The US Response to North Korea: The Cyber Option

https://www.e-ir.info/2017/08/07/the-us-response-to-north-korea-the-cyber-option/

MATTHEW S. COHEN, AUG 7 2017

The tragic death of Otto Warmbier, the continued captivity of three additional American citizens, and North Korea's recent launch of an apparent inter-continental ballistic missile (ICBM) again raise the question of how to handle the threating behavior. Unfortunately, the United States (US) has few good options. The US cannot successfully employ typical diplomatic actions against North Korea because the two nations have no formal diplomatic relations, and because China and Russia can block actions at the United Nations. The US also has limited economic leverage. Sanctions are already in place. There is no trade between the two nations, so additional bi-lateral sanctions are not available. It is not possible to shame North Korea into changing its behavior, as the hermit kingdom has shown time and again that it does not care what the outside world thinks, and the few outside nations that still do business or have diplomatic relations with North Korea have shown no interest in halting trade over any extended period simply due to North Korea's brutality and recklessness. The US could appeal again to China to assist, but there seems little reason to hope China will take meaningful long-term action.

There is, however, one thing the US can do to North Korea, despite the dangers this option poses. The US can block North Korea's access to cyber-space, and make it clear that the US is behind the attacks. North Korea is fairly advanced in cyber space, and often uses the cyber realm to promote its interests. North Korea is suspected to have been behind numerous high profile attacks, including the Sony hack in 2014 and a recent string of attacks on banks. These attacks serve a range of purposes for the regime, including retaliation against those who have offended North Korea and to steal money. Much of the money from these bank hacks is suspected to have been funneled to the nuclear weapons program.

North Korea has grown increasingly sophisticated and bold in its attacks; however, the kingdom's cyber-capabilities still lag badly behind the US'. North Korea, for example, lost all access to the internet in the wake of the Sony hack as a result of a cyber-attack. There have been no unrefuted claims regarding who was behind the attack. It may have been the US government or hacker groups. Either way, the success the attackers had underscores the weaknesses in North Korea's cyber-defenses. By contrast, the US is among the most capable actors.

This proposal does carry dangers. Cyber-attacks raise the risk North Korea might escalate its offensive behaviors, and that China may become angered, particularly if the attack inadvertently spills into Chinese systems. These issues can be addressed. North Korea may not be prepared to worsen the situation. In fact, there is speculation North Korea "freed" Mr. Warmbier in hopes of opening a dialogue. The US must reassure allies it will stand behind them if North Korea escalates, and the US must be prepared to do so as failing to act will further strengthen North Korea. In regards to China, the US should discuss the goals of its operation with China and do as much as it can to ensure North Korea is the only entity meaningfully impacted.

There is an additional risk. States have avoided claiming they have used cyber-space to punish another nation. Thus, by acting openly, the US runs the risk of setting a new norm of behavior that would allow other states to use cyber-space for similar reasons. This concern might be a bit overblown. This is a rare circumstance and is in regards to the world's most infamous actor. Further, the US use of Stuxnet is well known and did not usher in a new age of cyber-warfare. Another targeted use in an extreme circumstance is unlikely to lead to a different outcome.

The US could even use cyber-attacks on North Korea to help foster discussion regarding agreements on norms of

behavior. Such an outcome would be greatly beneficial. To achieve this, the US must be very clear that it is using cyber-space in this specific case because: 1) a US citizen was murdered by a foreign regime through cruel and inhumane treatment, thus making the release of remaining US citizens highly pressing; 2) the development of ICBM represents a threat to the security of the US and its allies; 3) there are no other tools available to respond; and 4) the US wishes to avoid escalation in the physical realm, and 5) the US does not want to harm North Korea's citizens. (Cyber-attacks should try to shut down offensive abilities and the connection to the outside world without affecting civil functions.) The US can stress that it is due to these factors that cyber-space is the correct venue for action, and that a broader use of cyber-attacks in other situations would not be acceptable.

The US must stress also that it has two main, narrow intents. First, the US must use these actions in cyber-space as a deterrent. The US can harm North Korea economically by damaging North Korea's ability to launch cyber-attacks on foreign targets. Second, the US should make clear it will only end the attacks once North Korea releases the three remaining US citizens it is holding and returns to fruitful negotiations regarding the nuclear program.

There is an additional possible benefit should the use of cyber-tactics lead to the release of US citizens held prisoner and the resumption of negotiations. It will show that offensive actions in cyber-space can lead nations to change policies. It will, of course, only show this works in a limited arena. It is not possible for the US, Russia, China, Israel, or other major cyber-powers to change each other's policies solely though cyber-actions. A successful outcome in regards to North Korea will instead show powerful nations that there is another way to achieve policy goals outside of sanctions and bloodshed. This is still a problematic outcome, of course, but far superior to the loss of life.

There is an additional danger posed by using offensive cyber-weapons against North Korea. North Korea will be able to learn from the code used against it and advance their own capabilities. It appears, for example, that Iran advanced its offensive capabilities after it uncovered Stuxnet. The benefits in this case outweigh the risks, however. Further, once it is known what vulnerabilities the US used to launch its attacks, nations and private entities can create defenses against similar attacks.

The US should not tolerate the continued detention of its citizens and growth of North Korea's nuclear threat, or allow the death of Mr. Warmbier to go unanswered. Cyber-space may be the best way for the US to respond. It is an option that causes direct harm to the regime while leaving the citizens of North Korea unharmed. North Korea's response to the cyber-actions would determine how long and extensive the cyber-campaign would be. Should this strategy work, not only may North Korea be deterred, not only will three people who are unjustly imprisoned be set free, but the world could be left slightly better off.

About the author:

Matthew S. Cohen is a PhD candidate and Lecturer in Political Science at Northeastern University and an Adjunct Instructor at Merrimack University specializing in both emerging security threats, with a focus on cyber-security, and the Middle East. His works can be found at his Academia profile.