Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
39/17

EXPEDIENCY AND VIABILITY OF CYBER-ATTACKS TO THWART THE NORTH KOREAN MISSILE THREAT

Gp Capt Ashish Gupta
Senior Fellow, CAPS

North Korea (the Democratic People's Republic of Korea, DPRK) has been keeping the world on tenterhooks with repeated rhetoric about a nuclear response to any attack or intervention in its ballistic missile programme. The security of the North East Asian region hinges on the US' ability to extend an explicit security guarantee to its non-nuclear allies from an increasingly belligerent North Korea. It is emerging as one of the most vexing foreign policy problems facing the US government over the past couple of years. North Korea's nuclear and missile programme, termed as primeval and unrealizable by the Western media some time back, is taking shape in a manner that even threatens the US mainland. Since its first nuclear test in October 2006,[1] North Korea's rhetoric towards neighbouring countries and US has become increasingly belligerent. The world is confronted with an imbroglio of a much more complex kind, one that has consequences for the present and the future. The international sanctions, aimed at economically 'squeezing' Pyongyang to force it to abandon its nuclear weapons and long-range missiles development program have not yielded the desired results. For the U.S., an assortment of options are fast drying up, so much so that the option of possible pre-emptive strikes against North Korean military facilities has not been ruled out in solving the North Korean conundrum, as evident from the statements of both vice-presidential candidates -Michael Pence and Tim Kaine - during the 2016 electoral campaign.[2]

North Korea has made significant headway in improving the effectiveness of warheads and ballistic missiles program and for the first time the regime poses a direct threat to mainland US. These achievements are partially attributable to the success of its *Byungjin* policy.

The DPRK autocratic leader Kim Jong-un, on 31 March 2013, during a plenary session of the Party Central Committee (PCC), announced the adoption of a new strategic posture, which was a transition from his father's Songun ("military-first") strategy. He launched a new political and economic policy of *Byungjin* ("parallel development")aimed at developing nuclear weapons, missile technology and the economy simultaneously.[3]

The Growing Nuclear Threat

The North Korean nuclear program is aimed at achieving two strategic objectives. In addition to using the deterrence value of nuclear weaponsto protect itself, North Korea aims to use these as bargaining chips in its dealing withUSand its allies in North East Asia. According to 2015 estimates, North Korea's nuclear stockpile comprises of 6-8 plutonium-based warheads and 4-8 uranium based devices. On 9 January 2016, Pyongyang announced that it had detonated its first thermonuclear warhead. Although Pyongyang's assertion was received with palpable scepticism, the possibility cannot altogether be dismissed. [4] The international concerns about North Korea grew even more pervasive in the wake of the success of its missile program. Under the *Byungjin* policy, its missile research programme was focused on the implementation of four strategic goals: the development of a new road-mobile missile, the production of a submarine-launched missile, the implementation of the dual-use space programme and the development of solid-fuel rocket technology.

In 2016, the frequency of the missile tests increased manifold as compared with the past and most of these tests were prominently advertised worldwide through media. A total of 21 were launched on 14 different occasions last year. Last year, the majority missile launches (a total of 21) were termed as successful even by the sceptical international observers. *The Hwasong-6, Nodong, Musudan, Taepodong* and *Pukkuksong-1* tests demonstrated North Korea's acquired capabilities in launching medium and long-range missiles from the ground and from the sea as well as their capability to hit the targets with relatively high precision. [5]

The US is exploring multiple options for containing North Korea's missile program and protecting its allies in North East Asia. In an overtly aggressive response, the Terminal High Altitude Area Defense (THAAD) anti-ballistic missile system was deployed in the Korean Peninsula to provide enhanced nuclear protection to South Korea. Despite vociferous opposition by China - which fears that THAAD system will hinder its ability to retaliate in the event of nuclear coercion or war with US- the system is slated to become operational by the end of the year. In the beginning of May 2017, the US conducted joint bomber drills with the South Korean air force, using two B1-B bombers, and

which was described as a "nuclear bomb-dropping drill" by North Korea.[6]

The media was abuzz with the news that on April 29, 2017, when Pyongyang tested another long-range missile, the missile only flew "for several minutes" before disappearing from radar. It was the second failed attempt in quick succession when another missile exploded just after launch. The needle of suspicion invariably turned to US involvement. However, when asked about it on "Face The Nation" TV show, President Trump refused to comment on US' involvement with Pyongyang's latest string of failed tests. But according to some foreign policy observers, Trump "hinted" that the Pentagon was sabotaging North Korea's nuclear efforts.[7]

While President Trump's "hint" is subject to numerous interpretations, a covertly executed cyber operation by US against North Korean missile systems is more than a matter of mere speculative conjecture. This issue is being hotly debated by the strategic community. The circumstantial evidences and past experiences have established with reasonable certainty that the US could have used cyber weapons in an effort to thwart Kim's weapons programs. Those who believe that the two failed missile launch tests by North Korea were due to a cyber-attack by the US, keep quoting the example of *Stuxnet*, which was a complex cyber weapon, developed with the specific objective of penetrating and compromising a specific uranium enrichment facility in the Iranian city of Natanz. The year 2009 witnessed the arrival of Stuxnet in the cyber warfare arena and the aftermath of the Iranian crisis made the security community sit back and take notice of the severity and effectiveness of a cyberattack. Some were quick to label the Stuxnet worm as an "evolutionary leap" unprecedented in its functioning, unpredictable in its actions, catastrophic in its effects and unimaginably successful in its ultimate consequences.

Some experts believe that President Trump has inherited a mandate from former President Obama, when Obama ordered Pentagon to step up its efforts to carry out cyber and electronic strikes against North Korea's missile program and try to sabotage missile test launches in their initial launch phase. Those who support such efforts believe that failed missile attacks of North Korea are an assertion of achieved capability of US to successfully use cyber weapons. But other experts are sceptical about the effectiveness of cyber weapons, arguing that a host of human, manufacturing and operating errors could destroy a test missile in its initial launch phase.[8]

In 2014, the Obama administration concluded that US $300 billion had been spent since the Eisenhower era on *antimissile systems*. In spite of the fact that such colossal amount of money and effort has been spent, the core objective of comprehensive protection of

America's homeland against missile attack is still untenable. Flight and effectiveness tests of missile interceptors under near-perfect conditions in US had an overall failure rate of 56 percent, which is likely to be far worse in real combat. This has resulted in intensification of efforts to develop cyber and electronic strike capabilities for missile interceptions. Besides, the use of cyber weaponry to remotely manipulate data inside North Korea's missile systems is the only alternative available with US because all other efforts to dissuade or stop North Korean missile program have already failed or are slated for failure.[9]

India and the Scourge of Stuxnet

The scourge of Stuxnet came to India in 2010 which was one of many countries infected and affected by Stuxnet; it was reported that India had the third-highest damages. According to media reports, of the 10,000 infected Indian computers at the time, 15 were located at what are called 'critical infrastructure' facilities.[10]On July 7, 2010, the Indian INSAT-4B satellite had a power glitch in its solar panels resulting in shutting down of 12 of its 24 transponders. It was speculated that INSAT-4B, which was put into orbit in March, 2007, was effectively rendered inoperable due to the Stuxnet effect. According to some sources, Indian Space Research Organization (ISRO), at its Liquid Propulsion Systems Centre, was using the Siemens software (In Iran, the control system made by Siemens were specifically targeted by Stuxnet), which could have activated the Stuxnet worm. The timing of discovery of Stuxnet and power glitch in INSAT-4B satellite also coincided which gave more credence to the Stuxnet effect.[11]

Speculations were also rife that failed launches of GSLV and Prithvi could be attributed to the presence of Stuxnet in ISRO and DRDO systems as Symantec reported that eight per cent of all Stuxnet infestations were reported from India. The seriousness of this can be gauged by the fact that on December 13, 2010, the same question was put before the Parliament seeking government's official response.[12] Though the government assured that no defence establishment in India had reported being affected by the Stuxnet worm, the serious concerns of various agencies about security of Indian satellites and missiles can be palpably and visibly felt.

Conclusion

The year 2016 was pivotal for DPRK's missile program. A series of missile tests demonstrated Pyongyang's technological advancement and heightened the threat perception of both the US and its allies in North East Asian region. Since the beginning of 2017, Kim Jong-un's rhetoric took on a more sinister tone with promise of testing of a new ICBM that can potentially target the US. The US has to explore and use all options available to it, and one of these is the use of cyber weapon. Cyber-attacks can manifest in various

forms and are often stealthy and unnoticeable. The consequential severity of attacks remains unpredictable. Because of the element of surprise, anonymity and attributability, cyber attacks are weapons of stealth and silent insinuation. It is yet to be established beyond reasonable doubts whether North Korea's failed missile tests were due to cyber-attacks by the US. Nonetheless, cyber weapons have such capabilities and any system which uses reasonably modern technology is inherently vulnerable to cyber-attacks.

(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])

Notes

[1] Amanda Erickson, "A timeline of North Korea's five nuclear tests and how the U.S. has responded", *The Washington Post*, April 14, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/04/14/a-timeline-of-north-koreas-five-nuclear-tests-and-how-the-u-s-has-responded/, accessed May 12, 2017.

[2] Anna Fifield, "North Korea Is 'Racing Towards The Nuclear Finish Line'", *The Washington Post*, October 08, 2016, http://www.ndtv.com/world-news/north-korea-is-racing-towards-the-nuclear-finish-line-1471723, accessed May 12, 2017.

[3] Lorenzo Mariani, *Assessing North Korea's Nuclear and Missile Programmes: Implications for Seoul and Washington*, IAI Working Papers 17, March 1, 2017.

[4] Ibid.

[5] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles", *The New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=1, accessed May 12, 2017.

[6] Jared Keller," Is The Pentagon Really Sabotaging North Korea's Missile Tests With Cyber Attacks?", *Task & Purpose,* May 2, 2017, http://edition.cnn.com/2017/05/02/asia/thaad-south-north-korea/ , accessed May 12, 2017.

[7] Ibid.

[8] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles", *The New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=1, accessed May 12, 2017.

[9] Ibid.

[10] Anirudh Bhattacharyya, Stuxnet hits India the most, The Hindustan Times October 04, 2010, http://www.hindustantimes.com/world/stuxnet-hits-india-the-most/story-KMX3bWo7kNG5Az6IXK3NKM.html, accessed May 12, 2017.

[11] Ibid.

[12] Lok Sabha Unstarred Question No. 5452, "Cyber Warfare Strategy", answered on 13.12.2010