Cyber

The case for humanitarian cyber operations

By **Jan Kallberg**

Aug 8, 2018

Featured: Whitepaper: Cloud-Centric Zero Trust Security for Defense Environments >

Intervention in 2018 does not need to be a military intervention with troops on the grounds, but, instead, a digital intervention. (matejmo/Getty Images)

Cyber operations are designed to be a tool for defense, security and war. In the same way as harmless computer technology can be used as dual-purpose tools for war, tools of war can be used for humanity, to protect the innocent, uphold respect for our fellow beings and safeguard human rights.

When a nation-state acts against its population and risks their welfare through repression, violence and exposure to mistreatment, there is a possibility for the world community to take actions by launching humanitarian cyber operations to protect the targeted population. In the non-cyber world, atrocities are intervened by military intervention using the principle of “responsibility to protect,” which allows foreign interference in domestic affairs to protect a population from their repressive and violent ruler without triggering an act of war. If a state fails to protect the welfare of its citizens, then the state that commits atrocities against its population is no longer protected from foreign intervention.

Intervention in 2018 does not need to be a military intervention with troops on the grounds, but, instead, a digital intervention through humanitarian cyber operations. A cyber humanitarian intervention not only capitalizes on the digital footprint but also penetrates the violent regime’s information sources, command structure and communications. The growing digital footprint in repressive regimes creates an opportunity for early prevention and interception against the perpetration of atrocities. The last decade the totalitarian states' digital footprint has grown larger and larger.

As an example, Iran had 2 million smartphones in 2014, but had already reached 48 million smartphones in 2017. Today, about 3 out of 4 Iranians live in metropolitan areas. About half of the Iranian population is under 30 years old with new habits of chatting, sharing and wireless connectivity. In North Korea, the digital footprint has grown as rapidly. In 2011, there were no cellphones in North Korea outside of a very narrow elite circle. In 2017, surveys assessed that over 65 percent of all North Korean households had a cellphone.

No totalitarian and repressive states have been able to limit the digital footprint, which continues to expand for every year. The repressive regimes rely on the computer to lead and orchestrate the repressive actions and crimes against its population. Even if the actual perpetrators of atrocities avoid digital means, the activity will be picked up as intelligence fragments when talked about, discussed, shared, eye-witnessed and silenced.

The planning and initiation to execute atrocities have a logistic trail of troop moments, transportations, orders, communications and concentration of resources.

If there is a valid concern for the safety of the population in the totalitarian states, then free, democratic and responsible states can act. Utilizing the United Nations' accepted principle, “responsibility to protect,” is a justification for the world community or democratic states that decide to act and to launch humanitarian cyber operations utilizing military cyber capacity in a humanitarian role.

Humanitarian cyber operations enable faster response, the retrieval of information necessary for the world community’s decision making to act conventionally, and they remove the secrecy surrounding the perpetrated acts of totalitarian and repressive regimes. The exposure of human rights crimes in progress can serve as a deterrent and interception against a continuation of these crimes. By transposing the responsibility to protect from international humanitarian law into cyber, repressive regimes lose their protection against foreign cyber intervention if valid human rights concerns can be raised.

Humanitarian cyber operations can act as a deterrent because perpetrators will be held accountable. The international humanitarian law is dependent on evidence gathering, and laws might not be upheld if evidence gathering fails, even if the international community promotes decisive legal action. Humanitarian cyber operations can support the prosecution of crimes against humanity and generate quality evidence. The prosecution of the human rights violations in the Balkan civil wars during the 1990s failed in many cases due to lack of evidence. Humanitarian cyber operations can capture evidence that will hold perpetrators accountable.

Humanitarian cyber operations are policy tools for a free democratic nation already in peacetime to legally penetrate and extract information from the information systems of an authoritarian potential adversary that represses their people and endangers the welfare of their citizens. Conversely, the adversary cannot systematically attack the democratic nation because that is likely an act of war with consequences to follow. There is an opportunity embedded in humanitarian cyber operations for humanity and democracy.

Jan Kallberg 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.

Share: