Strategic Implications of Internet Governance

Jaijit Bhattacharya

Background

More than one-third of the people in the world use the internet[1], an increasing number of governments are going online with their developmental initiatives[2], and the militaries of several countries are allowing easier access to the web[3] for their soldiers and employees. While, the volume of general, sensitive, and private information stored and exchanged on the internet has been increasing, there is little clarity on who owns and administers the internet. The ambiguity on ownership of the internet poses catastrophic challenges for national security and online privacy.

In a global economy that is interconnected through Information and Communication Technology (ICT), supremacy can be exercised through access and control of key resources and information. Warfare in the 21st century could be conducted using non-traditional means such as cyber warfare, economic warfare, food security warfare, water warfare (blocking and releasing very large amounts of water), and information/ social media warfare. Each one of these can severely impact the efficacy of the traditional military capability.[4]

The access and reach of the internet makes the possibility of cyber-warfare an increasingly probable one. That cyber weapons are not available

Dr **Jaijit Bhattacharya** is President, Centre for Digital Economy Policy Research, New Delhi.

in the global arms market, and countries that do not have such weapons cannot retaliate when cyber-attacked, creates a power imbalance, making certain countries more vulnerable. Without a robust security infrastructure in place, cyber space can become a vulnerable nerve-centre where any act of sabotage or espionage can compromise a country's financial systems, citizens' services, and sensitive data to the extent of partial or complete paralysis of the national critical infrastructure.

Although it is the government that primarily deals with threats to national security and warfare, government policy alone cannot mitigate the threats arising out of lack of internet governance. The private sector has a crucial role to play in ensuring that the nation has technological sovereignty. Often, it is the private sector which controls most of the critical information infrastructure of the country. Moreover, it is the private sector that has the capability of providing technological and intellectual leadership to establish and maintain technological sovereignty.

Internet Governance

Internet governance is not mere administration of the internet. It is concerned with how the internet should be governed so that it does not become a tool for causing social and economic damage to another country or a means of disrupting global peace. The need for internet governance arises from the fact that there is no recognised owner of the internet, and this has in the past led to breaches of national security. Despite there being no owner of the internet, there are agencies and bodies that regulate and control it.

Control of the domain name, such as .com and .org, and country specific addresses such as '.in' and '.uk' is important for the technological sovereignty of any country. These addresses are converted into numbers such as Internet Protocol (IP) addresses that the computers can understand. This is done by root servers that dissolve the addresses we type into the address bars on our browser to the actual numeric addresses.

This domain allocation is done by a Los Angeles based not-for-profit organisation called International Corporation for the Assigned Names and Numbers (ICANN). Of the 13 root servers, 10 are located in the US, 2 in Europe and 1 in Japan. Among the functions ICANN performs is the Internet Assigned Names Authority (IANA) function whereby it controls entries to the authoritative Root Zone File of the internet. The IANA function is overseen by the National Telecommunication and Information Administration under the US Department of Commerce. Technical standards are sent by the Internet Engineering Task Force (IETF). Therefore, the US has significant control over the domain name and IP address allocation through a legal contract with the US Department of Commerce.

The United Nations (UN) established the Internet Governance Forum (IGF) in 2005 to discuss the issues of global internet governance. However, the UN/IGF does not have the organisational structure or the mandate to agree on decisions and the enforcement mechanism to implement them. The meaning of internet governance can broadly include the following policy areas:

(1) Infrastructure and management of critical internet resources, including administration of the domain name system and internet protocol addresses, administration of the root server system, technical standards, network neutrality, and multi-lingualisation; (2) issues in the use of the internet, including spam, network security and cyber crime; (3) issues of wider impact such as Intellectual Property Rights (IPRs), freedom of expression, data protection and privacy rights, consumer rights and international trade; and (4) developmental aspects, in particular, capacity-building.[5]

In December 2012, India joined the US in opposing rules that would give governments control over the internet at the International Telecommunication Union (ITU), a UN agency that aims to update rules governing networks.[6] This demonstrates India's commitment to

preserving freedom of expression. However, as a recognised leader in ICT services, India is also committed to ensuring greater cyber-security, safe cross-border flow of information while creating technological sovereignty. India has an interest and stake in advocating an international framework in which India can participate on an equal footing, rather than being asked to subscribe to regimes and architectures in the framing of which India has played no part.

Strategic Implications of Internet Governance

Due to the absence of a comprehensive global internet policy that is geared towards technological sovereignty, different states are adopting diverse and often contradictory national policies on social media, search engines, and protection of whistle-blowers such as Wikileaks.[7] There are two main strategic implications of the lack of uniform internet governance policies and ambiguity over ownership of the internet.

Damage to Critical Information Infrastructure

The number of internet users will climb to 3 billion by 2016 and the size of the internet economy will reach $4.2 trillion in the G-20 economies. If the internet economy were a national economy, it would rank in the world's top five behind only the US, China, Japan, and India.[8] The internet is a major economic driver, providing banking and financial services to the world's business, acting as a global market place, and a facilitator for the infrastructural services such as railways. For instance, if India loses control of this domain, it will lead to catastrophic loss to Indian businesses and more than a million[9] websites registered on it, some of which carry proprietary and sensitive information.

The internet can be used to bring down telecommunications networks, banks, power grids, and railway and road transport networks. The 2010 cyber bombing of Iran's nuclear centrifuges[10] by the Stuxnet worm, is claimed to have been targeted at high value Iranian assets. If

this had involved use of a missile, it would have been considered an act of war. Apart from causing damage to critical information, any attempt to extend weapons and war to the internet has enormous dangers for every country, including the US. The Flame virus that took out the 10,000 centrifuges is estimated to have cost about $100 million.[11] The Computer Security Institute says if you're running a major e-business and are making $600,000 an hour, then denial of service means more than half a million dollars for every hour you are down.[12]

Cyber-attacks such as the recent one on South Korea, allegedly by North Korea, that led to computer networks running three major South Korean banks and the country's two largest broadcasters becoming paralysed, demonstrate that the military is often ill-prepared to handle these attacks.[13] Internet security issues can be broadly categorised as (1) telecom infrastructure security; (2) encryption standards and law enforcement; (3) the individual's security from identity theft, spam, viruses, Trojans, etc; (4) child protection, particularly against child pornography; (5) cyber threats such as hacking, denial-of-service attacks, worms, viruses against specific organisations, governments and institutions

Legislations for such issues need to be aligned and harmonised to include various stakeholder concerns. Multiple interactions at the levels of government-to-government, government-to-private sector and government-to-citizens are needed to achieve a fine balance between individual freedom, business security and cross-border law enforcement.

Social Warfare

From a social perspective, the lack of internet regulation can disrupt peace and harmony, rupturing the fabric of the society by the use of cyber techniques to indulge in social warfare. In August 2012, Bangalore witnessed social tension and rioting after rumours circulating via the internet and Short Message Service (SMS) created panic among people from northeast India regarding their safety in the city, leading to a mass

exodus.[14] Imagine such an attack being unleashed on the Indian Army which has personnel from various communities.

Weak internet governance can also lead to invasion of privacy, use of hate speech against individuals, nations and religious and social communities, or even changing of web history to instigate diverse populations. Moreover, the internet is a tool for implementation of welfare schemes and e-governance initiatives. In the absence of technological sovereignty, all these initiatives, and the data and services attached to them, can collapse. Lax cyber-security can also lead to damage within strategic institutions such as the military, which can be challenged to protect the nation from cyber-warfare. More importantly, military hardware itself could become a medium of cyber-attack because of the increased intelligence of the equipment. This implies that the entire military strategy could be threatened by compromising the critical information infrastructure having non-authenticated ICT components.[15]

Education, awareness and human resource capacity building is another dimension of a robust internet governance framework and the private sector is playing a huge role in raising citizens' awareness on the cyber-security front. This needs to be extended to raising further awareness on internet governance.

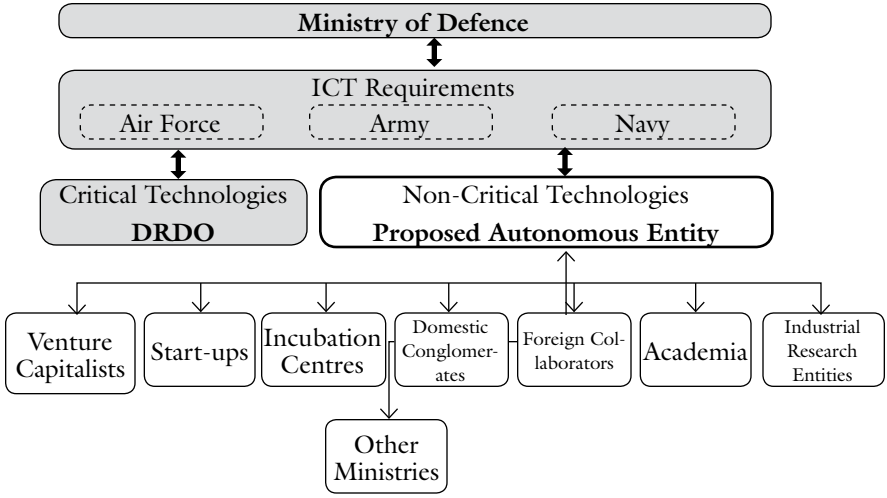
Recommendations for Achieving Technological Sovereignty

Create Private-Government-Military-Academia Collaborative Framework Through the Establishment of an Autonomous Body

The potential threat of cyber-warfare, and India's lack of preparedness to tackle such an attack, calls for a roadmap that includes collaboration between the private sector and the government to meet challenges arising from evolving means of warfare. Such a partnership between the private and public sectors makes it imperative that an autonomous body is

created to make this collaboration possible. Such a body should be given the freedom to develop Information and Communication Technology Enabled Commerce (ICTEC) strategies in consultation with the military, hence, becoming an enabler for the private sector to contribute to the development of tools for technological sovereignty. This autonomous body should also be linked to educational institutions and academic bodies, enabling it to leverage on the investment and knowledge of leading private sector players and the academia.

Fig 1: Proposed Structure of Autonomous Body to Facilitate Leveraging of Private Sector for ICTEC Requirements in Non-Critical Military Requirements



Become Self-Sufficient Through Domestic Procurement and Indigenous Production

To become self-sufficient, and keeping in mind the vulnerabilities of India's national information and communication infrastructure, it is recommended that India's Defence Procurement Policy be geared towards procurement of indigenous components. In this respect, the role of ex-Servicemen from the defence forces can be crucial as they

have domain expertise and can contribute to the domestic procurement strategies. The government's focus should be on incentivising of 'buying Indian', 'buying and making Indian' and 'making Indian' projects. The 'make Indian' projects are a new addition and should be the most incentivised.

Make Investments into R&D

Development, attainment, and maintenance of technological sovereignty will also require substantial R&D investments. The investments in R&D for core military technologies would lead to the development of patented core military technology, helping to achieve the goal of self-reliance. The investment in R&D will lead to development of facilities and products that are a class apart, and can then be exported, compensating for the lack of economies of scale at home in the initial years.

Incentivise Involvement of Private Sector to Develop Tools for Technological Sovereignty

In order to attain technological sovereignty, the defence sector needs to be opened to the private sector beginning with the non-critical technologies, and followed by core critical requirements on successful performance. To invest in new technologies, the private sector also requires assurance in the form of Return on Investment (ROI) and strategies for this need to be evolved.

Create an IT-Enabled Environment

To become technologically sovereign, India needs to create channels for Information Technology (IT) education, and greater awareness and usage of IT-enabled products at the grassroots level. For instance, the Ministry of Defence needs to lead by example by transforming itself from an organisation that still relies on paper communication to a body that operates on the latest IT infrastructure. In defence outfits, it could also be

beneficial to introduce 'reverse mentoring' wherein technologically savvy youth can train and educate their seniors.

India and Technological Sovereignty

The Government of India acknowledges the threat of cyber-attacks and has taken the decision to train half a million cyber-warriors in the next five years to beef up India's cyber-security. India faces a shortage of nearly half million cyber-security experts in spite of being a leader in ICT. The focal issue is India's heavy dependence in terms of imports of critical high-end equipment and software from foreign countries, some of which may be adversaries of India.

The lack of ownership over critical ICT technology can have serious ramifications for India's national security, especially during times of conflict. In the past, India has faced cyber threats from other countries.[16] India is in the favour of transforming the current internet governance regime to make it more multilateral, transparent and democratic.[17] India had proposed to set up a Committee on Internet-Related Policies (CIRP) at the United Nations that could facilitate discussions on public policy issues identified by the World Summit on Information Society (WSIS) without curtailing the freedom of expression.[18]

India wants a forum through which all stakeholders can participate in global internet governance. It seeks to create a system of transparency that, while maintaining the freedom and universal access to the internet, does not give any country or institution greater control over the internet, putting it in the advantageous position to abuse it.

Role of the Private Sector

The future of warfare, or the starting point of future warfare, could be the internet. For a fast-growing economy such as India that has a hostile neighbourhood, the probability of a cyber-attack is high. While national security is the concern of the government and the military, the private

sector can play a crucial role to support the government as it possesses the technical knowhow to do so. The private industry can offer innovative, technologically up-to-date solutions, which the government can then scale up. While the support of the government is needed to provide the infrastructure and a roadmap, the private sector can provide innovative solutions. The innovation can lead to the creation of patented core military technology that can make India more self-reliant. The private sector also has the potential to provide technical knowhow and investment in the R&D and manufacturing of critical defence technology. This will help India to develop quality products domestically and take a lead in boosting local manufacturing by doing local defence procurements.[19]

Conclusion

The impact of the internet is only going to increase as the next generation of the internet, IPV6 enabled internet, starts getting rolled out. This makes the need for technical sovereignty imperative. For this, India will have to work with countries that have similar concerns regarding internet governance. A vision and a roadmap are what India needs at the moment. For instance, China was investing in 4G technologies when India was still developing 2G technologies. India is growing as an economy and as an IT superpower. However, it has not been able to develop the basic technologies that provide technological sovereignty and defence preparedness. India needs to urgently develop frameworks to enable it to be technologically sovereign.[20]

Notes

1. 1See, Internet World Stats, available at http://www.internetworldstats.com/stats.htm
2. United Nations, Department of Economic and Social Affairs, 2012, E-Government Survey 2012, E-Government for the People,sy p. 9, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf
3. James Dao, "Military Announces New Social Media Policy," *The New York Times*, February 26, 2010. http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/

4. See, J Bhattacharya in "Outcome and Recommendations of National Seminar on Technological Sovereignty."
5. Global Internet Governance and India.
6. Amy Thomson, "India, US Reject Internet Regulation," December 14, 2012, available at http://www.livemint.com/Industry/3gtX8BWmMEaIfNyCfFI7xL/UN-group-gives-nod-for-greater-Internet-oversight.html
7. n. 5.
8. BCG perspectives, "The Internet Economy in the G20," 2012, available at http://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/
9. See http://www.inforum.in/general-indian-domain-name-discussion/9802-passes-one-million-registrations-looks-future-growth.html
10. Report available at http://www.bbc.co.uk/news/technology-11388018
11. See http://www.alertra.com/blog/2012/real-possible-cost-flame
12. K Kloosterman, "The Environmental Cost of Flame Computer Hacking," 2012, available at http://www.greenprophet.com/2012/05/environment-cost-hacking-computers/
13. C Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyber Attacks," *The New York Times*, 2013, available at http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0
14. K Mahr, "Fearing Attacks, Thousands Continue to Flee Bangalore," 2012, available at http://world.time.com/2012/08/18/fearing-attacks-thousands-continue-to-flee-bangalore/
15. J Bhattacharya, "Technological Sovereignty," E-gov Magazine, 2012, http://egov.eletsonline.com/2012/12/technological-sovereignty/
16. I Bagchi and V Mohan "12. 5 Lakh Cyber Warriors to Bolster India's e-Defense," *The Times of India*, October 16, 2012, available at http://articles.timesofindia.indiatimes.com/2012-10-16/india/34498075_1_cyber-security-cyber-attacks-cyber-warfare
17. n. 5, p. 6.
18. Ibid.
19. Bhattacharya, n. 4.
20. Bhattacharya, n. 15.