Cyber Non-State Actors:The Cyber Taliban
Colonel Sanjeev Relia@

Introduction

The world has got completely hooked to the information technology revolution. Computers, smart phones and internet have invaded into our lives to such an extent that our day to day functioning is now completely dependent on them. As we become more reliant on these technologies, we also expose ourselves to the dangers lurking around in the cyberspace. Cybercrime is one such danger. Millions of dollars are lost to cybercriminals every year. Yet cybercriminals are not the ones who pose the gravest of threats. It is the threat of presence of non-state actors in cyber domain that is worrying nations today. The very nature of cyberspace makes them a potent force that will play a pivotal role in any future cyberwar.

Non-State Actors and Cyberwarfare

While warfighting is all about opposing armies battling it out and dominating each other in the air, sea and on land, non-state actors too have always played some role in all conflicts. The best example in the Indian subcontinent is the “Mukti Bahini” the Bengali resistance that fought against the Pakistan Army by the side of Indian Army during the Bangladesh Liberation War in 1971. Tasks from espionage to surveillance to physical combat all have been undertaken in the past by such armed non-state actors. But in the cyberspace this may not be the case. While in an armed conflict, it is the armed forces that play the most vital role, in a conflict through the cyberspace, non-state actors may play a larger role than the armed forces would do in waging a war through this domain. This would be more so when the two nations are not in a state of armed conflict but hostilities do occur between them; e.g. India and Pakistan. We are not in a state of war, yet the relations between the two countries are not cordial. In such circumstances, non-state actors based in Pakistan and supported by Pakistan army/ government will play a crucial role in attacking our critical info-infrastructure through the cyber domain with the Pakistan army/government completely denying any involvement.

So who is a non-state actor in the cyberspace? They could be anyone from an ordinary citizen to a patriotic hacker to a cybercriminal to a cyber terrorist or even cyber militia. Past experiences of cyberattacks on Estonia in 2007 and Georgia in 2008 clearly show that the Russians, alleged of originating these attacks, completely denied any of its state machinery being involved in the attacks. Anonymity is a characteristic of cyber domain. The state machinery can, therefore, easily hide behind non state actors with little or no risk of attribution and deny any involvement in perpetrating devastating cyberattacks. In fact, the ease with which a cyber militia can operate and carryout cyberattacks, make them a better choice than establishing a full-fledged cyber wing as part of the armed forces.

What is Cyber Militia?

A cyber militia can be defined as a group of volunteers who are willing and able to use cyberattacks or other forms of disruptive cyber actions in order to achieve a political goal.1 They are men, not in uniform but motivated enough to be employed in covert government-orchestrated campaigns with the purpose to further the strategic political or military objective of the instigating state. It is said that China has established PLA Unit 61398 based at Shanghai staffed by thousands of computer professionals as “Cyber Troops” acting on direct orders of PLA.2 Unit 61398 is supposed to be responsible for all major cyberattacks and cases of cyber espionage against the USA and other countries including India. China on the other hand completely denies even existence of any such unit, leave alone its involvement or connection of any other state machinery. But if reports in the western media are to be believed and also if Snowden revelations are correct, then China does have a potent group of non-state actors organised in the form of Unit 61398, acting completely under the control of PLA.

Employing cyber militia in place of regulars has tremendous advantages. Some of these are:-

(a) **Counterstrike.** Although employing non-state actors to carry out cyberattacks might raise suspicion in the international community, the lack of any hard evidence will protect the attacker of any political ramifications. Thus, the threat of a counterstrike is negligible. In 2007 while all evidence showed that the Distributed Denial of Service (DDoS) attacks on Estonia originated from Russia, Estonia or the NATO could not retaliate due to lack of attribution. While Russia completely denied any involvement, the execution may have been carried out by patriotic cyber militia on behest of the Russian government.

(b) **Cost Factor.** To raise a well organised cyber wing as part of the government or the defence forces would cost a lot of money as such a force will have to be funded and manned by uniformed personnel. By recruiting suitably motivated and technically competent non-state actors, the same task can be achieved at little or no cost. Small nation states today by sponsoring such cyber militia at negligible costs can threaten the critical infrastructure of much bigger and stronger nations.

(c) **Sponsor Cyberwar.** Non-state actors with the backing of state machinery can form unholy alliances, where state provides advanced capabilities in the form of money or actual intrusion tools to non-state actors who can then pass them on to another state or its non-state actors which wants to build cyberwar capability. As on date there are no international laws or treaties banning such actions. Hence, sponsoring a cyberwar through transfer of such technologies via non-state actors is perfectly legal, or atleast beyond reproach.

(d) **Freedom to Attack from Anywhere.** Non-state actors need not be based in the same country which is sponsoring them. Cyberspace knows no boundaries. Hence, the attack can be carried out with the same precision and impact with the attacker based in a third country. This makes the task of the attacking another nation even easier as attribution becomes even more difficult in such cases.

(e) **Laws of War do not Apply.** Even if an indisputable link is established between a non-state proxy and a nation-state, no laws of war apply to these cyber militias. This is because status of such non-state actors

cannot legally be considered to be that of combatants. Also, in some cyberattacks, no physical damage may be caused by these cyberattacks; hence laws of armed conflict do not apply to them. Therefore, such non-state actors in the cyberspace may get away from being tried for war crimes despite the attacks having the same devastating impact as physical attacks.

Raising and employment of such cyber militia forces may have a flip side too. Just like there are no good or bad terrorists, similarly, there are no good or bad hackers. Armed with adequate knowledge and skills, the same attacker may turn against the state and threaten own infrastructure. They may even blackmail the government in order not to disclose sensitive details. Contracted cyber espionage agents might defect to the opposing nation if offered political asylum and cause damage like it happened in the case of Edward Snowden. However, the advantages of using such non-state actor outweigh the drawbacks. This is the reason that a number of nations are preferring employment of such forces instead of employing regular troops to attack the opponents through the cyber domain.

What Threat Does India Face from Cyber Non-State Actors?

Anyone who deals with the cyberspace would know about Stuxnet and the crisis the computer worm created for Iranian nuclear programme in 2010. But many of us would not be aware that Stuxnet was detected in Indian hardware too. Based on a study of the spread of Stuxnet conducted by 'Symantec' an American computer security company, the most affected countries in the early days of the infection were Iran, Indonesia and India. As per a report released by Symantec in September 2010, 8.31 per cent computers in India were found infected with Stuxnet.3 Stuxnet was designed to attack systems using certain specific software namely Windows Operating System, Siemens PCS 7, WinCC and STEP7 industrial software applications and one or more Siemens S7 PLCs. Only when presence of all software was detected by the worm, would Stuxnet be activated. If complete criteria were not met, the worm was programmed to destroy itself. This clearly indicates that Stuxnet was designed to target computers specifically associated with Supervisory Control and Data Acquisition (SCADA) systems as such software is found in SCADA/industrial control systems.

So how did the worm manage to reach well protected hardware in Iran and India and what damage was caused by it in India? Obviously no nation state was directly involved in perpetrating Stuxnet attack. The sophistication with which the worm's code was written and the lethality with which it carried out its task indicates that it was not a handiwork of some novice hacker. As no money or information was stolen by the exploits of the worm, it is unlikely that some motivated cyber criminals created and planted it to steal either money or information. That leaves only one option. The precision with which Stuxnet attacked SCADA systems indicate that it took a lot of planning and effort in implementation of the attack. Such a task could have been done either by cyber terrorists or non-state actors acting on behalf of some state. The same people who perpetrated the worm attack in Iran, also perhaps infected Indian systems also. While the damage caused by Stuxnet in Iran is well documented, unfortunately no survey is available in the public domain which could establish the nature of damage that may have been caused in India by it. Though some reports in the media indicate that INSAT- 4B a communication satellite launched by India in 2007 and which effectively went 'dud' in 2010 due to failure of its transponders affecting 70 per cent of Direct to Home services in India was a handiwork of Stuxnet.4 The same has though not been confirmed by either ISRO or by Siemens whose software the satellite was using. Whether the satellite went 'dud' because of Stuxnet or not, the mere fact that such a deadly computer worm was able to penetrate unnoticed into control systems of our satellite network (if the Forbes report is to be believed), is an indication of the penetration capabilities of offensive cyber tools available today with rogue elements.

Sabotaging the Critical Info-Infrastructure. The above two incidences clearly indicate that networks and infrastructure in our country are vulnerable to cyberattacks, specifically by non-state actors acting on behalf of states like Pakistan or China. Sabotage is an integral part of Cyber Warfare. Malicious software and cyberattacks are ideal instruments of sabotage. This is especially applicable for sectors which provide direct services to consumers such as Telecom, Banking and Power sector. The above three sectors rely heavily on information and communication technology (ICT) and networking. As all of these three sectors provide consumer services, use of internet is also essential for all three sectors. While it is difficult to attack a standalone network or service, any infrastructure which is connected to the internet becomes more vulnerable to cyberattacks. Therefore these three sectors are specifically vulnerable to well-coordinated cyberattacks resulting in breakdown of their services. State sponsored non-state actors can not only target such critical info-infrastructure but other spheres of life which rely on ICT. As systems become more complex, the knowledge required to attack them also becomes more complex and arcane. Unless the attacker is backed up with full financial and knowledge support, sabotaging industrial control system will be a difficult task. Non-state actors are the only group of cyber adversaries who can achieve such a task with ease as they have all the necessary backing.

Subversion. Another activity which a non-state actor can undertake effectively through the cyberspace against our country is subversion. As per Thomas Rid, a British scholar and writer, information technology has enabled proliferation of subversive causes and ideas. Because of the cyberspace, subversion has become more cause driven, it is seeing higher levels of membership mobility and is now characterised by lower levels of organisational controls5. One common tool of all subversion activity is media, may it be print or visual media. The exponential rise and infinite reach of social media today has made it a perfect tool for subversive activities. The kind of influence social media has on the society has got our government thinking about the impact it can have on internal security of the Country. Today politicians, senior government officials and scholars can often be heard voicing their concern about the negative and subversive impact of social media. A very recent example of this was the exodus of the northeast students from Bangalore and other southern cities in August 2012. Despite appeals and assurances of safety by the Karnataka government, people from the northeastern parts of India working in cities of Karnataka continued to flee the state in hordes. Whatever were the actual reasons for the event, social media was blamed for the massive exodus.

Social media in particular and internet in general are mediums which a non-state actor can exploit for creating an adverse public opinion against the government of the day. Examples of this can be found in the way Arab Spring of 2011 was triggered. Social network, especially Facebook, offered a platform for planning and after action deliberations. The moderators of various Facebook groups that helped spark the unrest remained anonymous during most of the Arab Spring. Even the shutdown of the internet could not prevent the spread of political movement. The

recent arrest of an ISIS Tweeter handler in Bengaluru shows the innovative ways a Jihadi organisation can make use of cyberspace. The IS militant group has made extensive use of social media for propaganda and recruitment, as well as for disseminating gory execution videos. If a banned jihadist rebel group based in Iraq and Syria can so well put to use the cyberspace, imagine how well a state sponsored organisation will be able to use it.

Listed above are just some of the ways a nation can employ non-state actors in the cyberspace. While sabotage, subversion and espionage would be the main motives behind employing cyber militia, there could be many other ways to use them in spreading terror in India using the cyberspace. Our armed forces and other governmental organisations have mastered the ways to counter state sponsored terrorism in J&K and the northeast; we will have to learn innovative methods for fighting actions perpetuated through the cyber domain. Time has come to recognise the potential of non-state actors in the cyberspace and take countermeasures against their likely method of operations.

Conclusion

Non-state actors wield more influence and pose greater national security risks in the cyber domain than they do on land, sea and air. With low barriers to entry and the ease with which technology today is available, a state can achieve its nefarious goals in the cyber domain by proxy non-state actors who can be as effective as a nation state in undertaking precision cyberattacks. It is time that the government took a serious view of this and addressed the issue of cyber conflict with non-state adversaries. It is a must to establish a secure and resilient cyberspace in the Country.

Endnotes

1 Ottis, R., “Proactive Defense Tactics Against On-Line Cyber Militia,” in the proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010), Thessaloniki, Greece, Jul. 2010.

2 China hacking charges: the Chinese army’s Unit 61398 as available at http://www.telegraph.co.uk/news/worldnews/asia/china/10842093/China-hacking-charges-the-Chinese-armys-Unit-61398.html

3 “W32.Stuxnet”. Symantec. 17 September 2010 available at http://www. symantec.com /security_respon se/writeup.jsp?docid=2010-071400-3123-99 viewed on 20 Dec 2014

4 Did The Stuxnet Worm Kill India’s INSAT-4B Satellite? As available at http://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/ viewed on 20 Dec 2014.

5 Cyber War Will Not Take Place by Thomas Rid P115

@ Colonel Sanjeev Relia was commissioned into the Corps of Signals on 20 Dec 1986. Presently, he is a Senior Research Fellow at the Centre for Strategic Studies and Simulation, United Service Institution of India, New Delhi.

Journal of the United Service Institution of India, Vol. CXLV, No. 599, January-March 2015.