TAKSHASHILA
INSTITUTION

DISCUSSION DOCUMENT
July 14, 2010

THE CASE FOR AN INDIA-US PARTNERSHIP IN CYBERSECURITY

Srijith K Nair

EXECUTIVE SUMMARY

The rapid development and the increasing reliance on information and communication technology (ICT) and cyberspace in the last couple of decades have changed the way every aspect of the society works. Countries like India that hope to exploit the power and reach of ICT for their development should at the same time be wary of the vulnerabilities in their systems.

These ICT systems and cyberspace are highly complex, some of whose properties we are just beginning to understand and appreciate. In order to successfully defend against attacks on these infrastructure and systems, India should actively invest in researching and developing cyber security solutions and collaborating with other countries that share similar objectives.

This paper recommends that Indian institutions, both in the private and public sector, should engage with those from the United States in a partnership role to tackle issues related to cyber security and information infrastructure protection.

Srijith K Nair is Fellow for Cyber Strategy Studies at The Takshashila Institution. The author would like to thank Shehjar Tikoo & Srikanth R from the Takshashila Cyber Strategy Studies project, K Gopinath from the Indian Institute of Science, Bangalore and M Vidyasagar from the University of Texas, Dallas for comments. The opinions expressed in this document are solely those of the author.

BACKGROUND

There has been a marked increase in recent times in the attention given to cyber security and information warfare by national administrations, policy-makers, corporations and the public. This can be attributed to the rise in the awareness of the crucial role played by networked systems like the Internet in the stability and security of a nation and also to various high profile incidents that have transpired in the recent past.

In 2007 Estonian interests were systematically targeted in cyber attacks that took down websites of Estonian organisations, including the Estonian parliament, ministries, banks, newspapers and broadcasters, amid the country's row with Russia[1]. Several credible reports have attributed the series of power outages experienced by Brazil in 2005 and 2007 as being caused by cyber attacks against the nation's power infrastructure[2]. This had left several cities without power for several days and caused financial grief to the industries in the region. These incidents have brought into question Brazil's ability to secure its critical infrastructure as the country prepares to host the 2014 World Cup and the 2016 Olympic Games. Such examples highlight the fact that cyber security indeed has significant physical manifestations.

INDIA MUST ACT URGENTLY

In the recent cyber-espionage operation, brought to light in 2009 by *Information Warfare Monitor* and dubbed "GhostNet", it emerged that computer systems belonging to ministries, embassies and other government offices of India, among others, were infiltrated and sensitive documents were exfiltrated[3]. While it is not very clear whether the attack was initiated by the Chinese government, one of the reports, from researchers at University of Cambridge, say they believe that Chinese operatives were indeed behind the operation[4].

As evident from the GhostNet attacks, Indian networks and systems are being systematically attacked by non-state (and potentially state actors). This did not start with GhostNet nor have we seen the last of these targeted "incidents". Above and beyond the attacks on public sector networks, Indian private sector interests have come under various forms of attacks for some time now, be it by amateurs ("script-kiddies"), activists ("hacktivists") or more nefarious attackers. Given that the outsourcing industry in India has the projected potential to earn $225 billion in revenue by 2020[5], a lot rides on maintaining

the security of the networks, systems and infrastructures of private sector enterprises.

Even though cyber attacks have targeted Indian interests for some time now, national level plans on cyber strategy are largely lacking. This has been on the mend in recent times with the defence minister calling on armed forces to take steps to secure their cyber systems[6] and the Ministry of Communications and Information Technology, taking up the issue of security of government systems at various levels and venues[7].

Notwithstanding the recent claim by the government that "not one attempt has been successful" with respect to the GhostNet attacks and that the "government's computer network system, maintained by the National Informatics Centre[8], is highly efficient,", it is clear from independent reports sensitive systems were breached[9] and that **India is not prepared for a direct or covert attack on its information infrastructures**.

The recent directive by defence minister AK Antony to the top officials of the armed forces to make the cyber systems of the forces "as secure as possible" is a tacit acknowledgment that a lot needs to be done in the area. **While we do have capable individuals to take up the challenge, the chronic absence of any sustained initiative over the years to bolster India's capabilities in the area of cyber security has left the existing systems weak and disjointed.** Cyber security, crime and warfare have advanced leaps and bounds over the years and any country that has not been on top of things throughout these years have a lot of catching up to do. Not surprisingly, this is the case with India.

THE CASE FOR COLLABORATION WITH THE UNITED STATES

As with any other technology, collaborations can go a long way in not only gaining ground faster but also allowing for the creation of mutually beneficial frameworks of operation. **Given that cyberspace extends seamlessly beyond national boundaries, it is imperative that India not work in isolation.** India should rather reach out to like-minded countries to not only engage with them and hope to influence their own policy but also to influence the proceedings of international developments in the area of legal frameworks, agreements, treaties and governance structures.

As in the physical world, the benefits of such outreach will accrue in the aftermaths of actual attacks in cyberspace, due to the information sharing and

attack attribution frameworks such institutions could bring about. **In these early days of cyber warfare, cyberspace focused diplomacy is also essential to frame the rules of engagement in cyberspace.**

From the early days of ARPANET, the United States has maintained technological superiority over both the hardware that powers every part (the core, the edge and the end devices) of inter-networked systems and the software that runs it. Its contribution to securing these system components, and cyber security by extension, have been no different. This has been largely due to heavy public and private investment in research and development over several decades. A joint program with the United States on cyber security will enable India to tap into cutting-edge developments in the area.

The United States has one of the more mature, forward thinking and open set of policies covering various aspects of cyber security, information protection and critical infrastructure security. At the very least, India should take advantage of the public nature of a lot of these policies and consider adopting parts that are relevant in its context. In addition, when compared to other foreign powers, United States has a relatively open policy for dissemination of cyber and software security related knowledge. Such policies have, unfortunately, not been as open as some would have hoped for, but as the interconnected nature of cyberspace and the importance of the security of its dispersed nodes spread across geography have become clearer, some of the self-imposed constraints and caveats have been set aside to some extent.

While cyber threats present a risk to India's critical systems and its economy, given the deep linkages in the ICT industry, these risks are shared to a significant extent by the United States. This will be a major factor that could pressure US enterprises to lobby for major investment and collaboration with Indian counterparts, at least at the private sector level. Above and beyond that, **India should take advantage of the research and development efforts taking place within the educational sector by engaging with universities and other educational institutions in the US studying cyber security issues, both from a technology and strategy point of view.** Such research should focus not just on the technological aspects but also on the risk framework , economic aspects of cyber attacks and their consequences.

EXERCISING CAUTION

There is a case for establishing a strategic relationship with the United States on the matter of cyber security. It has to be emphasised, however, that this requires a great deal of caution and prudence.

In 2001, the India-US Cyber Security Forum was established as a follow-up of initial discussions between the leaders of the two countries. The forum, which grew out of existing dialogues on counterterrorism, was tasked with protecting "the critical infrastructure of the knowledge-based economy" of both the countries and had participation from government agencies and the private sector[10].

Though the forum started off well, its operation was called into question in 2006 when three Indian government officials were arrested on the suspicion of passing on sensitive intelligence information related to vital aspects of India's national security[11]. The gravity of the situation can be gauged by the fact that one of the arrested individuals worked within the National Security Council Secretariat (NSCS), while another of the individuals was working as the director of computers in the Research & Analysis Wing (R&AW) of the Cabinet Secretariat. While subsequent media reports have questioned the validity of the whole case[12], the incident should be considered as a signal reminder of the sensitivity of the content involved. Any joint cyber security forum that is set up should have safeguards in place to prevent a repeat of the alleged misuse of earlier collaborative forums.

The engagement with the US should be conducted in the full knowledge that when push comes to shove, the United States is likely to adopt a very narrow definition of its "interests", and that at any point in time India might have to face the United States as in a non-friendly context.

India must also ensure that foreign parties do not exert undue influence on matters of national security. For example, **foreign entities should not be allowed to influence operational matters** related to securing the national network and infrastructures but it should be possible to consult and work with them on drawing best practices that are to be followed in securing the same. This is in no way different from any other joint task forums or military exercises that are held regularly by various countries, including India.

India should also avoid falling into the trap of becoming too reliant on knowledge and technology exchange brought about by the collaborative

relationship or on using these external collaborations as the only means to further our research agenda in the area.

CONCLUSION

Given the increasingly central role played by networked infrastructures in the security of a nation and that by cyber power on world affairs, **India should develop capabilities to protect its critical systems and position itself to play a major role in the power game centred around cyberspace.**

There is an urgent need to acquire these capabilities. A strategic collaboration with the United States presents a good way for India to do so. While this approach has its risks, previous experiences should not be allowed to cast a shadow on well-considered new initiatives.

REFERENCES

[1] Estonia hit by 'Moscow cyber war', BBC, http://news.bbc.co.uk/1/hi/world/europe/6665145.stm (accessed June 9, 2010)

[2] Cyber War: Sabotaging the System, CBS News 60 Minutes, November 8, 2009, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml (accessed June 9, 2010)

[3] Shadows in the Cloud, http://shadows-in-the-cloud.net/ (accessed June 9, 2010)

[4] The snooping dragon: social-malware surveillance of the Tibetan movement, University of Cambridge, Technical Report 746, March 2009

[5] Extending India's Leadership of the Global IT and BPO Industries, Nasscom, McKinsey, 2005

[6] Make cyber systems secure, Antony tells Army top brass, The Times of India, May 8, 2010

[7] Press release on the visit of Mr Sachin Pilot, Minister of State for Communications and Information Technology to US, Embassy of India, Washington DC, March 20, 2010

[8] Govt thwarted all hacking attempts: Sachin Pilot, One India, March 6, 2010

[9] Researchers Trace Data Theft to Intruders in China, The New York Times, April 5, 2010

[10] Plenary Meeting of India - US Cyber Security Forum, Ministry of External Affairs on India, April 30, 2002

[11] The perils of cooperating with the US, Rediff, July 03, 2006

[12] The Spy who was never, India Today, June 6, 2010