and cyber terrorism are punishable with imprisonment. In some cases, the act is punishable with imprisonment which may extend to imprisonment for life.

ARTICLES BY SAME AUTHOR

CHINA'S ASCENDANCY TO NUMBER ONE POSITION IN THE REALM OF SUPERCOMPUTING: ANOTHER 'SPUTNIK MOMENT 'FOR THE US?

ZERO DAY VULNERABILITY EXPLOITATION: CYBER WEAPON OF CHOICE

ROADMAP FOR UNITED STATES CYBER COMMAND AND ITS APPLICABILITY FROM INDIAN PERSPECTIVE

INDICTMENT OF CHINESE NATIONALS BY US ON CHARGES OF CYBER-ESPIONAGE: ITS IMMEDIATE IMPLICATIONS AND LONG TERM RAMIFICATIONS

The dramatic success of Stuxnet in its ability to do strategic harm has already firmed up the resolve, where there was already loose consensus, to have borders in cyberspace with enforceable laws to protect the legitimate rights of countries and its citizens. The international efforts for the success of this, however, are not without confronting and overcoming myriad difficulties. In the realm of cyber warfare, the question of attributability and accountability is a piquant one. For one, in its present form the Internet does not offer a mechanism for verifiable identification of potential perpetrators. This has propelled the individual states, wittingly or unwittingly, to adopt and use methods for controlling the web, without dwelling much on their authoritative, regressive and repressive nature. The clear delineation of cyberspace under formal agreement with nation states exercising their right of sovereignty over part of cyber sphere is not a distant possibility. The digital borders will provide security within its precinct against rouge intruders. The emergence of borders will also see the emergence of laws and rules applicable to cyberspace which might bring order in the chaotic world of Internet.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1]" John Gilmore's maxim", at http://techpresident.com/networked-public-sphere, accessed on 25 nov 14

[2] Thomas c. Wingfield, The law of Information Conflict: National Security Law in Cyberspace.

[3] "The Great Firewall of China", at http://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/ Freedom OfInformationChina/category/great-firewall-of-china/index.html, accessed on 28 Nov 14

[4] "Deputy NSA questions U.S. control over critical Net resources", athttp://www.thehindu.com/news/national/ deputy-nsa-questions-us-control-over-critical-net-resources/article5244419.ece, accessed on 20 Nov 14

[5] The Information Technology ACT, 2008'.
