I'll Be Seeing You

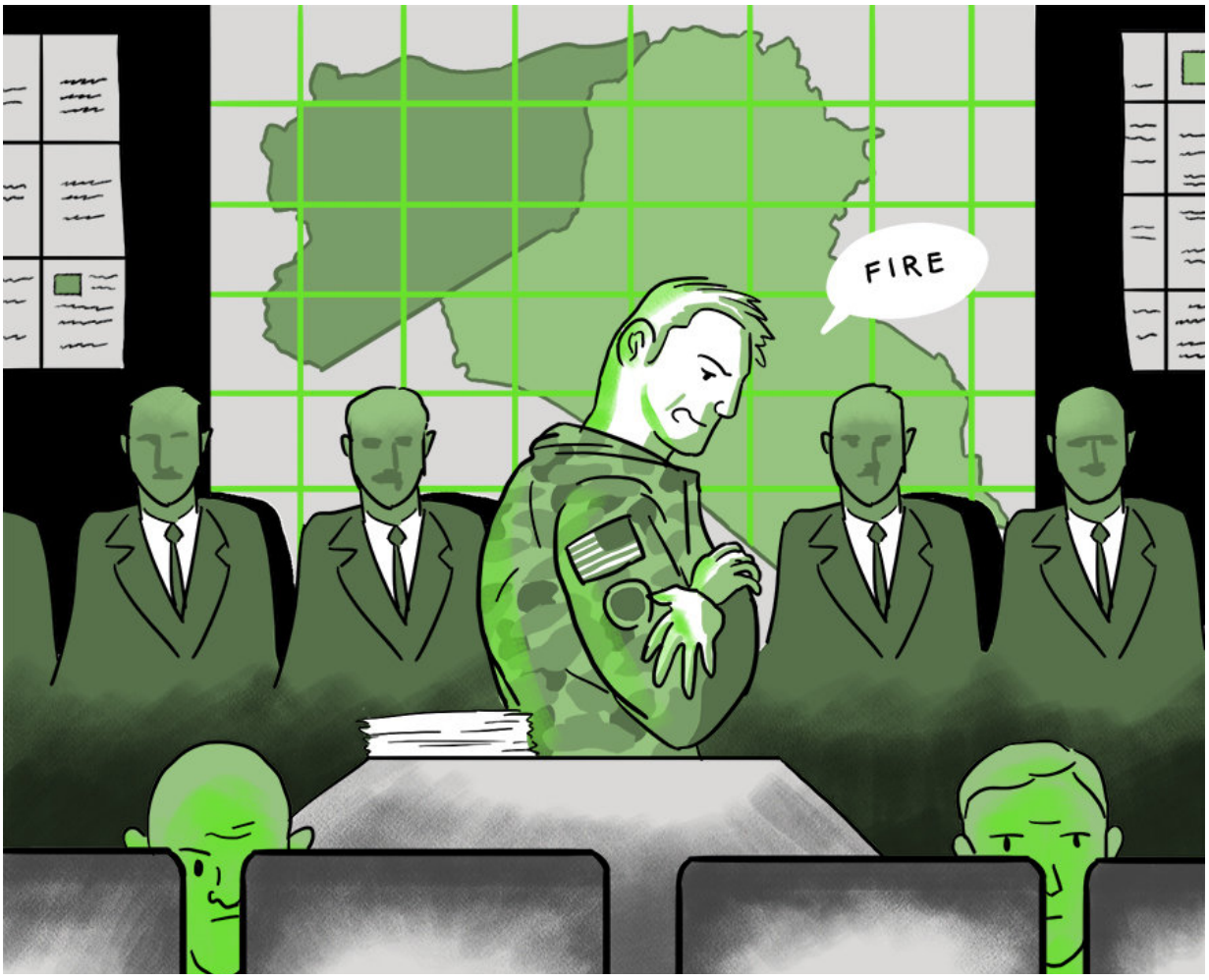
How The U.S. Hacked ISIS

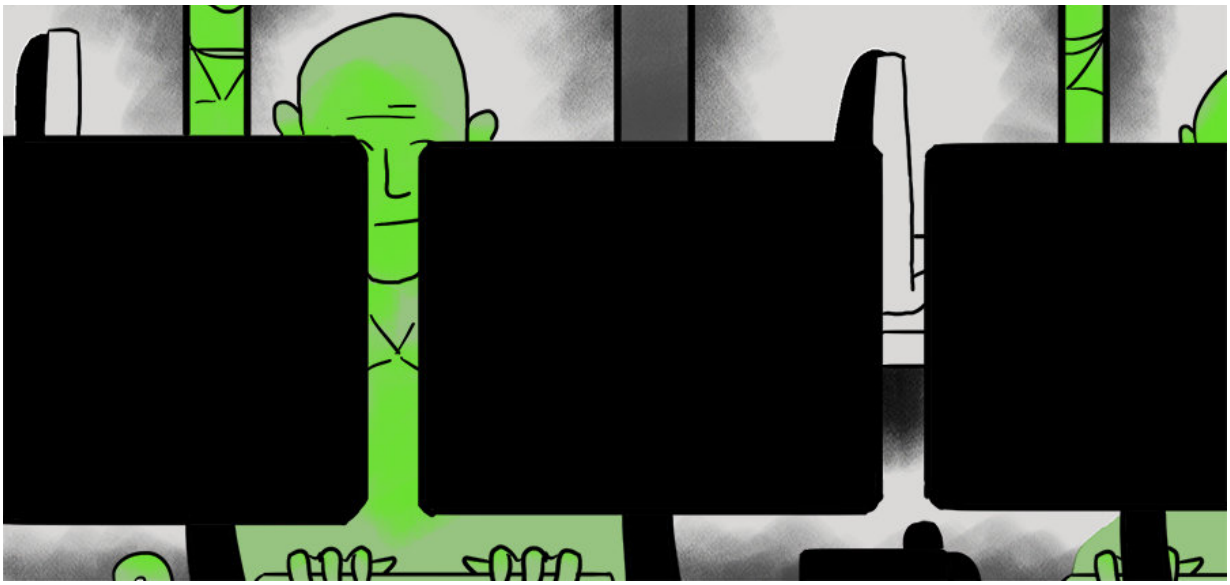
September 26, 2019 · 5:00 AM ET

DINA TEMPLE-RASTON

49-Minute Listen

PLAYLIST Download Transcript





Neil stands in a room with military cyber operators from Joint Task Force ARES to launch an operation that would become one of the largest and longest offensive cyber operations in U.S. military history.

Josh Kramer for NPR

The crowded room was awaiting one word: "Fire."

Everyone was in uniform; there were scheduled briefings, last-minute discussions, final rehearsals. "They wanted to look me in the eye and say, 'Are you sure this is going to work?' " an operator named Neil said. "Every time, I had to say yes, no matter what I thought." He was nervous, but confident. U.S. Cyber Command and the National Security Agency had never worked together on something this big before.

Four teams sat at workstations set up like high school carrels. Sergeants sat before keyboards; intelligence analysts on one side, linguists and support staff on another. Each station was armed with four flat-screen computer monitors on adjustable arms and a pile of target lists and IP addresses and online aliases. They were cyberwarriors, and they all sat in the kind of oversize office chairs Internet gamers settle into before a long night.

"I felt like there were over 80 people in the room, between the teams and then everybody lining the back wall that wanted to watch," Neil recalled. He asked us to

use only his first name to protect his identity. "I'm not sure how many people there were on the phones listening in or in chat rooms."

From his vantage point in a small elevated bay at the back of the Operations Floor, Neil had a clear line of sight to all the operators' screens. And what they contained weren't glowing lines of code: Instead, Neil could see login screens — the actual login screens of ISIS members half a world away. Each one carefully preselected and put on a target list that, by Operation Day, had become so long it was on a 3-foot-by-7-foot piece of paper hung on the wall.

It looked like a giant bingo card. Each number represented a different member of the ISIS media operation. One number represented an editor, for instance, and all the accounts and IP addresses associated with him. Another might have been the group's graphic designer. As members of the terrorist group slept, a room full of military cyber operators at Fort Meade, Md., near Baltimore were ready to take over the accounts and crash them.

All they were waiting for was Neil, to say that one word: "Fire."

In August 2015, the NSA and U.S. Cyber Command, the military's main cyber arm, were at a crossroads about how to respond to a new terrorist group that had burst on the scene with unrivaled ferocity and violence. The one thing on which everyone seemed to agree is that ISIS had found a way to do something other terrorist organizations had not: It had turned the Web into a weapon. ISIS routinely used encrypted apps, social media and splashy online magazines and videos to spread its message, find recruits and launch attacks.

A response to ISIS required a new kind of warfare, and so the NSA and U.S. Cyber Command created a secret task force, a special mission, and an operation that would become one of the largest and longest offensive cyber operations in U.S. military history. Few details about Joint Task Force ARES and Operation Glowing Symphony

have been made public.

Credit: Text: Dina Temple-Raston and Nicole Beemsterboer/NPR. Graphic: Renee Klahr/NPR. Illustrations: Josh Kramer for NPR.

"It was a house of cards"

Steve Donald, a captain in the Naval Reserve, specializes in something called cryptologic and cyber operations, and when he is not in uniform, he is launching cybersecurity startups outside Washington, D.C. He's pale, bespectacled and has the slightly shy demeanor of a computer geek. In the spring of 2016 he received a phone call from the leader of his reserve unit. He needed Donald to come in.

"I said, well, I'm not in uniform [and he said] it doesn't matter — if you have a badge come on in," Donald said. "I can't believe I can actually say this but they were building a task force to conduct offensive cyber operations against ISIS."

Donald had to find a team of specialists to do something that had never been done before — hack into a terrorist organization's media operation and bring it down. Most of the forces flowed in from Joint Forces Headquarters, an Army cyber operation in Georgia. Donald also brought in experts in counterterrorism who understood ISIS and had watched it evolve from a ragtag team of Iraqi Islamists to something bigger. There were operators — the people who would be at the keyboards finding key servers in ISIS's network and disabling them — and digital forensics specialists who had a deep understanding of computer operating systems.

I'LL BE SEEING YOU
Listen To The Radio Version Of This Story

I'LL BE SEEING YOU
The Mysterious Death Of The Hacker Who Turned In Chelsea Manning

I'LL BE SEEING YOU
Elephants Under Attack Have An Unlikely Ally: Artificial Intelligence

"They can say this is good, this is bad, this is where the files are located that we're interested in," he said. He found analysts, malware experts, behaviorialists and people who had spent years studying the smallest habits of key ISIS players. The mission, he explained to them, was to support the defeat of ISIS — to deny, degrade and disrupt them in cyberspace.

This was more complicated than it sounded.

The battle against the group had been episodic to that point. U.S. Cyber Command had been mounting computer network attacks against the group, but almost as soon as a server would go down, communications hubs would reappear. The ISIS target was always moving and the group had good operational security. Just physically taking down the ISIS servers wasn't going to be enough. There needed to be a psychological component to any operation against the group as well.

"This cyber environment involves people," Neil said. "It involves their habits. The way that they operate; the way that they name their accounts. When they come in during the day, when they leave, what types of apps they have on their phone. Do they click everything that comes into their inbox? Or are they very tight and restrictive in what they use? All those pieces are what we look at, not just the code."

Neil is a Marine reservist in his 30s, and it wouldn't be an exaggeration to say that Operation Glowing Symphony was his idea. "We were down in the basement at the NSA, and we had an epiphany," he said. He had been tracking ISIS's propaganda arm for months — painstakingly tracing uploaded videos and magazines back to their source, looking for patterns to reveal how they were distributed or who was uploading them. Then he noticed something that he hadn't seen before: ISIS was using just 10 core accounts and servers to manage the distribution of its content across the world.

The mission — led by a special unit working with U.S. Cyber Command and the NSA — was to get inside the ISIS network and disrupt the terrorist organization's media operation.

Josh Kramer for NPR

"Every account, every IP, every domain, every financial account, every email account ... everything," Neil said. The group's network administrators weren't as careful as they should have been. They took a shortcut and kept going back to the same accounts to manage the whole ISIS media network. They bought things online through those nodes; they uploaded ISIS media; they made financial transactions.

They even had file sharing through them. "If we could take those over," Neil said, grinning, "we were going to win everything."

The young Marine ran into his leadership's office at the NSA, grabbed a marker and started drawing crazy circles and lines on a whiteboard. "I was pointing everywhere and saying, 'It's all connected; these are the key points. Let's go," he recalled. "I felt like I was in *It's Always Sunny in Philadelphia,* when he's doing the mystery investigation for Pepe Silvia. Pictures on the wall and red yarn everywhere and nobody was understanding me."

But as Neil kept explaining and drawing he could see the leaders begin to nod. "I drew this bicycle tire with spokes and all the things that were tied to this one node and then there was another one," he said. "It was a house of cards."

We confirmed this account with three people who were there at the time. And from those scrawls, the mission known as Operation Glowing Symphony began to take shape. The goal was to build a team and an operation that would deny, degrade and disrupt ISIS's media operation.

The cyber equivalent of a surgical strike

The spring and summer of 2016 were spent preparing for attack. And while members of Task Force ARES didn't reveal everything they did to crack into ISIS's network, one thing they used early on was a hacking standby: a phishing email. ISIS members "clicked on something or they did something that then allowed us to gain control and then start to move," said Gen. Edward Cardon, the first commander of Task Force ARES.

Almost every hack starts with hacking a human, cracking a password or finding some low-level unpatched vulnerability in software. "The first thing you do when you get in there is you've got to get some persistence and spread out," Cardon said, adding that the ideal thing is to get an administrator's account. "You can operate freely inside the

network because you look like a normal IT person." (ISIS didn't just have IT people; it had an entire IT department.)

Once ARES operators were inside the ISIS network, they began opening back doors and dropping malware on servers while looking for folders that contained things that might be helpful later, like encryption keys or folders with passwords. The deeper ARES got inside ISIS's network, the more it looked like the theory about the 10 nodes was correct.

But there was a problem. Those nodes weren't in Syria and Iraq. They were everywhere — on servers around the world, sitting right next to civilian content. And that complicated things. "On every server there might be things from other commercial entities," said Air Force Gen. Tim Haugh, the first deputy commander of JTF ARES working under Cardon. "We were only going to touch that little sliver of the adversary space and not perturb anyone else."

If ISIS had stored something in the cloud or on a server sitting in, say, France, ARES had to show Defense Department officials and members of Congress that U.S. cyber operators had the skill to do the cyber equivalent of a surgical strike: attack the ISIS material on a server without taking down the civilian material sitting right next to it.

They spent months launching small missions that showed they could attack ISIS content on a server that also contained something vital like hospital records. Being able to do that meant they could target ISIS material outside Syria and Iraq. "And I looked at this young Marine and said, 'How big can we go?' and he said, 'Sir, we can do global.' I said, 'That's it — write it down, we're going to take it to Gen. Cardon.' "

That Marine was Neil. He began peppering the leadership with ideas. He talked to them about not just hacking one person ... or ISIS in Syria and Iraq, but how to take down the media operation's entire global network. "That's how these attacks work," Neil said. "They start very simple and they become more complex."

There was something else about Task Force ARES that was different: Young operators like Neil were briefing generals directly. "A lot of [ideas] come up that way, like somebody says, 'Well, we could gain access and do this to the files.' Really? You can do that? 'Oh yeah.' Would anyone notice? 'Well, maybe, but the chances are low.' It's like, hmmm, that's interesting, put that on the list."

Cardon said young operators on Joint Task Force ARES understood hacking in a visceral way and, in many respects, understood what was possible in cyberspace better than commanding officers did, so having a direct line to the people making the decisions was key.

"An incredible rush"

By the fall of 2016 there was a team, Joint Task Force ARES; there was a plan called Operation Glowing Symphony, and there were briefings — that had gone right up to the president. It was only then that there was finally a go. This account of the first night of Operation Glowing Symphony is based on interviews with half a dozen people directly involved.

After months of looking at static webpages and picking their way through ISIS's networks, the task force starting logging in as the enemy. They deleted files. Changed passwords. "Click there," a digital forensic expert would say. "We're in," the operator would respond.

There were some unintentionally comical moments. Six minutes in there was very little happening, Neil recalls. "The Internet was a little slow," he said without irony. "And then you know minute seven, eight, nine, 10, it started to flow in, and my heart started beating again."

They began moving through the ISIS networks they had mapped for months. Participants describe it like watching a raid team clearing a house, except it was all online. Logging into accounts they had followed. Using passwords they discovered.

Then, just as their move through targets started to accelerate, a roadblock: a security question. A standard, "what was your high school mascot"-type security question.

The question: "What is the name of your pet?"

The room quieted down.

"And we're stuck dead in our tracks," Neil said. "We all look to each other and we're like, what can we do? There's no way we're going to get in. This is going to stop the 20 or 30 targets after this."

Then an analyst stood up in the back of the room.

"Sir, 1-2-5-7," he said.

"We're like, what?" Neil says.

"Sir, 1-2-5-7."

"How do you know that? [And he said] 'I've been looking at this guy for a year. He does it for everything.' And we're like, all right ... your favorite pet. 1-2-5-7.

"And boom, we're in."

After that, the momentum started to build. One team would take screenshots to gather intelligence for later; another would lock ISIS videographers out of their own accounts.

"Reset Successful" one screen would say.

"Folder directory deleted," said another.

The screens they were seeing on the Ops floor on the NSA campus were the same ones someone in Syria might have been looking at in real time, until someone in Syria

hit refresh. Once he did that, he would see: 404 error: Destination unreadable.

"Target 5 is done," someone would yell.

Someone else would walk across the room and cross the number off the big target sheet on the wall. "We're crossing names off the list. We're crossing accounts off the list. We're crossing IPs off the list," said Neil. And every time a number went down they would yell one word: "Jackpot!"

"We'd draw the line out and I had stacks of paper coming up on the corner of my desk," Neil said. "I knew in about the first 15 minutes that we were on pace to accomplish exactly what we need to accomplish."

Once they had taken control of the 10 nodes, and had locked key people out of their accounts, ARES operators just kept chewing their way through the target list. "We spent the next five or six hours just shooting fish in a barrel," Neil said. "We'd been waiting a long time to do that and we had seen a lot of bad things happen and we were happy to see them go away."

And there was something else that Neil said was hard to describe. "When you reach through the computer and on the other side is a terrorist organization, and you're that close, and you're touching something that's theirs, that they possess, that they put a lot of time and effort in to to hurt you, that is an incredible rush," he said. "You have the control to take that away."

Enough to drive you nuts

Brig. Gen. Jennifer Buckner was one of the people who took the reins of Task Force ARES after Glowing Symphony had started. And after that first night, the mission shifted into a second phase, one aimed at keeping pressure on ISIS with essentially five lines of effort: Keep the media operation under pressure, make it difficult for ISIS to operate on the Web more generally, use cyber to help forces on the ground fighting

ISIS, hobble its ability to raise money, and work with other agencies in the U.S. and allies abroad.

The second phase of Operation Glowing Symphony focused on sowing confusion within ISIS. Joint Task Force ARES operators worked to make the attack look like frustrating, daily-life IT problems: dead batteries, slow downloads, forgotten passwords.

Josh Kramer for NPR

Once the distribution hubs were hamstrung, the second phase of the mission was more creative. Joint Task Force ARES operators started making all those things that drive you crazy about today's technology — slow downloads, dropped connections, access denied, program glitches — and made it start happening to ISIS fighters. "Some of these are not sophisticated effects, but they don't need to be," Buckner said. "The idea that yesterday I could get into my Instagram account and today I can't is confusing."

And potentially enraging. When you can't get into an email account, what do you do? You think: Maybe I mistyped the login or password. So you put it in again and it still doesn't work. Then you type it in more deliberately. And every time you type it, press enter, and are denied, you get a little more frustrated. If you're at work, you call the IT department, you explain the issue and then they ask you if you're sure you typed your login and password in correctly. It is enough to drive you nuts. It might never occur to you, or to ISIS, that this might be part of a cyberattack.

That's what the follow-on phases of Operation Glowing Symphony were about. Psy-ops with a high-tech twist. A member of ISIS would stay up all night editing a film and ask a fellow ISIS member to upload it. Operators with JTF ARES would make it so it didn't quite land at its destination. The ISIS member who stayed up all night starts asking the other ISIS member why he didn't do what he'd asked. He gets angry. And so on.

"We had to understand, how did all of that work?" Buckner said. "And so, what is the

best way to cause confusion online?"

The ideas that flowed up from operators like Neil were endless. Let's drain their cellphone batteries; or insert photographs into videos that weren't supposed to be there. Task Force ARES would watch, react and adjust its plans. It would change passwords, or buy domain names, delete content, all in a way that made it (mostly) look like it was just run-of-the mill IT problems.

"Pinwheels of death; the network's working really slow," Cardon couldn't help smiling as he went through the list. "People get frustrated."

According to three people who were privy to after-action reports, ISIS's media operation was a shadow of its former self six months after Neil said "Fire" to start Operation Glowing Symphony. Most of the media operations servers were down and the group had not been able to reconstitute them.

There were lots of reasons for that, not the least of which is that getting a new server in the middle of a war zone deep inside Syria isn't easy to do. ISIS had plenty of cash but few credit cards, bank accounts or reputable emails that would allow it to order new servers from outside the country. Buying new domain names, which are used to identify IP addresses, is also complicated.

ISIS's popular online magazine, Dabiq, started missing deadlines and eventually folded. The group's foreign-language websites — in everything from Bengali to Urdu — also never came back up. The mobile app for Amaq Agency, the group's official news service, vanished.

"Within the first 60 minutes of go, I knew we were having success," Gen. Paul Nakasone, director of the NSA, told NPR in an interview. "We would see the targets start to come down. It's hard to describe but you can just sense it from being in the atmosphere, that the operators, they know they're doing really well. They're not saying that, but you're there and you know it."

Nakasone was there because he was the head of Joint Task Force ARES when Operation Glowing Symphony actually launched. Nakasone said that before ARES the fight against ISIS in cyberspace was episodic. JTF ARES ensures it is continuous. "We were going to make sure that anytime ISIS was going to raise money or communicate with their followers, we were going to be there."

Some critics have said that the mere fact that ISIS is still on the Web means Operation Glowing Symphony didn't work. Nakasone, naturally, sees it differently. He says ISIS has had to change the way it operates. It isn't as strong in cyberspace as it was. It is still there, yes, but not in the same way.

"We were seeing an adversary that was able to leverage cyber to raise a tremendous amount of money to proselytize," he said. "We were seeing a series of videos and posts and media products that were high-end. We haven't seen that recently. ... As ISIS shows their head or shows that ability to act, we're going to be right there."

Three years after Neil said "Fire," ARES is still in ISIS networks. Gen. Matthew Glavy is now the commander of Joint Task Force ARES. He says his operators still have a thumb on ISIS's media operations; the group is still having a lot of trouble operating freely on the Web. But it is hard to be sure why that is. While ARES has been hacking into ISIS in cyberspace, forces on the ground have driven the group out of most of Syria and Iraq.

ISIS itself has spread out. It now has fighters in Libya and Mali and even the Philippines. Glavy says his operators are still there. "We cannot have for them to gain the momentum that we saw in the past," he told me. "We have to learn that lesson."

"The whole point of the doomsday machine"

For most of the Obama administration, officials refused to talk about cyberattacks. Now the U.S. has not only confirmed the existence of cyberweapons but is starting to tell journalists, like those at NPR, about how they wield them. Cyberattacks, once

taboo to even discuss, are becoming more normalized. In its military authorization bill last year, Congress cleared the way for the defense secretary to authorize some cyberattacks without going to the White House.

But there is a dark side to this new arsenal. The U.S. isn't the only country that has turned to cyber. Consider the case of *Washington Post* journalist Jamal Khashoggi, who was murdered in a Saudi embassy late last year; cybertools are thought to have been part of that case too. "A lot of the preparation for that and the lead-up to it had to do with Saudi Arabia using offensive weapons," said Ron Deibert, the director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

Deibert's researchers found offensive cybertools tracking the journalist and his inner circle. "When we talk about offensive cyber operations, I think it's important to understand that it doesn't always come in one flavor," Deibert said, adding that the Khashoggi case is far from the exception. In Mexico alone, Citizen Lab found 27 cases of this kind of offensive cybertool targeting political rivals, reporters and civil rights lawyers. Six years ago, it rather famously discovered that China had been hacking into the Dalai Lama's computer networks.

Deibert is worried about escalation. "You really create conditions for an escalation of an arms race in cyberspace that really could come back to haunt the United States in the long run," Deibert said. "There's a demonstration effect. The equipment, the software, the methods, the capabilities proliferate." Deibert says U.S. reluctance to use offensive cyber has vanished. "Now ... what we're talking about is something that is more active," he said.

Nakasone made clear things had changed when he talked to NPR a few months ago at the NSA campus at Fort Meade. He uses terms like "persistent engagement" and "defend forward." He says that they are "part of the DOD cyber strategy that talks about acting outside our borders to ensure that we maintain contact with our adversaries in cyberspace."

In other words, you don't wait to be attacked in cyberspace. You do things that would allow you to hack back if there is an attack in the future. That could be deploying a small team in another country that asks for help or "hunting on our networks to look for malware, or it could be as we did in Operation Glowing Symphony, the idea of being able to impact infrastructure worldwide," he said.

All this is important now because you can draw a straight line from Joint Task Force ARES to a new unit from the NSA and U.S. Cyber Command: something called the Russia Small Group. Just as Joint Task Force ARES focused on ISIS, the Russia Small Group is organized in much the same way around Russian cyberattacks.

The mission against ISIS in cyberspace continues, though there is a dark side to fighting with this new arsenal: The U.S. isn't the only country using these kinds of weapons, and experts worry about proliferation.
Josh Kramer for NPR

In June, the *New York Times* reported that the U.S. had cracked into Russia's electrical power grid and planted malware there. Nakasone wouldn't confirm the *Times* story, but it isn't hard to see how planting malware in anticipation of needing it later would fit into the Russia Small Group's operations if it is modeled on ARES.

Nakasone said the first thing he did when he became NSA director in 2018 was to review what the Russians had done in the runup to the U.S. presidential election, so U.S. Cyber Command could learn from it and reverse-engineer it to see how it works. "It provided us with a very, very good road map of what they might do in the future," Nakasone said. He said Cyber Command was poised to act if the Russians attempt to hack the 2020 elections. "We will impose costs," he said, "on adversaries that attempt to impact our elections. I think it's important for the American public to understand that as with any domain — air, land, sea, or space — cyberspace is the same way; our nation has a force."

So why is Nakasone talking about this now?

Deibert thinks this is part of a deterrent justification. "You can't have cyber operations meaningfully deter your adversaries unless they know that you have these capabilities," he said. "But what's not probably being discussed or appreciated is the extent to which there is a systemic effect of the use of these operations. Other countries take notice."

At the end of Stanley Kubrick's film *Dr. Strangelove* there is an iconic scene in which the doomsday bomb is seen as the ultimate deterrent, but it only works as a deterrent if people know it exists. If you don't tell anyone about it, what good is it? "The whole point of the doomsday machine is lost if you keep it a secret," Peter Sellers concludes in the movie.

You could say the same thing about American offensive cyber operations. They have been so stealthy for so long, maybe people don't realize we have them.

We hear all about Russia's influence campaigns and Chinese intellectual property thefts and Iranian hackers trolling American infrastructure, but we rarely hear in any detailed way about the American response. Nakasone appears to be starting to address that.

The irony is that offensive cyber's richest target is us. "The United States is the country most highly dependent on these technologies," Deibert said. "And arguably the most vulnerable to these sorts of attacks. I think there should be far more attention devoted to thinking about proper systems of security, to defense."

That would mean trying to find a way to harden soft targets across the country, getting private companies to beef up their cybersecurity, getting the U.S. government to mandate standards. Offensive cyber, at this point anyway, may seem easier.

NPR's Adelina Lancianese contributed to this story.