**Jamming their Jammers.**

In the February 2022 issue of Air Force Magazine, John Tirpak writes ofour **“Dominating the Spectrum - Foreign advances and U.S. neglect have realigned the electromagnetic battlefield. Here’s how USAF is fighting back.”**

**Have we been sleeping?** Our Chief of Staff, General Charles Brown notes that while we were focused on counterinsurgencies in the Middle East, not advanced modern warfare, necessary for victory in current warfare, both Russia and China have focused on Cyber and Electronic warfare, and are now more advanced than us. Many of our military leaders in all three services basically agree that while we were focused on the effort needed to fight the Taliban, we have not dedicated sufficient resources to deal with Cyber and Electronic warfare and need to change our policies to counter the capabilities of our major opponents, Russia and China.

Indeed our government agencies, hospitals and power grids have been disrupted and even penetrated by Russian hackers who are alleged to just be criminals blackmailing for money, but these hackers are strongly believed to be authorized by the Russian government to conduct these operations. We have also detected Chinese hackers probing our power plants.

These offensive attacks and probes are a dire warning that we are vulnerable and could suffer very serious consequences, if we have neither a great defense or a more effective cyber offense.capabilities. It is noted that even though we have seen the capabilities of Russian hackers, the Chinese are also very competent as they have spent a lot of money and have been strategizing their Cyber operations for many years.

General HInote, our Air Force Deputy Chief of Staff stated that he believes that the Chinese have become so good because they believe that Cyber warfare is a prerequisite for warfare victory.

Our Chief of Staff, General Charles Brown notes that while we were focused on counterinsurgencies in the Middle East, not advanced modern warfare, necessary for victory in current warfare, Russia and China have focused on Cyber and Electronic war and are now more advanced than us, leading our Air Force and Space Command to action.

“The Air Force approved a new Electromagnetic Spectrum Superiority Strategy last April, and Air Combat Command stood up the 350th Spectrum Warfare Wing last summer. In the fall, the service reorganized EMS under the Intelligence, Surveillance, Reconnaissance and Cyber Effects directorate. And this spring, the Air Force and Navy will send Congress a joint report on efforts to accelerate research and deployment of “cognitive” electronic warfare, which leverages machine learning.”

While this new focus is reassuring, we are warned that Space Command needs additional resources, both financial and staffing. The current staffing in Space Command needs additional competent manpower. Qualified manpower is not available within our current Air Force personnel, and must be supplement from the civilian Cyber staffs. This is being down now, but it is taking time to locate and recruit the precise talent and skills needed.

Our National Security Agency (NSA), of course is involved with our Cyber capabilities and we have learned from the Director of the NSA and Commander of the U.S. Cyber Command General Paul Nakasone assure us that NSA is very active conducting daily offensive operations described as “persistent engagement,” which would allow us to react quickly when needed. Our foes, both the Russians and Chinese are either hacking or probing our civilian and government computers regularly and it is good to know that our NSA is poised to respond when needed.

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

**SOURCES**

**Dominating the Spectrum**

***Foreign advances and U.S. neglect have realigned the electromagnetic battlefield. Here’s how USAF is fighting back.***

**By John A. Tirpak*, Air Force Magazine,* Feb. 17, 2022**

“**Asleep at the wheel.”** That’s how Chief of Staff Gen. Charles Q. Brown Jr. described the Air Force’s lackluster approach to advancing the art of warfare in the electromagnetic spectrum (EMS) over the past 30 years.

For most of that time, America was focused on counterinsurgencies in the Middle East, not peer warfare, where mastery of the spectrum can spell the difference between victory and defeat. But with Russia and China having advanced the state of the art, the United States is now fighting to catch up. It’s compelled to consider alternative strategies to dominating in EMS warfare while developing new weapons and systems to counter the advances of peer adversaries.

**Generally, we’re going to have to be able to fight in a fractured way.**

**Lt. Gen. S. Clinton Hinote, USAF deputy chief of staff**

The Air Force approved a new Electromagnetic Spectrum Superiority Strategy last April, and Air Combat Command stood up the 350th Spectrum Warfare Wing last summer. In the fall, the service reorganized EMS under the Intelligence, Surveillance, Reconnaissance and Cyber Effects directorate. And this spring, the Air Force and Navy will send Congress a joint report on efforts to accelerate research and deployment of “cognitive” electronic warfare, which leverages machine learning.

**Yet as the Air Force strives to put all these changes into effect, China and Russia continue to invest in and enhance their capabilities**. **Brewing conflicts in Ukraine, Taiwan or elsewhere may not allow the U.S. time to catch up,** **U.S. forces may have to settle for something far short of spectrum domination: mutual denial**. While U.S. skills in EMS atrophied during its long counterinsurgency fights in Southwest Asia, China matched and surpassed them. So said Lt. Gen. S. Clinton Hinote, deputy chief of staff for strategy, integration, and requirements—USAF’s “futurist”—in a December speech to the Association of Old Crows.

**The Air Force’s EW Quarterbacks**

To implement an EMS strategy, the Air Force needs hardware. It gave up its dedicated electronic warfare aircraft, the EF-111 Raven and F-4G, in the late 1990s. Their functions have since been taken over by the [F-16](https://www.airforcemag.com/weapons-platforms/f-16/) Block 50 Wild Weasel, the EC-130 Compass Call, and a number of other tactical platforms, pods, and systems integrated with aircraft such as the F-22 and F-35.**For the latter half of the 2020s, the Air Force’s tactical EW game will largely be handled by the F-35 Block 4, with its AN/ASQ-239 EW system, and the F-15, fitted with the AN/ALQ-250 Eagle Passive Active Warning Survivability System (EPAWSS).** The EPAWSS is actually based on the F-35’s suite, and BAE Systems, which makes both, expects that it will be able to produce modules common to both systems by mid-decade, sharply reducing sustainment costs while maximizing the efforts of software. The Air Force and Boeing are deciding whether to pursue that approach. Neither the Air Force nor BAE Systems can talk much about how, specifically, the EPAWSS works. Traditionally, such systems have either jammed enemy radars with so much energy that they can’t see targets in the cloud of electrons; or they send an inverse wave to fool the enemy radar that it isn’t there; or it manipulates the return signal to fool the enemy radar into thinking the jet is somewhere else.  
Broadly, it’s an internal system—not a pod—that rapidly senses and collects “hits” of electromagnetic energy, even from low probability of intercept radars, creating a wraparound view of threats for the pilot. EPAWSS is integrated with the F-15’s chaff and flare dispensers, and is “interoperable” with the F-15’s active electronically scanned array (AESA) radar, BAE said, meaning it can jam enemy radar without interfering with the jet’s own radar or radar warning receivers.  
The EPAWSS has a modular, open-system architecture so that even small businesses with “neat tricks” will be able to get onto the platform, said Jerry Wohletz, BAE Systems vice president and general manager for electronic warfare. And while he couldn’t say how fast the EPAWSS can detect a threat and respond, it’s “the fastest system that has ever been deployed.”   
“We’re using fundamental math and physics,” Wohletz said. “We’re not going after artificial intelligence  or machine learning,” but “raw, brute force overmatch against what the adversaries can field in speed.” He said that provides an advantage in decision-­making: “if you’re faster than your adversary, you own your adversary.”  
The system will provide “freedom of maneuver” for the non-stealthy, 1970s-vintage F-15 near highly contested airspace, Wohletz said. The F-15 will be able to get “within meaningful ranges” of enemy air defenses with a large load of weaponry, “so they can use all of that armament … at a very extended combat range.” Without EPAWSS, the Air Force has said the F-15 would be unusable near contested airspace after about 2025.

[](https://www.airforcemag.com/app/uploads/2022/02/002_F15E_F15EX_SIDEBAR.jpeg)EPAWSS will keep vintage F-15s in the fight by allowing the aircraft to get close to enemy air defenses carrying many weapons. The system will be fielded operationally on the F-15EX (at right) in fiscal 2024. **1st Lt Savanah Bray**

Rather than rely on a library of set piece responses, the EPAWSS can deliver a “cocktail of approaches” that will challenge an adversary’s ability to process the data on a useful timeline.

By building on the F-35’s system, the EPAWSS and F-35 will both be able to take advantage of software and update investments, Wohletz said.

“Now EPAWSS is feeding back into [F-35] Block 4 upgrades,” he said, “and we’re going to take that to the next level, and drive more commonality into the system, toward the ideal situation of some day, getting to … where the modules start to be interchangeable between aircraft.” That’s key, because “you hear from DOD leaders, ‘sustainment is killing us,’” he said. Common modules would ease maintenance by making more line replaceable units available and reduce cost by producing them in greater quantities.

Major software updates will likely be made in six-to-12 month intervals, Wohletz said, but in development, there have been as many as five a year, indicating that faster updates are possible if necessary.  
EPAWSS suffered from serious setback early in development, but BAE Systems put “a lot of skin in the game,” and those issues are largely resolved, Wohletz said. The Pentagon’s Director of Operational Test and Evaluation, in its 2022 annual report, said the Air Force is testing EPAWSS now and will start fielding it operationally on F-15Es in fiscal 2023, and on the new F-15EX in fiscal 2024.

“That was a time of de-emphasis of electronic warfare, electronic attack, electronic defense, maneuvering in the electromagnetic spectrum,” Hinote said. “They studied us. … They studied many of you and your work, and they did their best to come up with ways of countering what you were doing in the electromagnetic spectrum.”

Today, as a result, China can send pulses from their radars “that are different time,” Hinote said. “Yes—that’s happening right now.”

**The Chinese became so good at electromagnetic spectrum warfare in the interim that today “they absolutely believe that [EMS] superiority is a prerequisite for victory,”** Hinote said, suggesting that denying China use of the spectrum could be enough to deter it from fighting. “Maybe it’s enough that we deny the use of the electromagnetic spectrum to China,” he said, by filling “the airwaves with electromagnetic energy to the point where you could walk on it. … To make it so difficult to operate in the electromagnetic spectrum that it’s mutually denied space.”

Like the “no man’s land” between the opposing trenches in World War I, the spectrum would be a region where neither side has superiority or advantage. “Gum it up so much that China is fearful of their ability to operate in that area,” Hinote said.

The Air Force is “pretty good” at operating with communication severed, sensors jammed, and space connectivity denied, Hinote said. It’s practiced the concept for years in “A Day Without Space” exercises. “Generally, we’re going to have to be able to fight in a fractured way,” he said. A “fractured versus fractured force fight is a very interesting one to us.”

Hinote urged listeners to be “open” to  and accept as fact that wholesale superiority may no longer be possible. He urged listeners to be open to the idea of mutually denied EMS and accept that wholesale superiority may no longer be possible.

Critics warn that there are drawbacks to a scorched-sky, no-man’s-land approach to EMS. Ret. Maj. Gen. Kenneth R. Israel, in a January paper for AFA’s Mitchell Institute for Aerospace Studies, wrote that “slugging it out electronically with our adversaries obviates all the advantages of such innovative operational concepts such as mosaic warfare.”

U.S. strategy, he argues, should be using all its technological capabilities to gain decision advantage over adversaries.

Hinote, however, counters that **the answer is not so much abandoning dominance as narrowing the focus of where and when it’s needed.**

“There’s no one out there … who seriously believes we can project air superiority in all places, at all times, and at all altitudes,” **Hinote said. Rather, America must focus on ensuring the ability to dominate airspace at the place and time of its choosing. The same approach could be applied to EMS warfare.**

In a densely jammed battlespace, confusion can offer opportunities, Hinote suggested. Given that the battlespace will be filled with platforms that all have “apertures” and “energy producers,” the U.S. could “use software to be able to generate certain kinds of directed energy,” and could inject cyber weapons into the mix. He declined to elaborate because details are classified, but added: “I’m really excited about this.”

[](https://www.airforcemag.com/app/uploads/2022/02/003_China_J16D_EW_aircraft.jpg)China invested heavily in electronic warfare capabilities over the past two decades, and it paid off. One such investment was the J-16D electronic warfare aircraft with mounted EW pods, seen here. **China Ministry of Defense via CGTN**

**NEW INVESTMENT**

Brig. Gen. Tad  D. Clark, USAF’s director of the electromagnetic spectrum superiority directorate, told the Old Crows that it will be important to inject “that doubt, that hesitation” into an adversary’s decision-making. “That confusion is winning for us.” If adversaries can be forced to pause and reconsider whether “the odds are in their favor … we’re slowing their decision matrix down.”

Investing in new EMS capabilities will pay off, Clark said, because achieving cyber effects or spectrum denial “gets us to the desired effects—nonkinetic effects—for pennies on the dollar” compared to kinetic weapons.

**Col. William E. Young, commander of the 350th Spectrum Warfare Wing, said his job is to take all the sensors, jammers, directed-energy weapons and other tools and generate my­riad unpredictable combinations. Like Lego bricks, they can be mixed and matched “into on-demand, ad hoc kill webs.” This imposes complexity on adversaries by creating a nearly impossible task: anticipating all the different combinations they could face.**

This “Lego” approach signals another change, from packaging such systems “at the platform level” to instead doing so “at the subsystem level,” he said.

According to Hinote the U.S. remains the leader in “signature management stealth” in both long- and shortwave frequencies, as well as in other EMS efforts. Stealth “was revolutionary and it still is,” he said. “The idea that from very low frequencies to high frequencies, you can manage signature, and you can do it in all aspects, and you have the ability, in the same platform, to reduce infrared emissions—those are incredible advances.” U.S. platforms can now claim “very, very low signature” in radio frequencies and infrared.

The Pentagon is also rapidly building its partnership with the commercial sector, where competition is fierce in developing autonomous systems and leveraging machine learning for all manner of applications. Such automation also has huge implications for next-generation electronic warfare.

Commercial innovation may drive these advances more than defense requirements, making the Pentagon more of an adopter than a developer. By contrast, China requires close cooperation between commercial developers and military customers.

Because there is little commercial value to “catch a pulse,” manipulate it, and retransmit it all at very high speed, the military will always need focused programs in EMSO [EMS operations], Hinote said. “We have to bring together the military side and the commercially driven side,” he said. “We have to be ambidextrous.”

**MOVING FASTER**

 In his paper, Israel said the Air Force has been good at setting EMSO goals, but isn’t swiftly reaching them.

“We do not need an aspirational document, but an actionable document that lays out what we need to do and by when, to achieve spectrum superiority,” he said. “We do not have the luxury of time or promised future resources to fix our [electronic warfare and] EMSO gaps.”

Israel said the Air Force has too few EMS warfare specialists and insufficient incentives to retain the expertise it has, let alone to draw new people into the field.

“We must rebuild and expand our EMSO expertise fast,” he said. USAF graduates just 80 electronic warfare officers a year from the Navy’s Joint Combat Systems Officers school—too few to meet demand. Talent is needed with “a broad array [of] interrelated, spectrum-dominated technologies, to include artificial intelligence, networks, 5G, complex waveforms, interferometry, antenna designs, microelectronics, phase-reversing phenomena, digital processing, cloud topologies, metadata analytics, encryption, directed energy, and other forms and modes of electronic warfare.”

It is unreasonable to expect “a social studies or music major will understand and transition easily into mastering the essentials of cognitive and complex signals,” Israel said

=993Rather than seek to grow these experts organically, Israel said the Air Force should hire trained industry experts directly and insert them at the appropriate levels of command.

“If we can bring on doctors with special skills into the DOD workforce, we should be able to bring on highly qualified, commercially trained EMSO experts and give them an appropriate … rating commensurate with their expertise and training,” he wrote.

**Without spectrum superiority, it won’t be possible to achieve the dominance promised by joint all-domain command and control, Israel said.**

Hinote agreed. In his remarks to the Old Crows, Hinote said that without a fully integrated force, with all domains connected and working together, wargames show clearly that “it’s not pretty. …We lose.” With the passage of time, “we see an increasing trend where we don’t accomplish the objectives. And in fact, we lose faster,” without joint all-domain command and control. “That’s not a place any of us want to be.”

A simple way to look at it is that “if you have vulnerability in one domain, you can use strength in another” to compensate, he said. When broad networking is added to wargames, “then we actually did pretty well against the most advanced threats out there.” But there’s a “lot of work to do” to bring the domains together and eliminate stovepipe thinking and action. The longer the U.S. waits to truly implement it, the more adversaries will exploit “the investments they have made in tearing apart and fracturing the United States military command and control.”

Hinote also said a sea change is underway in how to conduct electronic warfare. The old method where there were “libraries” of threats and how best to respond to each of them “may not help us in the way they helped us in the past.” It will take AI and machine learning to rapidly assess and respond to threats.

“You’re going to see your worthy rival … change their force presentation in the electromagnetic spectrum pretty quickly. And that’s going to require us to be agile.”

Hinote’s upbeat about the future of EMSO, saying, “I actually think we compete pretty well. … And we certainly do not want a fight. We want to deter and protect our interests and those of our partners and allies.”

In a shooting war with China, “nobody wins,” Hinote admonished. So, “it’s important that we do things that help us accomplish our strategy on the strategic defense” and recognize that using the EMS “to support defense in all domains is really, really critical, and good for deterrence.”

It’s an arena where “there’s been … erosion over time and we need to build back, over time, but we need to build immediate capabilities today,” he stated.

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

***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.(Photo by Al Drago-Pool/Getty Images)*

WASHINGTON: 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 the 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.