Piercing the Fog of Data

Using Activity Based Intelligence to Combat the North Korea Missile Problem

Maj William Giannetti, USAFR

2017 was a banner year for Kim Jong Un and North Korea. Tensions between Pyongyang and Washington rose to an all-time high, and Kim has been eager to prove his credentials as a shrewd political thinker and military strategist. A provocateur like his father and grandfather before him, he launched 20 missile tests—all in violation of international sanctions.[1] Media sources reported that North Korea is irretrievably bent upon becoming a nuclear power. Since 2006 it has conducted six underground nuclear tests at Pungyee.[2] With probably its most hyperbolic rhetoric to date, the reclusive regime in Pyongyang threatened to launch "super-mighty" preemptive strikes against the US mainland and to turn Seoul into a "sea of fire."[3]

Officials in Washington expressed their exasperation about these developments. "The policy of strategic patience has ended," said Secretary of State Rex Tillerson on 16 March 2017, marking the White House's departure from Obama-era national security policy.[4] The USS *Carl Vinson* strike group was sent on a five-month deployment to the Western Pacific in a show of military might. The USS *Ronald Reagan* spent the summer patrolling the Sea of Japan. An advanced, missile-killing terminal high-altitude air defense (THAAD) battery deployed to South Korea to reassure our allies in Seoul and Tokyo. For almost eight years, the US and South Korea called, in vain, for a return to economic engagement with North Korea. Both nations offered to halt annual joint military exercises in the hopes that North Korea would reciprocate by curtailing its nuclear and missile programs. US and North Korean diplomats discussed the possibility of talks toward a peace treaty—a long-awaited event because the Korean War (1950–1953) ended in an armistice and an uneasy return to the *status quo ante*. Pyongyang seemed amenable to discussing a treaty in principle, but the nuclear issue was out of the question. "Diplomacy," according to *Foreign Affairs*, "has failed because Pyongyang remains determined to build its nuclear arsenal."[5]

Then, on 4 July 2017, things took a dramatic turn: North Korea test-fired an intercontinental ballistic missile (ICBM).[6] Even as President Donald J. Trump threatened "fire and fury" against it, Pyongyang stayed its course. In September 2017 Pyongyang undertook its largest nuclear test, which triggered an earthquake of 6.3 magnitude, a

seismic reading that suggests a thermonuclear weapon was detonated.[7] US and international pressure notwithstanding, in September and November Kim launched two more ICBMs.[8] His missile forces even threatened Guam, a US territory and the home of large Air Force and Navy bases, with a salvo of four intermediate-range missiles.[9]

With so much rhetoric and action from both sides, the risks of miscalculation have never been higher. Now, more than ever, the bedrock of Air Force intelligence assessments for senior leaders must be accurate data. Commanders from every service and at almost every echelon also demand the worldwide battlefield awareness the Air Force's Distributed Common Ground System (DCGS) provides. Yet, the DCGS' present challenge, from an intelligence, surveillance, and reconnaissance (ISR) standpoint, is to control the fog of "big data" that is enveloping it. According to a 2013 estimate, the DCGS processes 1.3 petabytes of data per month or about 1,000 hours of full-motion video (FMV) per day.[10] Our space-based assets provide sufficient warning of missile launches to America and its allies, but antiballistic missile defenses like THAAD are designed to destroy missiles as they reenter the Earth's atmosphere which, by then, might be too late. Time and lethality are of the essence; it will take a prudent combination of activity-based intelligence (ABI) and cyber-targeting to respond to Pyongyang.

Better ISR through ABI

As the North Korean threat has grown, the talk in Washington's intelligence and policy circles has turned to getting left-of-launch. This combination of science, technology, and operational art has the potential to disable or destroy North Korean missiles upon or within a few seconds of lift-off.[11] While this approach certainly seems tantalizing, there are two problems with it. First, a missile interceptor will have to be moving at hypersonic speed to destroy its target. This practice is so fraught with risk that military historians have likened it to "hitting a bullet with a bullet."[12] And, if the stakes are not high enough, shooting down one of North Korea's ICBMs upon ignition would put the US in a de facto state of war. Moreover, in some cases, a missile test is virtually indistinguishable from a hostile launch; intelligence that discerns between the two must be impossibly pristine. North Korea's military doctrine is modeled after the old Soviet *maskirovka*—a crafty, resourceful denial and deception campaign that makes positive identification of targets hard to attain.[13]

ABI demystifies North Korea's calculus and gives the DCGS the means to help military and civilian decision makers avoid a miscalculation. Chandler P. Atwood, a leading ABI advocate, defined the concept and its guiding principles handily in *Joint Force Quarterly*:

> ABI is an analysis methodology which rapidly integrates data from multiple [intelligence disciplines] and sources around the interactions of people, events, and activities, in order to discover relevant patterns, determine and identify change, and characterize those patterns that drive collection and create decision advantage.[14]

Many Airmen today—especially those who inhabit the DCGS—seek to stem the tides flowing from every sensor and to make sense of it, ideally without all the antiquated, human labor-intensive practices that come with processing, exploitation, and

dissemination (PED) of intelligence. With automation and machine-to-machine interaction, ABI can bridge the gaps between the virtual stovepipes our human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT), measurement and signatures intelligence (MASINT), and even open-source intelligence (OSINT) have become. Information from traditional intelligence sources such as these can be fused with data from nontraditional sources, such as moving target indicator (MTI) sensors, or space-based sensors such as overhead persistent infrared (OPIR) that captures IR emanations on the surface below them. This widens the information aperture and promotes the DCGS' transcendence from FMV imagery's narrow "soda-straw" view.[15] Fortunately, the bandwidth of our information technology systems is increasing at a rate that supports the surge of disparate data streams.[16] All-source analysts can correlate events quickly, discover anomalies and connections, and make comprehensive assessments with as much context possible. "The traditional process of stitching together sparse data," wrote Atwood, "is now evolving into a process of extracting conclusions from aggregation and distillation of big data."[17]

How can using ABI get us left-of-launch? Let's say we want to make a detailed examination of North Korea's missiles, not just ICBMs but the entire country's missile industry. ABI enables the automated georeferencing of the objects and entities associated with it—the people, places, and things that are responsible for the missiles' design, supply chain management, engineering, production, and deployment. ABI analysts determine remarkable events, locate them in space and time, and tune out extraneous information, so the identified problem can be solved more readily. It is in this stage where they put on their detective hats, looking forward and backward temporally, searching for activities that indicate missile checkouts from storage, possible routes to launch pads, or intercepts of communications between senior leaders in Pyongyang, to lower-ranking officers in North Korea's missile forces. Provided every facet of activity captured across the disciplines are georeferenced, with the aid of tools like Google Earth or ArcGIS, an ABI analyst can build an activity map that depicts the interactions between the target entities and then apply what Atwood calls "integration before exploitation."[18]

In the typical PED process, DCGS analysts look deeply into the intelligence discipline stovepipes, narrowly focusing on GEOINT for example, searching for the missiles themselves and their transporter erector launchers (TEL) moving from staging areas to hide sites or launch bays. In the old days, a correlation analyst might corroborate prelaunch activities by reaching into the SIGINT stovepipe for communications between missile convoys, or using OSINT to seek out provocative press statements from Pyongyang that might signal something is imminent. ABI moves analysts away from linear thinking and avails other intelligence disciplines for correlation analysis that may have otherwise been disregarded. It could have brought vital context to Pyongyang's threat to Guam, which certainly seemed menacing on its surface. But, a far different story takes shape when nontraditional sources of intelligence from MTI sensors are fused with information from other disciplines that correlate the threat itself with actual movements in time and space on the ground. Incorporating MTI data with an activity map might uncover if the North Koreans are using *maskirovka* to hide from our ISR assets, or bar us from seeing the total picture. Without bias for one intelligence means or the other ABI analysts

will give each piece of data equal consideration. SIGINT should not be favored over HUMINT because it is derived from more direct sources or technical means, and GEOINT should not be held up as absolute proof of movement to launch pads if MTI or electronic intelligence (ELINT) indicate facts to the contrary.

An ABI-focused approach considers every intelligence discipline as they interrelate with one another—spatially *and* temporally. This way, the analyst-as-detective can forensically judge if (or when) a launch might occur using a combination of historical data and data obtained in near real time. This is what Atwood calls "sequence neutrality;" a principle that considers "incidentally collected data" (information collected by happenstance) that "may be as significant or more significant than data collected in a more targeted fashion."[19] Of all ABI's principles, sequence neutrality is most important. It is the thing that permits analysts to take all present day and archival data into account when making fact-driven, unbiased, left-of-launch judgments about North Korea.

Weighing All the Options

In a left-of-launch scenario, a direct attack on North Korea's missiles would have little coercive value, and doing so could cause the situation to spiral perilously out of control. However, a cyberattack—if properly executed—would almost certainly cause less collateral damage and decrease the chances of a political liability for Washington. One of the revelations from the Stuxnet virus that infected Iran's uranium-enriching centrifuges was that it caused subtle variations in the machines' control code, causing them to spin out of control, and tear themselves apart.[20] These revelations beg the question—what industrial control systems (ICS) oversee the North Korean missile industry? Machine presses that heat, temper, and roll steel into tubes do a lot of the work—but mobile missiles tend to be air-gapped and isolated from any central command and control system that might be subject to interference or jamming.[21] Using the common space-based means of direction finding would be futile if enemy crews are instructed to halt any communications before launch. Small nations like North Korea are also adept at evading Air Force collection platforms, and their orbits would have to be adjusted to compensate for any loss of intelligence.[22] Applications that track commercial satellites are available on the open internet, making counterspace, as well as denial and deception, easy even for the most unsophisticated adversary.[23]

A good ABI analyst will have the entire North Korean missiles' industry charted with an activities map—from its machines down to the people who operate them. Collection managers could use these maps to reallocate assets and maximize potential so analysts will have the best available intelligence at the right time. Cyber operators can use the same data-driven technique to choose what logic ought to be discreetly implanted and at which missiles' manufacturer. A carefully crafted internet worm could circumvent all the obstacles; it could cause delicate, structural variations in metals that might defy the human eye. Missile production involves intricate engineering processes where the minutest defect in their engineering could cause catastrophic failure. Consider, too, that most of North Korea's missiles are mobile,

which is both a weakness and strength. Mobile missiles by their very nature are moving targets. But, once deprived of their mobility, they cannot evade detection or a counterattack. Wheels and tracks are comprised of common rubber and tires for mobile TELs. They are manufactured with antioxidants and stabilizers (like phenols) which prevent tread wear on the road and rot during storage.[24] Where do the North Koreans purchase them, or are they made domestically? In theory, for as much as Stuxnet caused nearly imperceptible damage to Iran's nuclear program, similarly "weaponized code" could decrease the shelf-life and reliability of North Korea's missiles and their TELs.[25]

The modern intelligence methods proposed here are just a few, but they cut through the fog of data smartly so that USAF intelligence analysts can decipher Pyongyang's true intentions and make recommendations that respond to it appropriately. In the meantime, forceful preemptive action has not been ruled out, but as Secretary Tillerson said, "All options are on the table."[26] His words signal each instrument of power will be evaluated deliberately before the US commits to action. If this is the case, then weaponized code applied precisely using ABI should be given its due consideration as well. Both make a powerful, one-two combination that will achieve the same effects as a conventional attack, but without the casualties an all-out war on the Korean Peninsula will surely bring. ✪

Notes

1. James Martin Center for Non-Proliferation Studies, "The CNS North Korea Missile Test Database," *Nuclear Threat Initiative*, accessed 27 December 2017, http://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/.

2. Joseph S. Bermudez Jr., Jack Liu, and Frank Pabian, "The Games People Play: Has the Punggye-ri Nuclear Test Site Transitioned to Stand-by Status?," 19 April 2017, *38North*, http://38north.org/2017/04/punggye041917/#_ftn2.

3. Fox News, "North Korea: 'Super-Mighty Pre-Emptive Strike' Will Reduce US to Ashes," *Fox News*, 20 April 2017, http://www.foxnews.com/world/2017/04/20/north-korea-super-mighty-pre-emptive-strike-will-reduce-us-to-ashes.html. *See* Mason Richey, "Turning It Up to Eleven: Belligerent Rhetoric in North Korea's Propaganda," *Parameters* 46: no. 4 (Winter 2016–17): 95–96, https://www.hsdl.org/?view&did=799478.

4. David E. Sanger, "Rex Tillerson Rejects Talks with North Korea on Nuclear Program," *New York Times*, 17 March 2017, https://www.nytimes.com/2017/03/17/world/asia/rex-tillerson-north-korea-nuclear.html?_r=0. *See* Barack H. Obama, "National Security Strategy: February 2015," *Obama White House Archives*, accessed 5 May 2017, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

5. Joshua Stanton, Sung-Yoon Lee, and Bruce Klingner, "Getting Tough on North Korea: How to Hit Pyongyang Where It Hurts," *Foreign Affairs* 96, no. 3 (May–June 2017): 73, https://www.foreignaffairs.com/articles/north-korea/2017-04-17/getting-tough-north-korea.

6. The Department of Defense misclassified the 4 July 2017 missile launch as a test of an intermediate range missile. On 5 July, it was reclassified as an ICBM with a range of at least 5,500 kilometers. The missile was launched from Panghyon Airfield, an area 90 miles north of Pyongyang. The airfield

was not previously associated with North Korea's missile industry. *See* David Nakamura and Emily Rauhala, "Haley Hits China and Russia at U.N.," 6 July 2017, *Washington Post*, sec. A1.

7. Michelle Ye Hee Lee, "Analysis: N. Korea Bomb Test Was Far Larger Than Thought," *Washington Post,* 14 September 2017, https://www.highbeam.com/doc/1P4-1938384106.html. The article cites an assessment by the Air Force Technical Applications Center. It estimated the September 2017 explosion at Pungyee was between 70 to 280 kilotons. These yields surpass the Hiroshima bomb's strength, which was about 15 kilotons.

8. Anna Fifield, "North Korea's Latest Missile Launch Appears to Put U.S. Capitol in Range," *Washington Post*, 29 November 2017, https://www.washingtonpost.com/world/north-korea-fires-missile-for-the-first-time-in-more-than-two-months/2017/11/28/0c136952-d46c-11e7-9461-ba77d604373d_story.html?utm_term=.917a36b75f0e.

9. Anna Fifield, "More Than War, Kim Wants to Stay in Power, Experts Say," *Washington Post*, 11 August 2017, sec. A10.

10. Marc V. Schanz, "ISR After Afghanistan," *Air Force Magazine* 96, no. 1 (January 2013): 24, http://www.airforcemag.com/MagazineArchive/Magazine/2013/0113fullissue.pdf.

11. William Broad and David Sanger, "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight," *New York Times*, 4 March 2017, https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html.

12. Michael J. Neufeld, "Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense by Kenneth P. Werrell," *Journal of Military History* 65, no. 2 (April 2001): 574, http://www.jstor.org/stable/2677252.

13. Scott Gerwehr and Russell W. Glenn, *The Art of Darkness: Deception and Urban Operations* (Santa Monica, CA: Rand Corp., 2000), 33, https://www.rand.org/pubs/monograph_reports/MR1132.html.

14. Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Force Quarterly* 77 (April 2015): 26, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/.

15. Ibid., 25.

16. During the opening days of Operation Iraqi Freedom, the United States used 30 times more bandwidth than it did during Operation Desert Storm in 1990, thus enabling the swift toppling of Saddam Hussein in 26 days. *See* Max Boot, "The New American Way of War," *Foreign Affairs*, 82, no. 4 (July-August 2003): 58, http://www.jstor.org/stable/20033648.

17. Atwood, *Activity-Based Intelligence*, 26.

18. Ibid., 27.

19. Ibid., 32.

20. Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 14 April 2011, http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs.

21. John Schilling, "How to Hack and Not Hack a Missile," 21 April 2017, *38North*, http://38north.org/2017/04/jschilling042117/.

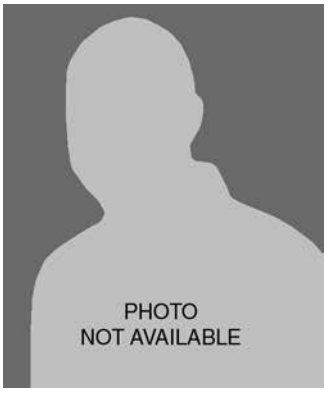
22. Gene H. McCall and John H. Darrah, "Space Situational Awareness: Difficult, Expensive—and Necessary," *Air & Space Power Journal* 28, no. 6 (November–December 2014): 7, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-28_Issue-6/SLP-McCall_Darrah.pdf.

23. Ibid.

24. Lawrence Fishbein, "Chemicals Used in The Rubber Industry: An Overview," *Scandinavian Journal of Work, Environment, and Health* 9, no. 2 (1983): 9, http://www.jstor.org/stable/40964975.

25. Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* 92, no. 6 (November–December 2013), http://www.jstor.org/stable/23527014.

26. Sanger, *Tillerson Rejects Talks*.



Maj William Giannetti, USAFR

Major Giannetti (MS, St. Joseph's University) is an Air Force reservist assigned to the joint staff at the Pentagon, Washington, DC. His 20-year career spans time as a civil servant, Philadelphia police officer, and Department of Defense analyst. He was a part-time mission operations commander in the Virginia Air National Guard. Major Giannetti has also served two tours in Afghanistan.