1-29-2021

Solorigate attack — the challenge to cyber deterrence

Jan Kallberg
Army Cyber Institute, jan.kallberg@westpoint.edu

Opinion

Solorigate attack — the challenge to cyber deterrence

Jan Kallberg

January 29

Is there a misalignment between civilian academic research and the cyber operational environment? (MF3D/Getty Images)

The exploitation of SolarWinds' network tool at a grand scale, based on publicly disseminated information from Congress and media, represents not only a threat to national security — but also puts the concept of cyber deterrence in question. My concern: Is there a disconnect between the operational environment and the academic research that we generally assume supports the national security enterprise?

Apparently, whomever launched the Solorigate attack was undeterred, based on the publicly disclosed size and scope of the breach. If cyber deterrence is not to be a functional component to change potential adversaries' behavior, why is cyber deterrence given so much attention?

Maybe it is because we want it to exist. We want there to be a silver bullet out there that will prevent future cyberattacks, and if we want it to exist, then any support for the existence of cyber deterrence feeds our confirmation bias.

Herman Kahn and Irwin Mann's RAND memo "Ten Common Pitfalls" from 1957 points out the intellectual traps when trying to make military analysis in an uncertain world. That we listen to what is supporting our general belief is natural — it is in the human psyche to do so, but it can mislead.

Here is my main argument — there is a misalignment between civilian academic research and the cyber operational environment. There are at least a few hundred academic papers published on cyber deterrence, from different intellectual angles and a variety of venues, seeking to investigate, explain and create an intellectual model how cyber deterrence is achieved.

Many of these papers transpose traditional models from political science, security studies, behavioral science, criminology and other disciplines, and arrange these established models to fit a cyber narrative. The models were never designed for cyber; the models are designed to address other deviate behavior. I do not rule out their relevance in some form, but I also do not assume that they are relevant.

The root causes of this misalignment I would like to categorize in three different, hopefully plausible explanations. First, few of our university researchers have military experience, and with an increasingly narrower group that volunteer to the serve, the problem escalates. This divide between civilian academia and the military is a national vulnerability.

Decades ago, the Office of Net Assessment assessed that the U.S. had an advantage over the Soviets due to the skills of the U.S. force. Today in 2021, it might be reversed for cyber research when the academic researchers in potentially adversarial countries have a higher understanding of military operations than their U.S. counterpart.

Second, the funding mechanism in the way we fund civilian research gives a market-driven pursuit to satisfy the interest of the funding agency. By funding models of cyber deterrence, there is already an assumption that it exists, so any research that challenges that assumption will never be initiated. Should we not fund this research? Of course not, but the scope of the inquiry needs to be wide enough to challenge our own presumptions and potential biases at play. Right now, it pays too well to tell us what we want to hear, compared to presenting a radical rebuttal of our beliefs and perceptions of cyber.

Third, the defense enterprise is secretive about the inner workings of cyber operations and the operational environment (for a good reason!). However, what if it is too secretive, leaving

civilian researchers to rely on commercial white papers, media and commentators to shape the perception of the operational environment?

One of the reasons funded university research exists is to be a safeguard to help avoid strategic surprise. However, it becomes a grave concern when the civilian research community research misses the target on such a broad scale as it did in this case. This case also demonstrates that there is risk in assuming the civilian research will accurately understand the operational environment, which rather amplifies the potential for strategic surprise.

There are university research groups that are highly knowledgeable of the realities of military cyber operations, so one way to address this misalignment is to concentrate the effort. Alternatively, the defense establishment must increase the outreach and interaction with a larger group of research universities to mitigate the civilian-military research divide. Every breach, small and large, is data that supports understanding of what happened, so in my view this is one of the lessons to be learned from Solorigate.

Jan Kallberg is a research scientist at the Army Cyber Institute at West Point, managing editor of the Cyber Defense Review, 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 or the Defense Department.

About Jan Kallberg

Recommended For You