**Our NSA pushes back and its offensive cyber operations have countered the many hackers and digital spies with apparent effectiveness.**

*NSA Director, General Paul Nakasone reports that NSA has, since 2018, executed offensive digital operations that have been successful in deterring the many digital criminals and digital spy operations. However the threat is intensive and constant, and our offensive operations are only partially successful. Our counter efforts will be continuing indefinitely.*

General Paul Nakasone, the Director of the National Security Agency and Commander of our Cyber Command quietly announce in early November that we are now fully focused on “persistent engagement,” needed to counter the many attacks on our government and civilian computer networks. Fighting fire with fire, persistent engagements have made the enemy pay for their offensive operations. One thing to note about digital warfare, it is conducted in the "grey area," which means the digital attacks are painful, costly and harmful, but do not cross the threshold that justifies kinetic response.

The enemy, which includes both foreign governments and criminal entities has penetrated our government and civilian computers networks and pilfered a huge amounts of valuable data. Our civilian computers attacked include major software companies, including Microsoft, power networks our hospital networks, and even food production plants. A major offensive against all these targets can easily cripple a nation.

Nakasone stated that our persistent engagement (offensive operations) are impacting our enemy's, key institutions, and are effective, but noted that only the enemy can reveal that effectiveness of our persistent engagements.

While the need for nuclear deterrence has not gone away, cyber operations now takes center stage in national security planning.

***==================================================================***

**SOURCE;** ***https://breakingdefense.sites.breakingmedia.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/***

**Nakasone: Cold War-style deterrence ‘does not comport to cyberspace’**

*"Strategic competition is alive and well in cyberspace, and we're doing it every day with persistent engagement," the CYBERCOM and NSA leader said.*

**By BRAD D. WILLIAMS, on November 04, 2021**

**

***Director of the NSA and Commander of the U.S. Cyber Command Paul Nakasone speaks during a hearing on April 15, 2021 in Washington, D.C.***

***W***ASHINGTON: Gen. Paul Nakasone reiterated on Wednesday that traditional military deterrence “is a model that does not comport to cyberspace,” despite oft-heard calls for cyber deterrence in the wake of the latest cybersecurity incident.

Indeed, **the idea that**[**traditional deterrence does not work in cyberspace is not new**](https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/). In fact, CYBERCOM formalized the view in its [2018 National Cyber Strategy](https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf). Yet many observers continue to ask how the US can completely deter adversaries such as Russia, China, Iran, North Korea, and even ransomware gangs in the cyber domain — a goal Nakasone and others have realized is practically futile.

“I grew up in the deterrence world,” the CYBERCOM and National Security Agency leader told the 2021 Aspen Security Forum, referring to the Cold War years when the US and Soviet Union operated according to nuclear deterrence, given the mutually assured destruction presumed to follow a misstep by either side. Traditional deterrence is a “binary world” of “yes or no” in regards to conflict, Nakasone observed.

But those rules don’t hold in cyberspace, where much of the nefarious activity — **whether by nation-states, cybercriminal ransomware gangs, or other threat actors plays out non-stop in an ambiguous strategic gray zone.**

To this point, in a separate talk at Aspen, **Joint Chiefs Chairman Gen. Mark Milley said the Pentagon sees “millions of attempts” to breach its networks every day. “We are in a very, very contested domain in cyber,” Milley said. “Every day our nation is literally being hacked**. Is it out there? Yes. Is it serious? Yes.”

The **benefits of cyber operations have proven significant for US adversaries, making total deterrence all but impossible.** After all, relative to kinetic conflict, the financial cost to operate in cyberspace is negligible, the barriers to entry practically nonexistence (given the right talent), and the ease of operating trivial. **And why bother with the time and risk involved in human intelligence gathering when one can sit halfway across the world and waltz right in the back door**[**to steal reams of data on US cleared personnel**](https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach)**? Or**[**pilfer Americans’ health care data in bulk**](https://en.wikipedia.org/wiki/Anthem_medical_data_breach)**? Or**[**exfiltrate heaps of Americans’ financial data**](https://www.fifthdomain.com/congress/capitol-hill/2017/10/03/congressmen-criticize-equifaxs-response-to-hack-ongoing/)?

Meanwhile, the consequences to adversaries for acting in cyberspace — assuming a hack can be attributed with high confidence in the first place — are oftentimes insignificant judging by adversaries’ continued operations, despite the [high-profile naming and shaming](https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion) or the occasional [arrest](https://www.justice.gov/usao-sdca/pr/fbi-takes-down-russian-based-hacker-platform-arrests-suspected-russian-site).

This is especially the case as **long as threat actors, particularly nation-states, keep cyber activities below a level justifying a kinetic response**, a concept known as operating in the gray zone. Cyberespionage campaigns such as SolarWinds and the Microsoft Exchange hacks are viewed as gray-zone activities — often frustrating, sometimes costly, but never justifying a traditional military response.

Limited deterrence generally keeps adversaries from escalating beyond the gray zone, observers note. James Lewis, a cyber expert at the Center for Strategic & International Studies, [suggested earlier this year](https://breakingdefense.com/2021/03/solarwinds-hack-the-truth-is-much-more-complicated/) it would be foolish for adversaries to do so.

“The question would be: When would it be in Russia’s interest to launch some kind of major, old-style attack, and I think the answer is never,” Lewis said. “Why would they do that? They’re winning now. …The Chinese probably feel the same way.”

**To address continued hacks against American infrastructure and institutions, CYBERCOM has adopted a doctrine known as “persistent engagement**.” Persistent engagement acknowledges the futility of totally deterring adversaries from operating in cyberspace and instead **focuses on proactively disrupting those activities** — ideally, before they can inflict damage.

Nakasone has [previously characterized persistent engagement](https://breakingdefense.com/2021/03/cybercom-plays-key-role-as-solarwinds-unfolds-gen-nakasone/) as “centered on the construct of both enable and act.” Nakasone said “enable” means sharing threat indicators, pooling resources, and providing insights. “Act” entails “hunt forward” — that is, proactively identifying security vulnerabilities in partners’ networks overseas, with permission — as well as offensive operations and information operations.

So, **rather than cyber deterrence, Nakasone and other officials speak instead of “imposing costs” on adversaries via persistent engagement**.

**“Strategic competition is alive and well in cyberspace, and we’re doing it every day with persistent engagement,” Nakasone told the Aspen audience**. “We’re in competition every day…. We’ve got to somehow impact adversaries who don’t get the message. We’ve got to impose costs. **The important thing to emphasize here is we have the capabilities, we have a process to enable capabilities, and we have the people to carry out the capabilities**.”

The latest known example of persistent engagement allegedly occurred **within the past few months, when CYBERCOM worked with an unnamed foreign government to “shut down” the ransomware gang REvil’s operations,** as [first reported by the Washington Post](https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html). REvil has conducted a number of high-profile ransomware attacks in recent years.

CYBERCOM declined to confirm or deny the Washington Post’s report and did not provide additional comments.

Despite the setback, REvil is unlikely to cease operations permanently. More than likely, the disappearance is merely a pause. The gang will likely reemerge in the future with a new online identity and brand before resuming its lucrative ransomware attacks. Or, put another way, it’s unlikely to be totally deterred.

In his talk, Nakasone also harkened back to the 2018 US midterm elections, which he called “the seminal event” in CYBERCOM’s evolution toward persistent engagement. “To understand future, you have to go back to 2018. Out of ’18, we learned a few things. We were putting the finishing touches on hunt forward,” the general said. In 2018, CYBERCOM decided, “We’re going to act. We’re not going to watch anymore,” he added.

**Washington Post columnist David Ignatius, who moderated the discussion, noted that some reports said CYBERCOM caused adversaries “pain” in 2018. “Did you make them feel pain?” Ignatius asked Nakasone. Nakasone smiled, paused for a moment, and said, “You’d have to ask them.”**

Still, despite the purported hunt forward operations to protect the 2018 and 2020 elections, as well as interfering with REvil, **the ability to permanently stop threat actors via persistent engagement or other means will likely continue to elude the US**.

Indeed, **Microsoft**[**revealed last week**](https://breakingdefense.com/2021/10/russian-solarwinds-hackers-launch-new-attack-on-it-supply-chain-microsoft-says/)**that the Russia’s Foreign Intelligence Service (SVR) has not been deterred from hacking US infrastructure and companies since**[**being outed and sanctioned**](https://breakingdefense.com/2021/04/us-slaps-russia-with-sanctions-other-actions-for-solarwinds-campaign/)**for the SolarWinds** campaign in April. Nor since President Joe Biden in June asked Russian President Vladimir Putin to please stop hacking the US. The SVR has continued operations, merely changing its targets and some tactics. And so the unseen competition in cyberspace continues unabated.

One unknown metric of success, of course, is just how many CYBERCOM (and NSA) operations have succeeded, given their reluctance to confirm or deny their own operations, much less discuss them in detail. So, for every periodic high-profile hack that is discovered, it could be that dozens or even hundreds of hacks are proactively prevented via persistent engagement.

Given the futility of total cyber deterrence, one thing is for certain: **“Going forward, cybersecurity is going to be central to our national security,” Nakasone said.**