North Korean Cyber Attacks

George Wald stated in 1969 “There is nothing worth having that can be obtained by nuclear war - nothing material or ideological - no tradition that it can defend. It is utterly self-defeating”. Yet even today nearly 50 years later the world views nuclear weapon capabilities as the greatest threat from adversaries seeking negotiating power to meet opposing demands. This view may have been true for past generations, but in a new digital era, cyber sophistication reigns supreme. While the world continues to seek sanctions and repercussions against North Korea for furthering their nuclear and ballistic missile capabilities, they continue to expand and refine an even greater threat – the Democratic People’s Republic of Korea (DPRK) cyber-army. Cyber-attacks provide North Korea with a semi-anonymous method of pushing negotiations in their favor, whereas nuclear strikes would simply be a non-utilized deterrent. A shift in focus to cybersecurity policy and techniques, rather than nuclear disarmament, is the most effective way to stifle DPRK aggression.

The first reason that cybersecurity is more effective than nuclear disarmament at deterring North Korean aggression is that they have historically shown a willingness to conduct cyber-attacks, regardless of sanctions. "What they provide is another tool for DPRK to show their displeasure if the talks are not going their way, and a way to refocus the world's attention on their ability to disrupt regional stability if talks break down," said Adam Segal, director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations. Sanctioning has been an effective tool at bringing North Korea to the negotiation table after conducting nuclear-capable ballistic missile launch testing, even triggering a historic meeting with the president of the United States, but no such results have been attained following DPRK cyber-attacks. Sanctioning, though limited, has failed to slow or halt DPRK cyber actors. Furthermore, if North Korea is displeased with how negotiations are proceeding, they may be inclined to utilize cyber-attacks as a show of force in order to sway opinions in their favor. Nuclear attacks could not be used to the same strategic effectiveness as they would trigger an immediate international retaliation resulting in the destruction of North Korea. Cyber-attacks may also be carried out against civilian banks and crypto-currency exchanges, such as the “AppleJeus” hack by North Korea in August 2018, subverting any financial harm caused by sanctions. In a single hack alone in January 2018, DPRK cyber actors allegedly stole $523 million from the Japanese cryptocurrency exchange Coincheck.

The second reason that cybersecurity is more effective than nuclear disarmament at deterring North Korean aggression is that cyber-attacks can easily be conducted internationally with minimal attribution, unlike nuclear strikes. Utilizing cyber-attacks can provide an uncertainty as to the perpetrator in order to achieve desired effects, whereas nuclear weapons show a definite originator. “A nuclear attack against the United States by North Korea would be “one and done”, while a cyber-attack by North Korea is the gift that keeps on giving for Kim Jong Un.” (Wright, 2018) While North Korea appears to be slowing down nuclear production and dismantling facilities they have nearly doubled the number of cyber actors working for the government to 6,000 personnel, according to the South Korean military (2). The attacks perpetrated by these cyber-army personnel are attributed to the DPRK based on their methodology and targets, however, there is typically no definitive proof that the North Korean regime is the orchestrator.

The third reason that cybersecurity is more effective than nuclear disarmament at deterring North Korean aggression is that cyber-attacks can attack be carried out by lone individuals or small groups against targets more devastating to civilians, the military, or public infrastructure on a larger scale, possibly even worldwide. As shown by the Stuxnet attack in 2010, a small group of individuals working on behalf of the North Korean government were able to infiltrate and infect the Iranian nuclear program with a computer virus. German expert Ralph Lagner described Stuxnet as a military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program'. Such attacks perpetrated by the DPRK indicate that nuclear armament may be totally unnecessary, given that they could simply utilize cyber-attacks to manipulate the nuclear weapons of another country. Protecting computer systems both physical and digitally are the only way to ensure that these attacks can be thwarted in the future. The International Journal of Critical Infrastructure Protection states "Cyberspace, the ever-expanding manifestation of the pervasive information and communications infrastructure, is a rich environment for the projection of power and influence. Entities of all types – nation-states, corporations, terrorist and criminal organizations, and non-profit groups – are embedding critical aspects of their operations in cyberspace hoping to reap the benefits offered by the domain. Cyberspace is an equalizer. It offers all actors speed and reach anonymity and protection, and the ability to create and participate in virtual economies and wield cyber weapons, all with a low buy-in cost. This drastically alters the power equation. The gap between major powers and lesser powers is shrinking; non-state actors could become cyber powers. (3) North Korean regime sponsored cyber-attacks are proving to be a greater threat to the world each year. Nuclear strike threats have evolved into a policy of mutually assured destruction, ensuring that they will almost certainly never be used.

Cyber-attacks allow for uncertainty in attribution providing a more lethal tool for offensive attacks swaying negotiations. A worldwide shift in focus to cybersecurity policy and techniques, rather than nuclear disarmament, is the most effective way to stifle DPRK aggression. No amount of sanctioning has proven effective at halting DPRK cyber-attacks; therefore, defensive measures and policy shifts are required to combat this growing threat. Cyber-attacks can be carried out by small groups, even lone individuals, acting on behalf of adversary governments. Cybersecurity is the only way to be certain that these cyber-criminals do not gain the upper hand on the world stage. A nuclear strike may seem like some foreign concept that will never affect an area with you or your loved ones, but the next time you check your email and see a suspicious link, how far away do you think the cyber actors are?