IN FOCUS

07 JUN 2014

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

Wg Cdr Ashish Gupta

Research Fellow, CAPS

The anonymity and impunity, with which the acts of cyber terrorism and espionage are being carried out, have made the process of fixing of accountability and subsequent prosecution extremely difficult. Cyber space, being a common entity, shared by government, institutions, companies and individuals, does not offer a sense of security as the physical/ geographical boundaries do. The perpetrators with mala fide intentions do not have to undertake the arduous task of breaching the security over physical boundaries to carry out intended cyber-attacks.

Once the masks of anonymity are taken away and the true perpetrators are identified in flesh and blood, the process of indictment becomes tangible, subject to condition that either the perpetrators belong to the State or are physically present within the legal boundaries of the State. The prosecution of members of "Lulz Sec" of charges ranging from computer misuse, fraud, hacking to "unauthorised impairment of protected computers" is one such example[1]. The members of the group were arrested from various locations in US, Australia, Ireland and UK by respective law enforcement agencies. They were charged under the prevailing laws of respective nations for perpetrating crimes there. However, on 19 May 14, in a first-of-its-kind case, US Justice Department indicted five Chinese military officers on charges of stealing data from six US companies. Other than antagonising China over the issue of economic cyber-espionage, this episode brings to fore a very piquant situation having long term ramifications.[2]

Though the Chinese government has tacitly sponsored the acts of corporate data theft for many years, this is the first time the US has formally accused Chinese officers of involvement. Attorney General Eric Holder announced that US would seek extradition of Chinese officials to face charges under US laws for infiltrating the computer networks of six US companies and for stealing data, which could be leveraged for the benefits by their trade competitors. The FBI has gone to the extent of putting the faces of five officials on 'Wanted poster'. The companies allegedly affected are Alcoa, US Steel, the US Steelworkers Union, Westinghouse, Allegheny Technologies Inc and Solar World.

The Chinese response was on predicted lines calling the allegations "extremely ridiculous". China's foreign ministry spokesman Qin Gang categorically stated that China "never engages in the activity of stealing commercial secrets through the internet." He went to the extent of accusing US of conducting large-scale, organized cyber-theft and cyber-espionage activities against foreign dignitaries, companies and individuals.

The US posture on economic and security matters in cyber-space, appears to be dichotomous, in the back drop of Snowden's revelations of widespread NSA surveillance. While the acts of cyber-espionage for security purposes, even when it entails infiltrating the private lives of its own citizens, is considered as legitimate by US, surveillance intended for economic advantages is not. The NSA has been accused of spying on Brazil's biggest oil company, an act which can't be justified by any logical reasoning to fall within the realm of national security.[3] Petrobras is the largest company in Brazil, with state being the biggest stakeholder. It is a major source of revenue for the Brazilian government. In a placid attempt to distinguish between economic and security surveillance, Attorney General Holder stated, "All nations are engaged in intelligence gathering, but the current indictment involves a state sponsored entity, state sponsored individuals, using intelligence tools to gain commercial advantages, and that is what makes this case different."[4]

In context of international relations, extradition is the formal process regulated by mutual treaty, by which a person found in one country is surrendered to another country for trial or punishment. The country seeking the extradition will request the appropriate agency of the foreign government. The extraditability of an alleged fugitive depends on the sole discretion of government, which normally bases its decision after consideration of charges within its legal framework. The acceptance by the government of any wrong doing by its citizen is the first step in the extradition process. The whole exercise orchestrated by US appears to be an attempt to "send a strong message" to Beijing, though China is not going to buckle under pressure from the supposedly strong arm tactics of US.

ARTICLE BY SAME AUTHOR

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

In the realm of cyber warfare, the question of attributability and accountability is a piquant one. In a hypothetical situation, let us examine a scenario in which a group in State A assimilates computers located in State B into its botnet. The group then uses the botnet to overload computer systems in State C based on instructions received from State D. Though by the conventions of laws of natural justice, the attributability of the conduct rests with State D, it will take a long legal battle to exonerate State A and State B from the responsibility of conduct.

As the situation unfolds, it will give valuable insight to our understanding as to how the identity of these five Chinese officials was established and what was the incriminating evidence against them? It will also be interesting to know the extent to which the Chinese officials could assimilate the computers and networks of these US companies. It will not come as a surprise if one obverses a similar kind of vindictive action by the Chinese government. China will certainly retaliate; hopefully the amount and extent should not impact the economic development of either US or China.

The shroud of anonymity behind which cyber-criminals operate has made the process of establishing the identity of transgressors an arduous one. Attribution is the first step in

assigning responsibilities and seeking legal recourse against transgressors. Present legal system and enacted laws are unable to deter cyber-criminals from writing computer codes useful for launching a clandestine cyber-attack. For rule of law to be effective, it must ensure that the costs of non-compliance exceed the costs of compliance. Anonymity makes the process of assignment of responsibility and imposition of penalties almost impossible. The outcome of this incident needs to be monitored closely as it may provide a tangible recourse for indicting and prosecuting cross- borders cyber-attackers.

(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]" Self-proclaimed LulzSec leader arrested in NSW", available at http://www.abc.net.au/news/2013-04-24/lulz-security-hacking-leader-arrested-in-nsw/4648134, 24 Apr 2013, accessed on 21 May 14

[2] " Chinese military officials charged with stealing US data as tensions escalate", available at http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage, 20 May 14, accessed on 21 May 14

[3] "NSA spying on Petrobras, if proven, is industrial espionage", available at http://www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909, 09 Sep 13, accessed on 21 May 14

[4] " Chinese military officials charged with stealing US data as tensions escalate", available at http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage, 20 May 14, accessed on 21 May 14