Opinion

5 assumptions that should change how we think about hackbacks

By **Jan Kallberg**

Dec 5, 2018

The idea of legalizing hack back operations is based on the assumption that the defending company can attribute the initial attack with pin-point precision. (Welcomia)

The demand for legalizing corporate hackbacks is growing – and there is significant interest by private corporations to utilize hack back if the technique was lawful.

If private companies were able to obtain the right to hack back legally, the risks for blowback is likely more significant than the opportunity and potential gains from private hackbacks. The proponents of private hackback tend to build their case on a set of assumptions. But if these assumptions are not valid, private hackback could become a federal problem through uncontrolled escalation and spillover from these private counterstrikes.

Here are five assumptions commonly made in discussing hack backs:

Private companies can attribute.

The idea of legalizing hack back operations is based on the assumption that the defending company can attribute the initial attack with pin-point precision. If attribution is not achieved with granularity and precision, the right to cyber counterstrike would be the right to strike anyone based on suspicion of involvement. Very few private entities can, with high granularity, determine who attacked them. The lack of norms and a right to strike back, especially if the precision in the counterstrike is not perfect, would increase entropy and deviation from emerging norms and international governance.

Counterstriking corporations can engage a state-sponsored organization.

Things might spin out of control. The old small tactics rule – anyone can open fire, only geniuses can get out unharmed - applies. A counterstriking corporation may perceives that it can handle the adversaries, maybe believing the bad guys are an underfunded group of college students that hacks for fun, only to later find out that it is a heavily funded and highly potent foreign state agency that hacks for destruction and mayhem. A probing counterattack would not be enough to determine the operational strength, ability, and intent of the potential adversary. Following the assumption that the counterstriking corporation can handle any adversary is embedded the assumption that there will be no uncontrolled escalation.

The entire engagement is locked in between parties A and B.

Perhaps a follow-up assumption in this scenario is that a hack back would create a deterrence that prevents the initial attacker from continuing attacking. The defending company needs to be able to counterattack with such magnitude that the initial attacker thinks twice about further attacks. If deterrence cannot be established it would likely lead to escalation or a tit-for-tat game without any decisive conclusion and continue until the initial attacker decides to end the interchange.

The initial attacker has no second strike option.

The belief is that the exchange will occur with a specific set of cyber weapons and aim points. This means the back-and-forth cannot lead to further damages. A new set of second strikes would not be an uncontrolled escalation as long as the targeting occurred within the same realm and values as the earlier strikes. The second strike option for the initial attacker could target unprecedented targets at the initial attackers discretion. Instead, it is more likely that the initial attacker has second strike options that the initial target is unaware of at the moment of counterstrike.

The counterstriking company has no interests or assets in the initial attacker's jurisdiction.

If a multi-national company (MNC) counterstrikes a state agency or state-sponsored attacker the corporation could face repercussions if it has assets in the jurisdiction of the initial attacker. Major companies have interests,

subsidiaries, and assets in hundreds of jurisdictions. The question is then if Company A responds to a cyberattack from China, what will the risks be for Company A's subsidiary in China. The majority of the potential source countries for hacking attacks are totalitarian and authoritarian states. A totalitarian state can easily, and it is in their reach, switch domain and seize property, arrest innocent business travels, and act in other ways as a result of corporate hackback. I am not saying that we should let totalitarian regimes act any way they want – I am only saying that it is not for private corporations to engage and seeking to resolve. It is a government domain to interact with foreign governments.

The idea to legalize corporate hack backs could lead to increased distrust, entropy, and be counterproductive to the long-term goal of a secure and safe Internet. The upside for government to allow corporate hackbacks is likely far lower than the potential for damaging outcome as spillover and multi-domain escalation.

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.

›