IN FOCUS

12 FEB 2014

US DRAWS THE LIST OF ADVERSARIES FOR CYBER ATTACK THROUGH PRESIDENTIAL POLICY DIRECTIVE – 20

Wing Commander MK Sharma
Research Fellow, CAPS

Recent leak of 'TOP SECRET/NOFORN'[i] US Presidential Policy Directive PPD-20[ii] asking National Security Advisor (NSA) to draw list of target nations' systems, processes and infrastructures[iii] against which US should establish and maintain offensive cyber capability has brought to fore some serious consequences of employing offensive cyber warfare capabilities outside the geographic boundaries of any nation state. US plans to employ such capability to support operational and tactical commanders. The agencies involved in drawing such list are – the secretary of defence, the director of national intelligence, the director of NSA, in coordination with Attorney General, the secretaries of state and homeland security, the relevant IC and sector specific agencies.

ARTICLES BY SAME AUTHOR

WHY CHINA WILL PURSUE CYBER WARFARE MORE AGGRESSIVELY?

The directive authorises conduct of mainly two types of operations – Defensive Cyber Effect Operations (DCEO) and Offensive Cyber effect Operations (OCEO), on behalf of US Government in or through cyber space that are intended to enable or produce cyber effects outside US government networks. This is also being viewed as Barack Obama's tough stance against his Chinese counterpart Xi Jinping for ongoing Chinese cyber intrusions on US' critical infrastructures including the most advanced military programmes of Pentagon.[iv]

The 18 page directive though signed on 16 October 2012 but never published, reveals a framework of cyber operations that include – cyber collection, OCEO and DCEO with the provisions of 'Emergency Cyber Action' when there is no time for prior presidential approval. The directive is inherently aggressive and raises fears of increased militarisation of Internet. While the controversy over legality of the use of Stuxnet worm believed to have been launched by US and Israel, that targeted Iranian uranium enrichment centrifuges is still brewing, China has also stepped up allegations of wide spread American cyber attacks of serious nature on its infrastructure.

Such precursors to cyber arms race between US and China only reinforce the postulate that cyber attacks would invariably be used as pre-emptive strike in any future conflict. Also there are some, who argue that, 'When militarist cyber rhetoric results in use of offensive cyber attack it is likely that those attacks will escalate into physical, kinetic uses of force'.[v] Nevertheless, these developments would raise questions on the very definitions of sovereignty, international boundaries and law of land, forcing law enforcement agencies and international law making bodies to rethink.

ARTICLES BY SAME AUTHOR

WHY CHINA WILL PURSUE CYBER WARFARE MORE AGGRESSIVELY?

While the directive in each section talks of prior approval of the President for any cyber operation, two sections are left as exception – firstly, 'emergency cyber action' at page no 3 that authorises several departments including Department of Defence to conduct cyber effect operations inside the US and lastly, it authorises the use of OCEO against systems and infrastructures outside the US without their government's consent whenever 'US national Interests and equities' require such action. In essence it authorises military commanders the use of OCEO at operational and tactical levels, within and outside the US, without seeking prior approval in certain circumstances. Therefore, this directive aims to integrate cyber operations into the US' diplomatic, military, economic, intelligence, and counterintelligence capabilities. Towards which the US shall identify potential targets of

importance where OCEO can serve as the most efficient capability to achieve a given national objective or interest.[vi]

Had it not been by Snowden, another aspect of looking at this development could have been that it might be a deliberately intended leak by US to increase cyber deterrence threshold for China in order to decelerate the ongoing cyber arms race between them, while such vigour in actual policy planning might not be existing. This however would not stand to the logic of cyber deterrence - firstly, that a nation would not show its cyber weapons and plans as the development of counter attacks and defences can be achieved at very low cost against a known cyber threat and lastly, if China is cautioned of such plans it would accelerate building cyber offensive tools in all likelihood defeating the very purpose of such intended leak. Furthermore, in the backdrop of recent major expansion of its Cyber Command Unit, under the command of General Keith Alexander, it seems consistent with US policy to implement such a plan to better understand the potential benefits, determine the degree to which practical and policy concerns are warranted, and determine the best way forward in this poorly understood but possibly revolutionary area of future warfare.

(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)

----------***XXX***----------

[i] Classification of the document as 'Top Secret/ No Foreign State'.
[ii] Presidential Policy Directive 20, U.S. Cyber Operations Policy (Oct. 16, 2012).
[iii]' Presidential Policy Directive – 20', Anenex: Implementation – Policy Review and Preparation, pg 15.
[iv] http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas
[v] Sean Lawson, Assistant Professor in the department of communication at the University of Utah. http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas accessed on 09 Feb 14
[vi] http://www.lawfareblog.com/wiki/the-lawfare-wiki-document-library/post-911-era-materials/post-911-era-executive-materials/presidential-policy-directive-20/#.Uvb_-7T9FLM accessed on 09 Feb 2014.