DELHI POLICY GROUP

DPG POLICY NOTE

Advancing India's Rise as a Leading Power

Vol. II, Issue 2

March 6, 2017

COUNTERING THE THREAT OF CHINA-PAKISTAN CYBER COLLUSION

by Lt Gen Aditya Singh, Senior Fellow, Delhi Policy Group

"It would be prudent to assume that the military and Deep State in Pakistan would be seething and itching to react. Given their past record of springing surprises, there must be extensive thought on of new ways to strike at India. ..."

There is unanimity in forecasts for 2017 that the main foreign policy and security challenges will be China and Pakistan. Animosities, issues of unsettled borders and traditional rivalries will further play out. Catalyst to all this is the perception of a strong leadership in India. Thus India's rise and growth will continue to invite resentment among sections in Pakistan and China. No change is anticipated in Pakistan's policy of *'Bleed India with a 1000 cuts'*.

In China's case, seeking its rightful place in the global order and concept of the middle kingdom remains. The coming in of President Trump may mellow its approach to Asia however; its capabilities continue to increase. President Xi Jinping's leadership has overseen vast changes and consolidation of not only defence power, but also in the war of informationalisation. The last three years have seen major restructuring of the PLA, consolidation of its cyber prowess, overt statements with respect to cyber philosophy and raising of the Strategic Support Force (SSF).

2016 witnessed greater Pakistan-China partnership and along with it, the tacit anti-India collusion. Denial of NSG membership, voting against Masood Azhar's declaration as a terrorist on the one hand and the CPEC, increased visits, bringing in the Russians on Taliban and Afghanistan on the other, are visible portents.

While all this will continue, something **of greater concern is the possible collusion in the exploitation of the cyber domain against India. Given its potential and characteristics of causing disruption and damage, 2017 could see the emergence of CPCC.**

Cyber Options

Indo-Pak relations are at a low and situation post the surgical strikes, delicate. Notwithstanding their outward denial, it would be prudent to assume that the military and **Deep State** in Pakistan would be seething and itching to react. Given their past record of springing surprises, there must be extensive thought on of new ways to strike at India. They would also be conscious that any direct or identifiable action, even asymmetric or proxy will invite severe response. Logic therefore dictates options which are un-attributable and ambiguous.

IN THIS ISSUE

DPG Policy Note is produced by the Delhi Policy Group, an independent and autonomous, not for profit think tank which focuses primarily on strategic issues of critical national interest.

In keeping with the growing dynamism of India's foreign and security policy, the DPG is expanding its focus areas to include India's broader regional and global role and the strategic partnerships that advance India's rise as a leading power. To support that goal, the DPG undertakes research and organizes policy interactions across a wide canvas, including strategic and geo-political issues, geo-economic issues and defence and security issues.

DPG does not take specific policy positions; accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

Ambassador Hemant Krishan Singh
Director General

The cyber domain offers all this. More so, as dependency on information technology (IT) in India is growing, along with the potential for visible damage. India's open acceptance of surgical strikes were a change from the past. They found global acceptance as acts of self defence. Retaliation without sufficient proof however, becomes complex. While Pakistan has no qualms on resorting to asymmetric or proxy war, major powers such as India can only act in accordance with international law under identifiable norms. Open societies also do not take action against innocents and avoid collateral damage. This does not apply to a nation like Pakistan, which in the past has struck with impunity and disregard.

Post the strikes of September 2016, a number of Pakistani hacker groups had attacked and defaced Indian websites. Times of India put the figure at over 7000. The damage or disruption however, was minor as the websites were academic, State Government, or institutional and penetration limited. What was however of concern was the attack on BSNL and MTNL networks which carry most of India's official traffic. The potential of manipulation and disruption and damage is thus, considerable. This is further compounded by the fact that a very large proportion of the hardware is of Chinese origin, with the possibility of trap doors and other vulnerabilities.

India has to plan for the contingency that proxies and terror pawns would have been tasked and the coming months should possibly see an increase all round. Recent reports of defacements of Indian websites are testimony, one of the latest being that of the National Security Guard on 1 January 2017 as reported by the Times of India and others. So far these appear to be acts of individuals and hacker groups with limited impact. This may not be so in the future.

Another aspect that needs to be taken note of is the relative **'quiet'** on the cyber front in the last few years. The period 2010-2012 saw very large number of attacks on Indian websites and networks. The then NSA announced to the media that 'Ghost Net' had penetrated NSC websites and other networks of the NIC. There have, however been very few reports in this regard for the last four years. It would be naive to consider that no such activity is taking place. A pragmatic assessment would be that adversaries are using more sophisticated methods for cyber penetration and conducting espionage in such a manner that they remain undetected. This could also include installing of malware, collecting data, identifying vulnerabilities and building weapons to take down or disrupt systems when needed.

"A pragmatic assessment would be that adversaries are using more sophisticated methods for cyber penetration and conducting espionage in such a manner that they remain undetected. ..."

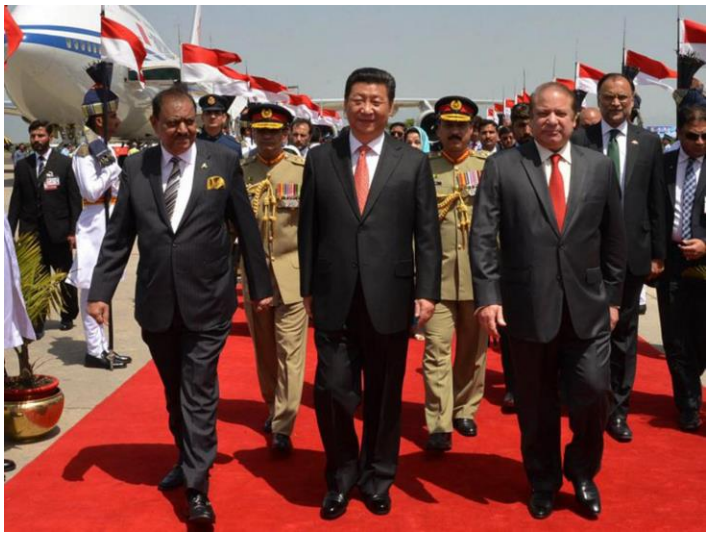
This is the proverbial 'doubly whammy' because on the one hand the 'quiet' means increased penetration and on the other, lulls the user and system into a false sense of security.

Cyber Prowess of China and Pakistan

Countries normally do not reveal their cyber prowess. However, in the past three years there has been a distinct change in this regard with respect to China. This openness has to be taken into account, as also their ability to leverage countries like Pakistan and North Korea to target adversaries.

In 1995 General Wang Pu Feng[1], considered as the Father of Chinese doctrine on Information Warfare (IW) said *"it is no longer conquest of territories or the destruction of enemy troops, but the destruction of the enemies will to resist"*. In their book 'Unrestricted Warfare' published in 1999 Colonels Qiao Liang and Wang Xiangsui emphasized that *"technological progress has given us the means to strike at the enemy nerve centre directly without harming the other things, giving us enormous new options for achieving victory and all these make people believe that the best way to achieve victory is to control and not to kill"*. Following this China in the past two decades has built up immense capabilities. Exploits of its PLA Unit 61398 are well documented as also that the Department of Justice in May 2014 had indicted five of its Officers for theft of confidential business secrets and intellectual property[2].

The Snowden revelations and recent presentations by the intelligence agencies of USA to President Trump with respect to interference by Russia to influence the Presidential poll are pointers of things to come and need to be considered in the regional context.



President Xi Jinping, arriving in Rawalpindi on Monday, April 20, 2015 to announce the China-Pakistan Economic Corridor (CPEC). Source: AP

Until then China had consistently denied its involvement in hacking. In 2015 it changed its position and openly admitted of having cyber warfare units, both military and civilian. In November 2015 President Xi Jinping announced at the meeting of the Central Military Commission the establishment of the SSF. This was set up in January 2016 and three military intelligence units formerly under the General Staff Department, have been integrated into it. SSF has the same stature as the Chinese Army, Navy, Air Force and Missile Services. It includes the 3 PLA, which is believed to have as many as 1000 cyber warfare hackers. The 4 PLA is responsible for military electronic intelligence and electronic warfare services. Further, it is understood that the military spy services known as 2 PLA has been combined in this force. Classified documents made public by the US reveal that hackers of 3 PLA conducted more than 30,000 attacks on US networks. President Xi Jinping announced on 29 August 2014[3] that China's military needed *"a new strategy for information warfare amid a global military revolution"*. China is seeking to work on the precepts of Sun Tzu, who maintained that acme of skill was defeating the enemy without shooting.

Alongside this China has taken major steps to isolate its systems and protect its people by creating internal networks and not use global services. It has its own equivalent of Google in Baidu; Twitter in Weibo and a messenger application We Chat which is similar to Whatsapp. All these are hosted on Chinese servers and closely monitored. Estimates indicate that up to two million Chinese police the net[4].

> ***"President Xi Jinping announced on 29 August 2014 that China's military needed "a new strategy for information warfare amid a global military revolution". ..."***

An organized structure for cyber and information war and protection of its networks has thus been established.

Participants listen to a speech by Chinese President Xi Jinping shown on a screen during the opening ceremony of the third annual World Internet Conference in Wuzhen, China, on November 16, 2016. Source: REUTERS

There is very little information in the public domain about Pakistan cyber units. However, given its proximity to the Chinese as also their thinking, it would be logical to assume establishment of such capabilities. General V P Malik in December 2014 specifically mentioned that China could support Pakistan's strategy to shape world opinion against India in the UN and other world fora. He added that China has shown capability to exploit India's faultlines and instigate the ethnic strife which could result in diversion of India's war effort.

In 2014 there were also reports of 'Operation Arachnophobia'[5], a cyber espionage campaign against India. It featured a custom malware family dubbed *Bitterbug* that served as the backdoor for siphoning information. Researchers established having spotted malware bundled with decoy documents related to Indian issues. The *Bitterbug* malware was geared for cyber espionage and hidden behind pilfered US infrastructure as a way to hide its origins. Specifically, the attacks employed infrastructure from a US virtual private server to make the attacks appear to have come from the US.

Pakistan Cyber Army (PCA) which emerged in 2009 has targeted hundreds of Indian websites. Its Facebook wall is used by its followers to share hacking-related content and tutorials. A 20 April 2013 post revealed its location as Karachi. It describes itself as a *"board of professional ethical hackers and server system security professionals."*

Its blogs indicate hacking of Indian websites. The PCA-allied hackers seem to have targeted prominent websites based in India and Israel. These include website of BSNL, wherein data of 10,000 customers was stolen. According to a July 26, 2011 post; the website of Central Reserve Police Force (CRPF) of India was also hacked.

Reports about cyber-attacks and disruption after the strikes of September 2016 have been mentioned earlier. Given the possibility of penetration not only in computer networks, but also influence through social media, the potential in serious mischief and danger exists. It is an established fact that in 2012 a number of false messages with images in the social media which led to exodus of people of the North East from Bangaluru and Mumbai, were traced back to Pakistan.

> *"While Pakistan may not have a formal structure, it enjoys the advantage of language and agents to do its bidding both within and outside India. This presence of insiders is a serious threat in the cyber world. ..."*

While Pakistan may not have a formal structure, it enjoys the advantage of language and agents to do its bidding both within and outside India. This presence of insiders is a serious threat in the cyber world. All this could be leveraged in building a collusion with China and use their established structures to hit Indian networks and cause grave damage. **Imagine the damage by a hundred Snowdens**. **The Deep State can now strike deep and it is the citizen who is under threat! War has now come to the hinterland and the common man.**

Likely Targets

The potential for harm from cyber-attacks, or social media campaigns is vast and unpredictable. It extends from mere defacements disruption of financial system, power black outs, paralyzing communication or transportation networks, causing major loss of life and so on. Social media drove the post Burhan Wani death agitation. Induction of malware or false data, into sensitive networks such as air traffic control(ATC) can in theory, even bring down aircraft or cause collisions. Recent disruptions in ATC at Jammu, Delhi and Lucknow need to be looked at in this light. Richard Clark[6] and others have listed the havoc that could be wrought.

Internet has been used by terror organizations for funding and recruitment. While there has so far been no major incident of 'Cyber Terror', its ability to influence minds, propagate divisive tendencies is vast. Given vulnerabilities, lack of awareness along with a large number of bots, perception can be shaped and panic generated. It could greatly effect credibility of the government. Recent revelations of Russia's alleged interference in the US Presidential Poll need to be examined and studied in light of the large number of elections that take place in India.

Possible targets for the CPCC thus, are many. India may also become a testing ground. Assuming that the Military and strategic communications are secure, there is need to assess where and what damage could be inflicted. This would primarily be in critical infrastructure under verticals like telecom, the internet; energy; transportation; banking and finance; law and order; intelligence; public health; water; e-governance *et al*. These span both the public and private sector with varying degrees of security. Given the thrust for Digital India, sheer numbers involved and levels of awareness, this vast lake of vulnerability, is worrisome.

The possibility of an untraceable yet, disruptive cyber-attack is today many times greater than a conventional attack. Is India prepared for it?

India's Preparedness

India issued a Cyber Security Policy in 2013 and a Cyber Security Coordination Officer has been appointed at the National Security Council Secretariat (NSCS). The much awaited National Cyber Security Coordination Center (NCSCC) is yet to be set up[7]. A number of organizations such as Computer Emergency Response Team (CERT), NIC, NASSCOM, Data Security Council of India (DSCI) are working with respect to cyber security and there is some coordination. However given the challenges, number of agencies involved, tendency to work in silos and lack of trust, the field is open for mischief. In addition are inadequate staff and poor manning standards. In this fast changing domain, India lags far behind. The question simply is: **'Has a Cyber 26/11 been planned for?'**

On a positive note it must be stated that India can get together in crisis situations. During the Common Wealth Games of 2010, the threat had been anticipated and more than 2500 attacks were foiled during the Opening Ceremony. The problem, however, is in daily matters, where there is need for a system in place to monitor the whole spectrum and ensure immediate counter measures. **There is deployment and alertness on India's physical borders, is there a similar vigil to protect the digital frontiers?**

The National Critical Information Infrastructure Protection Centre (NCIIPC) was set up in 2014 under NTRO with a mission *"to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders"*[8]. It has made an effort to bring agencies together however, open source information suggests that there is a long way to go to be able to prepare for attacks as envisaged.

The main issue is building trust. India is handicapped by the traditional bureaucratic milieu which has no place in the cyber world. Perception of the 'ruler vs the ruled' approach cannot work where stakeholders have an equal, if not greater responsibility. This is specially so as most institutions would not like to make public an attack as it may be perceived as a failing. In case of private enterprises, it effects credibility and reputation which in turn, impacts business. **Building this faith and balancing confidentiality is thus the key.**

"This is specially so as most institutions would not like to make public an attack as it may be perceived as a failing. In case of private enterprises, it effects credibility and reputation which in turn, impacts business. ..."

What Needs to be Done

Building faith and cooperation among all the stakeholders has to become a mission. While guidelines may be set by the National Information Board (NIB) and NSCS, the approach adopted has to be a collaborative one. Challenges to national security, danger and linkage of IT with all aspects of economy, infrastructure, intellectual property, social harmony, law and order and so on need to be understood as also the need for greater awareness. Strength lies in numbers and consensus can only emerge after a series of interactions at various levels. **This has to be generated. In sum, every citizen has to be a soldier and every institution, a war formation**.

While this silent war is on, there is little realization of its seriousness or possible impact. The political class will act once they appreciate that elections and people can be influenced, as also the mayhem that can ensue. The private sector will respond when it appreciates that a financial crash will hit them. Danger of carnage and panic will drive public agencies. All this needs constant and regular dissemination.

"While this silent war is on, there is little realization of its seriousness or possible impact. The political class will act once they appreciate that elections and people can be influenced, as also the mayhem that can ensue. ..."

These realities must also compel studies and pragmatic assessments to identify what disruption and damage that could take place in each sector as also the cross domain linkages. Worst case situations need to be considered and war-gamed. Priorities need to be laid down and counter-measures planned for. These would be in accordance with standard principles, i.e. identification of damage; its containment or isolation and restoration of networks. This may sound simple but like the proverbial Pandora's box may open up many a new challenge. It must be appreciated that in the cyber domain there will never be a perfect or comprehensive solution. However collective cooperation can ensure a modicum of security**. Suitable publicity can also serve as a deterrent. Specially in case the inimical state is not that well protected. It is a mind game.**

The Indian Context. Notwithstanding the wide ambit, a brief analysis in the Indian context reveals that given the present state of internet penetration and dependency, the agencies and people involved would not be too many. Hence, preparing for such a cyber or information attack is today, feasible. Also there is general awareness among those who control the networks. **In theory it is thus possible to reach out and ensure a system.** With greater penetration and cross linkages this will become more difficult in the years to come. Hence the urgent need for building a solid foundational structure today.

NCIIPC. NCIIPC is the lead agency. At present it is under the NTRO which primarily has an intelligence charter. This restricts its open interaction. Role of the NCIIPC is going to increase and unless it works closely with all the stakeholders both, public and private, the trust mentioned above, may never be built up. It thus has to be independent or under the planned NCSCC with representation from all stakeholders to generate confidence and faith. This will also allow it to determine priority sectors and interdependencies. Consequently it will be able to develop sector-specific guidelines and SOPs. State Governments, CII and other federations need to be involved. **A web of CERTs has to be created. Regular meetings need to be mandated and record of progress maintained.**

Banking and Finance. While vulnerabilities exist in all sectors, current trends indicate that the banking and financial sector needs special attention. The Digital India drive with thrust for a cashless economy as also cyber crime on the one hand and an under prepared public along with shortage of trained staff on the other, is an explosive mix. Most financial institutions zealously guard their vulnerabilities and breaches are seldom reported. Cost constraints dominate and investment in security is generally kept to the minimum. The insider threat is all pervading. A financial CERT was envisaged but never took off. A new ReBIT (Reserve Bank IT Private Ltd) has been set up with an ambitious charter. A perusal of website however reveals that it is in a nascent stage with most vacancies yet to be filled. This needs to be accorded utmost priority and trust built up. The fact that it is headed by a renowned IT expert[9] from the private sector is a good indicator. What is essential is that it in keeping with the electronic age, it must work in a digital and flexible manner. More importantly, it must find presence in each State.

"The Digital India drive with thrust for a cashless economy as also cyber crime on the one hand and an under prepared public along with shortage of trained staff on the other, is an explosive mix. ..."

Other Sectors. Post the war games and assessments mentioned earlier, network of CERTs need to be set up in other sectors. Section 70 of the IT Act 2008 sanctioned formation of National agencies like the NCIIPC and CERT-IN. This network must develop to meet the needs of India's federal nature and be flexible as interdependencies will continue to evolve, e.g. linkages of the Energy Sector with Transportation as also IT and Communication. These may not be formal. The objective is to meet as often as possible, review live possibilities of damage and based on need, build faith and systems. Penetration testing of critical systems and cyber audit must become obligatory. **If the Companies Act makes internal and external financial audit mandatory, similar provisions need to be enacted for cyber systems in respect of critical infrastructure.** Section 6A of the IT Act covers provision of IT related services and charges by Government notification. Sections 43 and 43A mention requirement to protect networks and data. All this to include regular IT meetings, can be legislated to compel managements. Shri Ravi Shankar Prasad had mentioned this and the need for legislation in November 2016[10]. **Specific norms and checks also need to be laid down by formal audit to counter the insider threat.**

Human Resources (HR). Shortage of personnel has been mentioned earlier. The Cyber Security Policy 2013 mentions training of five lakh cyber professionals. Given need and scope for employment generation, this should be easy to implement. Once compelled, all ISPs and agencies will have to create cyber workforces which will generate demand. Sponsored programmes such as 'US Air Force Cyber Patriot'[11] can be initiated at no cost to the state to identify a cyber pool. Similarly, funded events like Black Hat Conventions[12] also need to be initiated. There is one for Asia in Singapore. India with its size needs a country specific one. Notwithstanding the cut downs envisaged in outsourcing, the need for IT professionals is going to increase and India is well placed to provide the HR. Thus here too, it is a win-win.

Crisis Response Capability. The NSCS or NCSCC needs war-game situations and in a manner similar to disaster management and ensure back up forces. The proposal for Cyber Territorial Army Battalions needs immediate implementation. These would comprise personnel from all spheres in the IT field who could be enrolled to augment resources in crises and provide for immediate repair and resuscitation. Back-up facilities especially power and communication needs to be created for all critical services. If mandated, costs will be defrayed.

"The NSCS or NCSCC needs to war-game situations and in a manner similar to disaster management and ensure back up forces. The proposal for Cyber Territorial Army Battalions needs immediate implementation. ..."

International Cooperation. A **'Framework for the US-India Cyber Relationship'** was signed on 30 August 2016[13]. While terror is not specifically mentioned, the text covers protection of critical infrastructure and measures for national security. A similar agreement was signed with Russia during the BRICS Summit in October 2016. Though the document is not public, it allows government agencies to work together on counter terrorism[14]. Terror is a universal concern. Cooperation with like-minded countries specially, those which are threatened must become a priority. Expertise of countries such as Israel can be sought for the Indian scenario. It may also be advisable to reach out to nations like Taiwan, who have not only been targeted, but also understand the Han psychology. International cooperation also generates confidence building and deterrence value, as also consensus for global

norms and conventions to protect non-combatants and citizen services.

Indian Defence Minister Manohar Parrikar and US Defence Secretary Ashton Carter, signed the logistics agreement and discussed the CISMOA and BECA agreements during the former's visit to the US on August 30, 2016. Source: Defense News

Social Media. Social media is the new rage in Psy-War. This is more so for a large and open society like India. Bots and false identities abound. There are reports of fake Tweets[15] used by promoters for their cause. Facebook reported over 83 million[16] fake identities in 2012. 2016 witnessed the splurge in 'fake news' in the USA. Evil spreads like wild fire and incites passion. Its use can influence elections, cause disharmony, riots, distrust with attendant harm. Constant monitoring of what is trending, quick and transparent response from credible institutions is need of the day. Both governments and social media networks can together work to establish 24x7 credible fact checking organisations to counter this malaise. Two recent examples are:

- Facebook declared in September 2016 that it has become a member of the First Draft News Coalition, a Google-backed organization that includes partners such as Twitter, the New York Times, CNN and the Washington Post. The aim of the coalition is to help these organizations manage the process of verifying true stories and stopping their spread. Facebook also announced in December 2015 it would begin to address the fake news problem by making such news easier to report and by working with fact-checking organizations.

- BfV, Germany's domestic intelligence agency confirmed that a cyber-attack in December 2016 used the same 'attack infrastructure' as a 2015 hack of the German Parliament attributed to Russian hacking group APT28[17]. BfV further stated that it had seen an *"enormous use of financial resources and the deployment of a wide variety of Russian propaganda tools to carry out disinformation campaigns aimed at destabilising the German government"*. German officials stated that they were creating a separate branch of the government press office that would specifically evaluate and respond to fake news items. Other countries too, are doing so too.

Cyber Forensics. Good forensics can trace most messages and tweets. There are also systems to identify sources of attacks by studying patterns. USA used these to identify those of PLA Unit 61398 whom it charged. **This is also necessary to counter the insider threat where own networks are under some degree of control.** Cyber forensics is a growing field not only for information security but also crime. It thus has employment spinoffs. Sadly, this has not received its due and Post Graduates in this field in India continue to languish. Setting in place norms mentioned earlier is thus, necessary. Here too, international cooperation would help.

Conclusion

India is in a neighbourhood in which inimical forces and anti-India frenzy abound. The Nation has been a target of terror and asymmetric warfare for over quarter of a century with no possible end in sight. Cyber war with its advantageous ambiguity and possibility of visible impact through a terror attack in this domain, is a live possibility. Collusion between China and Pakistan in this sphere needs to be considered and planned for. The threats and challenges have been outlined as also pragmatic measures that can be put in place. **The measures are such that they, in the long term will not only make India more secure, but alongside generate employment and awareness for its digital path. They are not only a necessity to protect its people, but can be achieved at fraction of the cost vis-à-vis what the nation spends on conventional defence.**

> *"Collusion between China and Pakistan in this domain needs to be considered and planned for. ..."*

Most of what has been recommended can be implemented under present structures and laws. Building awareness and realization of this 21st Century phenomena is however, the key. Its unseen potential needs understanding and response. War-gaming scenarios; mandating regular and wider discourse as also audit; strict norms to guard against the insider threat; building trust and involvement should be the new mantras. Rapid advancements in IT and increased dependency on matters

digital have brought about this necessity which the Government can only ignore at its peril. **Uri or Pathankot will be insignificant to what the CPCC can achieve. The time to prepare and act is NOW**.

***

References:

1. The Challenge of Information Warfare. China Military Science (Spring 1995).
2. US Department of Justice Office of Public Affairs, Monday, 19 May 2014.
3. Meeting of the Political Bureau of the Communist Party Central Committee, 29 August 2014.
4. CNN, Katie Hunt and Cy Xu, 7 October 2013.
5. India Today, Manu Pubby, 20 August 2014. Security Affairs, Pierluigi Paganini, 21 August 2014.
6. Cyber War, Richard Clark, 2010.
7. Statement by Shri Ravi Shankar Prasad, Former Minister of Telcom, 1 September 2016.
8. NCIIPC Mission 2014.
9. Mr Kiran b Karnik, ReBIT website.
10. Economic Times 11 November 2016.
11. Website www.uscyberpatriot.org.
12. Website www.blackhat.com.
13. US Embassy Website. Signed by Ambassador Richard Verma and Dr Gulshan Rai on 30 August 2016.
14. ORF Report by Arun Mohan Sukumar of 15 October 2016.
15. Economic Times 24 January 2017.
16. Regulatory filing by Facebook with US, Securities and Exchange Commission in 2012.
17. The Guardian www.theguardian.com, 9 January 2017.

Delhi Policy Group
Core 5A, First Floor, India Habitat Centre
Lodhi Road, New Delhi 110003
Phone: +91 11 48202100
Website: www.delhipolicygroup.org
Email: dg@dpg.org.in; dgoffice@dpg.org.in

DPG POLICY NOTE
Volume II, Issue 2
March 2017