4-7-2021

Bye bye, cyber Pearl Harbor

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

By **Jan Kallberg, US Army Cyber Institute** Mar 17, 2021

The Editors: We're pleased to share this op-ed from Jan Kallberg, of the US Army Cyber Institute at West Point. He'd note of skeptical caution about the historical metaphors that often inform thinking about cybersecurity policy and stra he takes up one of them: concern about a "cyber Pearl Harbor." It's not that a damaging cyberattack couldn't achieve surprise, as the 1941 attack on Pearl Harbor did. (Consider, for example, the possibility of exploiting SolarWinds for r espionage by using it to stage attacks that could have a kinetic effect on critical infrastructure.) Rather, it's that it's im understand that the adversary has its own challenges to overcome, and any credible adversary will have its own stra And it's also worth remembering that the adversaries have their problems, too.

The repeated cyber analogy from the US historical past invokes the concept of a "cyber Pearl Harbor," a story of a pot massive cyber-attack that, with no warning, would knock out American infrastructure and leave the U.S. vulnerable a respond. The concept of a cyber Pearl Harbor assumes a surprise attack by a prepared and determined adversary lau premeditated sneak attack that has a systematic and crippling impact on the United States.

Is "cyber Pearl Harbor" still a useful metaphor?

The question is if the term is still relevant in year 2021. It's a plausible narrative: a cyber Pearl Harbor could have happ term was first introduced. The name originated in the 1990s. With industrial control systems designed without securi with immature Internet applications, with a massive growth of systems going online without reliable defenses, and w security awareness, it was probably a genuine concern in the 1990s. As an example of security awareness in the 199 term "cyber defense" only had four references in the search engine of that time – Altavista. When I search "cyber defe in Google, the search engines tell me they've found 1,480,000 references.

What makes the term "cyber Pearl Harbor" relevant is the fact that Pearl Harbor was a sneak attack. So was 9-11, w warnings of a massive cyberattack. But in both these cases there were significant warnings and indicators that an ev could unfold. That may be one difference between Pearl Harbor and Cyber Pearl Harbor: in the cyber Pearl Harbor na incremental buildup of hostilities, conflict, or tension. According to cyber Pearl Harbor proponents, there are no warni U.S. is not prepared. That leaves you with the feeling that a cyber Armageddon is just around the corner. I'm not conv

In my personal view, the cyber Pearl Harbor analogy is no longer relevant, if it ever was, because it's based on severa assumptions.

Where's the cyber knock-out punch?

First, a cyber Pearl Harbor would require a systematic point of failure that impacted multiple technical infrastructure la our society. Even if not all sectors are well defended or completely resilient, we cannot ignore the fact that over the las vast majority of corporations, utilities, local and state governments, have made significant investments in cybersecurit is not only hardware and software, in forming defenses in depth, and in hiring trained staff. Exercises and data resilien also followed, as have planning for continuity of operations, deployment of backup facilities, and of other steps taken preparedness and recovery.

A nation-state cyberattack would normally have a strategic objective.

Second, if the majestic cyber Pearl Harbor systematic point of failure existed, the potential adversary would sit on it fo potential adversary had in their hand this opportunity to give the Americans a significant blow, they would be unlikely same moment they acquired it. An adversary cannot repeat the high magnitude exploitation of a given vulnerability, a adversary has acquired this opportunity, it would be a loss to execute the attack in isolation, at the point of discovery. point of discovery, the opportunity would have no tangible value unless there were some strategic goal the end state

That also assumes that there are only two actors – the U.S. and an evil empire out there waiting to pull the trigger on vulnerability. The U.S. information technology infrastructure is persistently under attack from multiple actors, including networks, and hostile groups, and they're active 24/7/365. Suppose a systematic massive vulnerability existed that w execution of Cyber Pearl Harbor. In that case, it would be improbable that no one else, except one adversary, had iden scale vulnerability. Every threat actor has its agenda. If several threat actors discovered the vulnerability, it is logical th actors would launch an attack at the point of discovery or near time after that. An actor with no strategic end game, c online vandalism and defacement, would not sit on the vulnerability and wait.

event.

Note on the author: Jan Kallberg is a research scientist at the Army Cyber Institute at West Point, managing editor of Review, and an assistant professor at the U.S. Military Academy. The views expressed are those of the author and do official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy, or the Defense Depart

Trending News

1. Keeping tabs on who the Shanghai PD is tracking. DPRK phishing for security researchers. US DHS cyberstrategy. Wa
2. COVID-19 phishing might be Goblin Panda. Ubiquiti confirms extortion attempt. More universities hit by Accellion com
3. CyberWire Live - Q1 2021 Cybersecurity Analyst Call
4. Malware droppers posing as video game cheats. Bahamut may be behind new cyberespionage campaign. North Korea security researchers.
5. Cyber intelligence sharing. Bug disclosure for Defense contractors. Crypto Wars update. Surveillance vendors. SolarWi response.