Written by **C. Mitchell Shaw** on December 2, 2018

NATO Practicing Cyber-Warfare Games

To address the growing concern of cyber-warfare, NATO has launched the "Cyber Coalition 2018" in Estonia — a mere 30 miles from the Russian border. The exercise is a "War Game" focused on defense and counter-attack in the arena of digital battle.

As AFP News reported:

> The activity is taking place just 50 kilometres (30 miles) from the border with Russia, seen by the West as the biggest cyber threat after a string of attacks blamed on the Kremlin. Targets have included world sports bodies, the US Democratic Party and the world chemical weapons watchdog in the Netherlands.
>
> NATO says such assaults are becoming more "frequent, complex, destructive and coercive", and are launched not just by state actors like Russia, China and North Korea but also by criminal gangs intent on extortion and "hacktivists" looking to embarrass big organisations.

In an age in which computers run everything from televisions and cars to ships and planes, and from water treatment centers to nuclear power plants, the threat of cyber-warfare is the threat of a very real and present danger. Regardless of whether Russia was actually responsible for "hacking" the Democratic Party — or if "hacking" was even the means by which embarrassing and damning e-mails were obtained and then leaked to WikiLeaks during the 2016 election cycle — Russia is accused of operating a vast cyber-warfare campaign. As AFP reported:

> Last month, Dutch authorities took the unusual step of identifying four suspected Russian intelligence agents accused of trying to hack the headquarters of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague and sharing a detailed account of their plot.
>
> The move was part of Dutch efforts to build up cyber deterrence — based on naming and shaming culprits coupled with an ability to strike back if so ordered.

The Dutch are not alone in ramping up efforts to combat cyber-warfare by those who would threaten national security. United States Colonel Don Lewis, deputy director of the new cyber-operations center set up by NATO, remarked about the relative ease and affordability of cyber-warfare compared to more conventional methods. "The price of entry into operations in cyber is extremely low." Lewis said, adding, "If you want to come at my nation in the air, you have to build an F-35 — that is not easy to do and it's very, very expensive. But for the price of a latte at Starbucks and a laptop you can get on the internet and for a few hundred dollars you can get malware off the black web."

NATO says that attacks such as those mentioned above are becoming more "frequent, complex, destructive and coercive." Regardless of whether those attacks come from state-sponsored hackers in

nations such as China, Russia, or elsewhere, or are carried out by criminal organizations or "hacktivist" groups with ideological or political goals, NATO is preparing to meet digital fire with digital fire. Again, from AFP:

> NATO has two cyber rapid reaction teams on standby round the clock, ready to respond within 48 hours. Their weapons are fast computers with vulnerability-analysis code, forensic software and special database-management tools.

Jeremy Tod of the NATO Communications and Information Agency likened NATO's elite hacking squad to "the men in black, carrying lots of strong black plastic boxes with them." The current "cyber-war game" exercise involves a hypothetical situation in which a fictional east African nation is the subject of a major cyber-attack during elections. The fictional attack involves hacking computers to contaminate the water supply while simultaneously hacking the railway system to divert trains carrying NATO troops who are supposed to guard polling stations.

The exercise calls for 700 NATO cyber-security experts from different nations to both defend the intended target of the attack and launch their own counter-attack using "offensive cyber-weapons" made available by the governments of the nations working together under the NATO banner. AFP reported:

> The US, Britain, Denmark, Estonia and the Netherlands have all pledged to offer their cyber weapons for NATO operations if requested, figuring that aggressors could be deterred if they knew they would counterattacked.
>
> But Lewis said deploying cyber weapons carries the same risks of real-world arms. Consideration must be given to the risk of "collateral damage," he said, and the commanders in the exercise stopped short of actually deploying them.

Air Commodore Elanor Boekholt-O'Sullivan, commander of a Dutch cyber unit authorized to use offensive tactics, favors the threat of a strong, unified offense as the best defense. She asked, "Who gets punched in the schoolyard by the bully?" Answering her own question, she went on to say, "Certainly not the kid who is known for his karate skills and who's surrounded by friends who will stand up for him." Boekholt-O'Sullivan certainly crossed the line into exaggeration, though, when she said, "Everything that has an on and and off switch, you can manipulate it." One is left to wonder whether blenders and desk lamps would be on her short list of devices waiting to be weaponized.

Of course, the act of sharing U.S. cyber-weapons with NATO may carry its own dangers. NATO is — after all — a creature of the United Nations, which ultimately controls the organization. To borrow Boekholt-O'Sullivan's playground analogy, what happens when those "friends who will stand up for [you]" turn on you because they weren't true friends in the first place? You may wish you had never taught them all your "karate skills."

While the threat of cyber-attack by state actors, criminals, and "hacktivists" is real, one salient point that is far too often overlooked is that many of the tools they use were developed by agencies of the U.S. government and allowed to get into the hands of those who would harm us.

Photo: gorodenkoff/iStock/Getty Images Plus