Opinion

The opportunities of cyber in arctic warfare

By **Jan Kallberg**

Apr 26, 2018

A U.S. Army Special Forces Soldiers assigned to the 10th Special Forces Group (Airborne) conducts snow machine movement and evasive maneuver training near Kiruna, Sweden, February 24, 2017. Cyber could be a weapon to make the environment even more forbidding for enemies. (Staff Sgt. Matt Britton/Army)

The change from a focus on counter-insurgency to near-peer and peer-conflicts has also introduced the likelihood, if there is a conflict, for a fight in colder and frigid conditions.

The weather conditions in Korea and Eastern Europe are harsh during winter time, with increasing challenges the farther north the engagement is taking place. In traditional war theaters, the threats to your existence line up as follows: enemy, logistics and climate. In a polar climate, it is reversed: climate, logistics and the enemy.

An enemy will engage you and seek to take you on different occasions, but the climate will be ever-present. The battle for your own physical survival in staying warm, eating and seeking rest can create unit fatigue and lower the ability to fight within days, even for trained and able troops. The easiest way to envision how three feet of snow affects you is to think about your mobility walking in water up to your hip, so to compensate either you ski or use low ground pressure and wide-tracked vehicles, such as specialized small unit support vehicles.

The climate and the snow depth also affect equipment. Lethality in your regular weapons is lowered. Gunfire accuracy goes down as charges burn slower in an arctic subzero-degree environment. Mortar rounds are less effective than under normal conditions when the snow captures shrapnel. Any heat, either from weapons, vehicles or your body, will make the snow melt and then freeze to ice. If not cleaned, weapons will jam. In a near-peer or peer conflict, the time units are engaged is longer and the exposure to the climate can last months.

I say all this to set the stage. Arctic warfare takes place in an environment that often lacks roads, infrastructure, minimal logistics, and with snow and ice blocking mobility. The climate affects both you and the enemy; once you are comfortable in this environment, you can work on the enemy's discomfort.

The unique opportunity for cyberattacks in an Arctic conflict is, in my opinion, the ability to destroy a small piece of a machine or waste electric energy.

First, the ability to replace and repair equipment is limited in an arctic environment — the logistic chain is weak and unreliable and there are no facilities that effectively can support needed repairs, so the whole machine is a loss. If a cyberattack destroys a fuel pump in a vehicle, the targeted vehicle could be out of service for a week or more before repaired. The vehicle might have to be abandoned as units continue to move over the landscape. Units that operate in the Arctic have a limited logistic trail and ability to carry spare parts and reserve equipment. A systematic attack on a set of equipment can paralyze the enemy.

Second, electric energy waste is extremely stressful for any unit targeted. The Arctic has no urban infrastructure and often no existing power line that can provide electric power to charge batteries and upkeep electronic equipment. If there are power lines, they are few and likely already targeted by long-range enemy patrols.

The winter does not have enough sun to provide enough energy for solar panels if the sun even gets above the horizon (if you get far enough north, the sun is for several months a theoretical concept). The batteries do not hold a charge when it gets colder (a battery that holds a 100-percent charge at 80 degrees Fahrenheit has its capacity halved to 50-percent at 0 degrees Fahrenheit). Generators demand fuel from a limited supply chain and not only generate a heat signature, but also noise. The Arctic night is clear, with no noise pollution, so a working generator can be pick up by a long-range skiing patrol from 500 yards, risking an ambush. The loss or intermittent ability to use electronics and signal equipment due to power issues reduces and degrades situation awareness, command and control, the ability to call for strikes, and blinds the targeted unit.

Arctic warfare is a fight with low margins for errors, where climate guarantees that small failures can turn nasty, and even limited success with arctic cyber operations can tip the scales in your favor.

Jan Kallberg is a research fellow/research scientist at the Army Cyber Institute at West Point. As a former Swedish reserve officer and light infantry company commander, Kallberg has personal experience facing Arctic conditions. The views expressed herein 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.