COULD CYBER ATTACKS DEFEAT NORTH KOREAN MISSILE TESTS?

The NAPSNet Policy Forum provides expert analysis of contemporary peace and security issues in Northeast Asia. As always, we invite your responses to this report and hope you will take the opportunity to participate in discussion of the analysis.



Recommended Citation

Markus Schiller and Peter Hayes, "COULD CYBER ATTACKS DEFEAT NORTH KOREAN MISSILE TESTS?", NAPSNet Policy Forum, March 06, 2017, https://nautilus.org/napsnet/napsnet-polic--forum/could-cyber-attacks-defeat-north-korean-missile-tests/

Markus Schiller and Peter Hayes

March 6, 2017

I. INTRODUCTION

This essay by Markus Schiller and Peter Hayes suggests that it is improbable that US cyber attacks were the cause of DPRK intermediate range missile failures as was suggested in a March 6, 2017 *New York Times* story.

Markus Schiller is an aerospace engineer, with rocket analysis experience gained at Schmucker Technologie and RAND. In 2015, he started the rocket and space consulting company ST Analytics in Munich. Peter Hayes is Executive Director of Nautilus Institute and Honorary Professor at the Center for International Security Studies, University of Sydney.

Acknowledgment: This report was funded by MacArthur Foundation.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Credit: Banner photo is from March 21, 1988 video of the US Navy's first Trident II Performance Evaluation Missile (PEM-1) test launched from USS Tennessee off the coast of Cape Canaveral, Fla.

II. POLICY FORUM BY MARKUS SCHILLER AND PETER HAYES

COULD CYBER ATTACKS DEFEAT NORTH KOREAN MISSILE TESTS?

March 7, 2017

On March 6, 2017, the *New York Times* published an article[1] that stated that the United States deployed cyber attacks against North Korea's missile tests. The article implied that these attacks may have succeeded in causing the failure of North Korean missile tests, stating:

> *The North's missiles soon began to fail at a remarkable pace. Some were destroyed, no doubt, by accident as well as by design. The technology the North was pursuing, using new designs and new engines, involved multistage rockets, introducing all kinds of possibilities for catastrophic mistakes. But by most accounts, the United States program accentuated the failures.*
>
> *The evidence was in the numbers. Most flight tests of an intermediate-range missile called the Musudan, the weapon that the North Koreans showed off in public just after Mrs. Clinton's warning, ended in flames: Its overall failure rate is 88 percent.*

This article set of a buzz of commentary about the wisdom of such attacks against a nuclear armed state.[2]

The assertion that cyber attacks could cause a higher rate of failure than would otherwise have occurred is, to put it mildly, a stretch, given the intervening variables and other factors that are well known to cause high failure rates early in missile testing programs. It is useful, therefore, to examine the fundamentals of how a missile could be caused to fail by a cyber-attack.[3]

Fundamentals of Missile Guidance

In principle, interference with a missile's guidance system may cause it to veer it off course, or even

destroy it in flight. What happens when the missile continuously steers into the same direction can be seen here:

But this is not as easily done as people would imagine, or as is suggested in the *New York Times* article.

To mess with a guidance system by hacking into it, it has contain a computer system that uses software. This sounds very obvious, but it is very important to be reminded of this, because different rockets use very different guidance system.

The Falcon 9 space launcher from SpaceX, for example, uses a guidance system with a software that is based on Linux. It should be possible to hack this software, or plant some virus in it that does something weird during launch. To do this, the attacker must be able to meet two conditions. First, the attacker must know which software is used, and understand how the software is working to create compatible lines of code that actually do what you want them to do, and to plant this code into the existing software.

Second, the attacker must have access to the software, either by direct access to the guidance system you want to sabotage, or by infecting the software before it is transferred into the missile's computers. Also, the malware should not be detected once it is planted.

Certainly the DPRK would have established a guidance laboratory early in its missile program to develop accelerometers, gyroscopes, computers, and inertial platforms in the quest for an indigenous inertial guidance system and developed the transformation techniques needed to convert inertial measurements into targeting information.[4] However, the DPRK is not yet capable of developing and producing the required sensors and computers and has had to buy in many of these parts from the world market. The chances that the United States could identify and implant malware in such black market imports are low.

Moreover, it is not likely that that the DPRK would have failed to take cyber warfare defensive counter-measures to protect its guidance research and development program. Of course, all bureaucracies make mistakes, especially when operating in compartmentalized, vertical silos like those in the DPRK. But it is unlikely that the DPRK military did not mount cyber defenses given that it was forewarned by media reports in 2011[5] of the Stuxnet attack on Iran's centrifuge program. It may also have been aware of the US National Security Agency attempts starting in 2010 to penetrate North Korea's cyber systems[6] And it certainly has highly capable and world class cyber warriors to lend a hand.

Even if the DPRK missile guidance system community let down its guard, US knowledge of North Korea's missile program is quite limited. It is doubtful that the United States has sufficient knowledge of the DPRK's missile guidance software code, or even which software is used. It is also highly improbable that the DPRK's missiles have a WiFi link, or Internet access, which could be used to infect the guidance software.

But, even more basic: some missile guidance systems cannot be hacked, because they are not software-based.

The Scud B guidance system, for example, is quite close to the guidance system that the German A4/V2 used during World War 2. This system is based on mechanical inputs. You cannot hack it, just as you cannot hack old Wurlitzer jukeboxes, or mechanical computers. There is no software, no line

of code that could be modified.

Scuds, of course, use a Scud-type guidance system, as does the Nodong. And judging by the technology that was found inside the Unha first stage, the Unha satellite launcher also uses some kind of this guidance type, perhaps just a modified Scud guidance system. There is simply no way to infect these systems with malware.

Musudan and KN-11 Guidance Systems

The question today is whether the DPRK's Musudan and the KN-11 missiles use a similar non-cyber guidance system; or if they use some type of modern strap-down guidance system that is based on sensors and a computer, and is running some software. And this question leads us straight to the old questions of where these missiles come from, what technology they are based on, and at what time they were actually developed.[7]

If the Musudan indeed is based on the R-27/SS-N-6, the chances are high that the original guidance system of this missile was also used for the Musudan, which means Soviet technology from the nineteen sixties, which would have been mechanical and therefore "hack-proof".

Even if the DPRK uses a modern guidance system on the Musudan, it is doubtful that the United States would have had access to the guidance software and be able to plant a code in there. And missiles do not have an USB port that you can use to infect their computer via USB stick, or just connect from a distance via Bluetooth. Such an insertion would have to be highly targeted, specific to the design and software used in the DPRK's laboratory, and able to circumvent all the obvious countermeasures and barriers that would stand in the way of such an effort in the first place. Such a combination strains credulity.

Conclusion

The *New York T*imes article hearkens back to the movie "Independence Day", where the world is saved from the Alien invasion by simply planting a computer virus into the mothership's main computer by somehow just sending it over with a standard laptop. This might work in movies, but not in reality.

Perhaps the more interesting story is who leaked to the New York Times the claims of the efficacy of cyber attacks on North Korea's missiles and why now? We wonder if it is part of a policy battle in the course of the Trump Administration's North Korea policy review,[8] possibly designed to get President Trump's attention. It might also be an intentional effort to conduct psychological warfare against the DPRK by creating paranoia and purges within the DPRK missile program. It might also be a way to impress allies and third parties that the United States has been doing more behind the scenes than patiently waiting for the DPRK threat to resolve itself and imposing ineffectual sanctions. We don't know.

III. REFERENCES

[1] D. Sanger, W. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times*, March 4, 2017, at: https://mobile.nytimes.com/2017/03/04/world/asia/north-kore--missile-program-sabotage.html?smprod=nytcore-iphone&smid=nytcore-i-hone-share&_r=0&referer=

[2] K. Waddell, "Is It Wise to Foil North Korea's Nuclear Tests With Cyberattacks? "This could set off very serious alarm bells in Beijing and Moscow,"" *The Atlantic*, March 5, 2017, at:

https://www.theatlantic.com/technology/archive/2017/03/north-korea-cyberatta-k-nuclear-program/518634/

[3] See J. Constant, F*undamentals of strategic weapons: offense and defense systems,* 2 volumes, James Constant. Nijhoff, 1981, at: http://www.springer.com/gp/book/9789401501576

[4] For an introduction to missile guidance systems, see Arnold Engineering Development Center, *Short-Range Ballistic Missile (SRBM) Infrastructure Requirements for Third World Countries,* AEDC-1040S-04-91, Arnold Air Force Base, Tennessee, September 1991, pp. 31-36, at: https://nautilus.org/foia-document/short-range-ballistic-missile-srbm-infrastructure-requi-ements-for-third-world-countries/attachment/short-range-ballistic-missile-srbm-infra-tructure-requirements-for-third-world-countries-1991/

[5] W. Broad, J. Markoff, D. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, January 15, 2011, at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[6] D. Sanger, M. Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times,* January 18, 2015, at: https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

[7] On which see T. Postol, M. Schiller, "The North Korean Ballistic Missile Program," *Korea Observer*, 47:4, Winter 2016, pp. 751-805, at: http://www.iks.or.kr/board/index.html?id=vol47no4

[8] Lee, A. Gale, "White House Explores Options, Including Use of Military Force, To Counter North Korean Threat, The strategy review comes as recent events have strained stability in Asia," Wall Street Journal, March 1, 2017, at:

https://www.wsj.com/articles/white-house-explores-options-including-use-of-military-force--o-counter-north-korean-threat-1488407444

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

View this online at: https://nautilus.org/napsnet/napsnet-policy-forum/could-cyber-attacks-d-feat-north-korean-missile-tests/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org