Private Cyber Retaliation Undermines Federal Authority

Jan Kallberg, University of Texas at Dallas
Private Cyber Retaliation Undermines Federal Authority

Jul. 28, 2013 - 02:39PM | By JAN KALLBERG |
defensenews.com

During the last year, several op-eds and commentaries have proposed that private companies have the right to strike back if cyber attacked and conduct their own offensive cyber operations.

The demarcation in cyber between the government and the private spheres is important to uphold because it influences how we see the state and the framework in which states interact. One reason we have a nation state is, in a uniform and structured way, under the guidance of a representative democracy, to deal with foreign hostility and malicious activity.

The state is given a monopoly on violence by its citizenry. The state then acts under the existing laws on behalf of the citizens to ensure the intentions of the population it represents. These powers grant the federal government an authority to enforce compliance of the laws and handle foreign relations. If the federal government cannot uphold that authority, confidence in government will suffer.

The national interest in protecting legitimacy and maintaining the confidence in the federal government is far stronger than the benefits of a few private entities departing on their own cyber odysseys to retaliate against foreign cyber attacks.

The importance of demarcation between government and private entities can be visualized with an example. A failed bank robbery leads to a standoff where the robbers are encircled by government law enforcement. The government upholds its monopoly on violence and, on behalf of the people, engages the robbers in a potential shootout.

All other citizens are instructed to leave the area. The law enforcement officers seek to solve the situation without any violence. This is how we have designed the demarcation between the government and the private sphere in the analog world.

If the US allowed companies to strike back following a foreign cyber attack, it would be abandoning this demarcation.

Going back to the example of bank robbers surrounded by law enforcement, the logic of private cyber retaliation would allow any customer who had an account in the robbed bank to show up and open fire at the robbers at their own discretion, leaving the police to sort out the shootout and the aftermath with no responsibility for the triggering event.

Abandoning the clear demarcation between government and private spheres leads to entropy, loss of control, and is counterproductive for the national cyber defense and the national interest.

The counter argument says private companies are defenseless against cyber attacks and therefore have the right to self defense. The independent Commission on the Theft of American Intellectual Property recently published a report that strongly supported allowing private companies to retaliate against cyber attackers. According to the commission, these counterstrikes should be conducted as follows: “Without damaging the intruder’s own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information.”
The proponents for private cyber retaliation base their view on several assumptions. First, that the private company can attribute the attack and determine who is attacking them.

Second, that the counterstriking companies have the cyber resources to engage, even if it is a state-sponsored organization on the other end, and that there will be no damages.

And third, that the events do not lead to uncontrolled escalation and that the cyber interchanges only affect the engaged parties.

An attacker has multiple options and can target other entities and institutions in reprisal. If the initial attacker is a state-sponsored organization in a foreign country, multinational companies could have significant business and interests at risk if the situation escalates. Private companies would not be responsible for the aftermath, and the entropy that could occur would undermine the American stance and cost its higher ground in challenging the state sponsors behind the cyber attacks in the framework of the international community. The answer to who should hack back, if deciding to do so, is simple: It should be the federal government for the same reason that you would not fly on a passport issued by your neighbor across the street. Only the federal government is suitable to engage foreign nations and the private entities.

The unaddressed core problem is that we have not yet been able to create mechanisms to transfer cyber incidents from the private realm to the authorities. This limited ability during the short time frame when an attack occurs initially gives the attacker an advantage, but this will be solved over time and does not outweigh the damages from an undermined federal authority due to entropy in cyber.

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