Offensive Cyber: Superiority or Stuck in Legal Hurdles?

Jan Kallberg, University of Texas at Dallas
Offensive Cyber: Superiority or Stuck in Legal Hurdles?

By JAN KALLBERG

In recent years, offensive cyber operations have attracted significant interest from the non-Defense Department academic legal community, prompting numerous articles seeking to create a legal theory for cyber conflicts. Naturally, cyber operations should be used in an ethical way, but the hurdles generated by the legal community are staggering.

At a time when the United States has already lost an estimated $4 trillion in intellectual property as a result of foreign cyber espionage, not to mention the loss of military advantage, focusing on what the United States cannot do in cyberspace only hinders efforts to defend the country from future cyber attack. The country is facing an enemy unrestrained by limitations, clearly visible in blatant cyber attacks on military networks, major banks and media outlets.

Academics who question the legality of offensive counter cyber operations often have limited technical understanding of the unique characteristics of cyberspace. The theoretical framework for an emerging cyber law under development by the legal community uses analogies from international law, such as the laws of the high seas and international commercial air treaties. But these are highly inappropriate for the cyber domain.

For example, the vast majority of these academic legal scholars would require the United States ensure that malicious software attack only combatant systems and legitimate military targets, and not affect any other systems.

What these requirements ignore is the issue of control. Those digital bits easily can be copied and distributed, and targeting removed or redesigned. How can a coder control the duplication of the code?

While code can be targeted to a specific military system, that is no guarantee it will be limited because of the dual use of information technology. There is no control of the code once it is released.

The legal perception of cyber is based on an assumption that actors are either civilian or military, but there is no such clear distinction in the militarized and contested digital world. It is digital bits; in the same way that we cannot distinguish military air and civilian air. It is just air.

In cyberspace, universities, municipal utilities, communication companies and other actors are a part of the war-fighting effort without clear boundaries to being civilian or military. If the U.S. became engaged in a cyber conflict with Hezbollah in southern Lebanon, an organization that is a mix of crude arms manufacturing, terrorism training and soup kitchens for the poor, there is no way to ensure that a counter cyber attack would not affect the soup kitchens.

Second, to avoid the slightest collateral damage, the counter-attacker needs to be able to identify each computer in the counter-attacked network and verify its purpose. That requires full overview of the targeted system, maybe beyond even what the defending system administrators are aware of. The only way you can verify resources in another network is to pre-emptively gain access to their networks and gain targeting information.

Third, international laws rely on territorial boundaries. The laws of the high sea are effective in international water. The national laws apply to territorial waters. But there is no territorial or international cyberspace as long as attribution is unsolved — and even with attribution solved, the answer to where, when and by whom is troublesome to answer.
Applying laws of war that have origins in the 1800s, when massive armies fought on a field in broad daylight, in an
apundance of object permanence, is not relevant to cyber when the contested space is changed, lost, created, reborn
and redesigned in real time. Inferences about cyber operations made in published articles in the academic legal press
are in many cases, to use a mild word, spurious.

Retired Air Force Maj. Gen. Dale Meyerrose, former associate director of national intelligence, said in regard to
offensive cyber operations, “Like everything else in cyber, our legal system is about 20 years behind.”

The risk for the nation is tangible. The proposed legal hurdles evaporate the opportunity to successfully conduct
offensive cyber as a soft policy option. The non-DoD academics’ legal theories on how to conduct cyberwar fail to
recognize the human costs in the alternative: traditional kinetic warfare.

The absence of relevant legal guidance creates confusion and undermines a coherent and systematic approach. Cyber
can help the U.S. achieve political and military goals. These operations will require a legal framework based on the
unique tenets of cyber to enable, not disable, American options and abilities.

———

Jan Kallberg is a researcher at the Cyber Security Research and Educational Center, Erik Jonsson School of
Engineering and Computer Science, the University of Texas at Dallas.