Opinion

After a cyberattack, the waiting is the hardest part

By **Jan Kallberg**

Sep 6, 2019

U.S. Marines debark from an MV-22B Osprey at Al Asad Air Base, Iraq in June 2018. A cyberattack could slow how U.S. forces respond to a battlefield. (Cpl. Jered T. Stone/Marine Corps)

We tend to see vulnerabilities and concerns about cyber threats to critical infrastructure from our own viewpoint. But an adversary will assess where and how a cyberattack on America will benefit the adversary's strategy. I am not convinced attacks on critical infrastructure, in general, have the payoff that an adversary seeks.

The American reaction to Sept. 11 and any attack on U.S. soil gives a hint to an adversary that attacking critical infrastructure to create hardship for the population might work contrary to the intended softening of the will to resist foreign influence. It is more likely that attacks that affect the general population instead strengthen the will to resist and fight, similar to the British reaction to the German bombing campaign "Blitzen" in 1940. We can't rule out attacks that affect the general population, but there are not enough offensive capabilities to attack all 16 sectors of critical infrastructure and gain a strategic momentum.

An adversary has limited cyberattack capabilities and needs to prioritize cyber targets that are aligned with the overall strategy.

Trying to see what options, opportunities, and directions an adversary might take requires we change our point of view to the adversary's outlook.

One of my primary concerns is pinpointed cyber-attacks disrupting and delaying the movement of U.S. forces to theater.

Seen for the potential adversary's point of view, bringing the cyber fight to our homeland - think delaying the transportation of U.S. forces to theater by attacking infrastructure and transportation networks from bases to the port of embarkation - is a low investment/high return operation. Why does it matter?

First, the bulk of the U.S. forces are not in the region where the conflict erupts. Instead, they are mainly based in the continental United States and must be transported to theater. From an adversary's perspective, the delay of U.S. forces' arrival might be the only opportunity. If the adversary can utilize an operational and tactical superiority in the initial phase of the conflict, by engaging our local allies and U.S. forces in the region swiftly, territorial gains can be made that are too costly to reverse later, leaving the adversary in a strong bargaining position.

Second, even if only partially successful, cyberattacks that delay U.S. forces' arrival will create confusion. Such attacks would mean units might arrive at different ports, at different times and with only a fraction of the hardware or personnel while the rest is stuck in transit.

A transportation delay to ports of entry will also give more time for the adversary to attack the sealift at sea and the units from the port of debarkation to the operational area. The distance from Hamburg and Amsterdam to Eastern Poland is equal to the distance between New York City and Chicago. Any delay for the U.S. forces leaving the continental United States and heading to a European theater gives more time for the adversary to disrupt transportation within Europe through a mix of cyber, special forces, and standoff weaponry.

Third, an adversary that is convinced before a conflict that it can significantly delay the arrival of U.S. units from the continental U.S. to a theater will do a different assessment of the risks of a fait accompli attack. Training and Doctrine Command defines such an attack as one that " is intended to achieve military and political objectives rapidly and then to quickly consolidate those gains so that any attempt to reverse the action by the U.S. would entail unacceptable cost and risk." Even if an adversary is long-term strategically inferior, the window of opportunity due to assumed delay of moving units from the continental U.S. to theater might be enough for them to take military action seeking to establish a successful fait accompli-attack.

In designing a cyber defense for critical infrastructure, it is vital that what matters to the adversary is a part of the equation. In peacetime, cyberattacks probe systems across society, from waterworks, schools, social media, retail, all the way to sawmills. Cyberattacks in war time will have more explicit intent and seek a specific gain that supports the strategy. Therefore, it is essential to identify and prioritize the critical infrastructure that is pivotal at war, instead of attempting to spread out the defense to cover everything touched in peacetime.

Jan Kallberg, Ph.D., LL.M., is a research scientist at the Army Cyber Institute at West Point and an assistant professor in the department of social sciences at the United States Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the United States Military Academy, or the Department of Defense.

›