Opinion

The long-term cost of cyber overreaction

Jan Kallberg

2 hours ago

Getty Images

The default modus operandi when facing negative cyber events is to overreact. It is essential to highlight the cost of overreaction, which needs to be a part of calculating when to engage and

how. For an adversary probing cyber defenses, reactions provide information that can aggregate a clear picture of the defendant's capabilities and preauthorization thresholds.

Ideally, potential adversaries cannot assess our strategic and tactical cyber capacities, but over time and numerous responses, the information advantage evaporates. A reactive culture triggered by cyberattacks provides significant information to a probing adversary, which seeks to understand underlying authorities and tactics, techniques and procedures (TTP).

The more we act, the more the potential adversary understands our capacity, ability, techniques and limitations. I am not advocating a passive stance, but I want to highlight the price of acting against a potential adversary. With each reaction, that competitor gainscertainty about what we can do and how. The political scientist Kenneth N. Waltz said that the power of nuclear arms resides with what you could do and not within what you do. A large part of the cyber force strength resides in the uncertainty in what it can do, which should be difficult for a potential adversary to assess and gauge.

Why does it matter? In an operational environment where the adversaries operate under the threshold for open conflict, in sub-threshold cyber campaigns, an adversary will seek to probe in order to determine the threshold, and to ensure that it can operate effectively in the space below the threshold. If a potential adversary cannot gauge the threshold, it will curb its activities as its cyber operations must remain adequately distanced to a potential, unknown threshold to avoid unwanted escalation.

Cyber was doomed to be reactionary from its inception; its inherited legacy from information assurance creates a focus on trying to defend, harden, detect and act. The concept is defending, and when the defense fails, it rapidly swings to reaction and counteractivity. Naturally, we want to limit the damage and secure our systems, but we also leave a digital trail behind every time we act.

In game theory, proportional responses lead to tit-for-tat games with no decisive outcome. The lack of the desired end state in a tit-for-tat game is essential to keep in mind as we discuss persistent engagement. In the same way, as Colin Powell reflected on the conflict in Vietnam, operations without an endgame or a concept of what decisive victory looks like are engagements for the sake of engagements. Even worse, a tit-for-tat game with continuous engagements might be damaging as it trains potential adversaries that can copy our TTPs to fight in cyber. Proportionality is a constant flow of responses that reveals friendly capabilities and makes potential adversaries more able.

There is no straight answer to how to react. A disproportional response at specific events increases the risks from the potential adversary, but it cuts both ways as the disproportional response could create unwanted escalation.

The critical concern is that to maintain abilities to conduct cyber operations for the nation decisively, the extent of friendly cyber capabilities needs almost intact secrecy to prevail in a critical juncture. It might be time to put a stronger emphasis on intel-gain loss (IGL) assessment to answer the question if the defensive gain now outweighs the potential loss of ability and options in the future.

The habit of overreacting to ongoing cyberattacks undermines the ability to quickly and surprisingly engage and defeat an adversary when it matters most. Continuously reacting and flexing the capabilities might fit the general audience's perception of national ability, but it can also undermine the outlook for a favorable geopolitical cyber endgame.

Jan Kallberg, Ph.D., is a research scientist at the Army Cyber Institute at West Point and an assistant professor at the U.S. 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 U.S. Military Academy, the Department of Defense or the U.S. government.

About Jan Kallberg

Recommended For You

Biden urged by tech firms to embrace commercial software

Army tests new techniques with airborne jamming pod