By **Jan Kallberg** and **Col. Stephen Hamilton**

Mar 23, 2020

Army Spc. Reagan Long, left, a horizontal construction engineer with the New York Army National Guard's 827th Engineer Company, and Army Pfc. Naomi Velez, a horizontal construction engineer with the New York Army Guard's 152nd Engineer Support Company, register people at a COVID-19 mobile screening center in New Rochelle, New York, March 14, 2020. More than 1,500 National Guard members in 22 states have been activated in support of state and local authorities responding to the COVID-19 outbreak. In addition to operating mobile screening centers, Guard members have been disinfecting public spaces, providing logistical and transportation support and coordinating with state and local health officials. (U.S. Army photo by Sgt. Amouris Coss)

The COVID pandemic is a challenge that will eventually create health risks to Americans and have long-lasting effects. For many, this is a tragedy, a threat to life, health, and finances.

What draws our attention is what COVID-19 has meant our society, the economy, and how in an unprecedented way, family, corporations, schools, and government agencies quickly had to adjust to a new reality.

Why does this matter from a cyber perspective?

COVID-19 has created increased stress on our logistic, digital, public, and financial systems and this could in fact resemble what a major cyber conflict would mean to the general public. It is also essential to assess what matters to the public during this time. COVID-19 has created a widespread disruption of work, transportation, logistics, distribution of food and necessities to the public, and increased stress on infrastructures, from Internet connectivity to just-in-time delivery. It has unleashed abnormal behaviors.

A potential adversary will likely not have the ability to take down an entire sector of our critical infrastructure, or business eco-system, for several reasons. First, awareness and investments in cybersecurity have drastically increased the last two decades. This in turn reduced the number of single points of failure and increased the number of built-in redundancies as well as the ability to maintain operations in a degraded environment.

Second, the time and resources required to create what was once referred to as a “Cyber Pearl Harbor” is beyond the reach of any near-peer nation. Decades of advancement, from increasing resilience, adding

layered defense and the new ability to detect intrusion, have made it significantly harder to execute an attack of that size.

Instead, an adversary will likely focus their primary cyber capacity on what matters for their national strategic goals. For example, delaying the movement of the main U.S. force from the continental United States to theater by using a cyberattack on utilities, airports, railroads, and ports. That strategy has two clear goals: to deny United States and its allies options in theater due to a lack of strength and to strike a significant blow to the United States and allied forces early in the conflict. If an adversary can delay U.S. forces' arrival in theater or create disturbances in thousands of groceries or wreak havoc on the commute for office workers, they will likely prioritize what matters to their military operations first.

That said, in a future conflict, the domestic businesses, local government, and services on which the general public rely on, will be targeted by cyberattacks. These second-tier operations are likely exploiting the vulnerabilities at scale in our society, but with less complexity and mainly opportunity exploitations.

The similarity with the COVID-19 outbreak to a cyber campaign is the disruption in logistics and services, how the population reacts, as well as the stress it puts on law enforcement and first responders. These events can lead to questions about the ability to maintain law and order and the ability to prevent destabilization of a distribution chain that is built for just-in-time operations with minimal margins of deviation before it falls apart.

The sheer nature of these second-tier attacks is unsystematic, opportunity-driven. The goal is to pursue disruption, confusion, and stress. An authoritarian regime would likely not be hindered by international norms to attack targets that jeopardize public health and create risks for the general population. Environmental hazards released by these attacks can lead to risks of loss of life and potential dramatic long-term loss of life quality for citizens. If the population questions the government's ability to protect, the government's legitimacy and authority will suffer. Health and environmental risks tend to appeal not only to our general public's logic but also to emotions, particularly uncertainty and fear. This can be a tipping point if the population fears the future to the point it loses confidence in the government.

Therefore, as we see COVID-19 unfold, it could give us insights into how a broad cyber-disruption campaign could affect the U.S. population. Terrorist experts examine two effects of an attack – the attack itself and the consequences of how the target population reacts.

Likely, our potential adversaries study carefully how our society reacts to COVID-19. For example, if the population obeys the government, if our government maintains control and enforces its agenda and if the nation was prepared.

Lessons learned from COVID-19 are applicable for the strengthening U.S. cyberdefense and resilience. These unfortunate events increase our understanding of how a broad cyber campaign can disrupt and degrade the quality of life, government services, and business activity.

Jan Kallberg, Ph.D., is a research scientist at the Army Cyber Institute at West Point and an assistant professor at the U.S. Military Academy. Col. Stephen Hamilton, Ph.D., is the technical director of the Army Cyber Institute at West Point and an academy professor at the U.S. Military Academy. The views expressed are those of the authors, and do not reflect the official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy, or the Department of Defense.