An Interview with Paul M. Nakasone

JFQ: *How do you view cyberspace in relation to the world that the joint force operates in? How is operating in cyberspace different from other warfighting domains?*

General Nakasone: As we think about cyberspace, we should agree on a few foundational concepts. First, our nation is in constant contact with its adversaries; we're not waiting for adversaries to come to us. Our adversaries understand this, and they are always working to improve that contact. Second, our security is challenged in cyberspace. We have to actively defend; we have to conduct reconnaissance; we have to understand where our adversary is and his capabilities; and we have to understand their intent. Third, superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral. That's why we must operate continuously to seize and maintain the initiative in the face of persistent threats. Why do the threats persist in cyberspace? They persist because the barriers to entry are low and the capabilities are rapidly available and can be easily repurposed. Fourth, in this domain, the advantage favors those who have initiative. If we want to have an advantage in cyberspace, we have to actively work to either improve our defenses, create new accesses, or upgrade our capabilities. This is a domain that requires constant action because we're going to get reactions from our adversary. From that reaction stems our next move.

Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the *use* of cyber capabilities that is strategically consequential. The *threat* of using something in cyberspace is not as powerful as *actually* using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action.

In the last 10 years, our adversaries have been operating below the threshold of armed conflict, stealing our intellectual property, leveraging our personally identifiable information, or attempting to influence our elections—again, all below the threshold of armed conflict. We have seen our adversaries conduct these strategic campaigns where a series of tactical actions allow our adversaries to have strategic impact by degrading our sources of national power. This is why U.S. Cyber Command [USCYBERCOM] evolved its strategic concept and operational

General Paul M. Nakasone, USA, is Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

approach from a response force to a persistence force, as I explain in my follow-on article in this issue of *JFQ.*

JFQ: *How big is the threat matrix that your command faces? What is the relationship between what your command can do to deter, defend, and defeat adversaries, and what you must rely on other entities to do for cyber defense?*

General Nakasone: Let's take a step back and think about what the threats are to our nation. Ten years ago, threats were primarily other nations trying to exploit us. They were trying to get into our classified systems, steal our information. This is what we consider espionage. There was a period of time where we were concerned primarily about foreign intelligence services coming into our networks and stealing information. That rapidly changed after 2013 when states began disrupting a series of networks within the United States. In 2012–2013, the distributed denial-of-service attacks conducted by the Iranians against the financial networks in New York changed our calculus. These were *disruptive* attacks. So we moved from exploitation to disruption. And by 2014, we saw *destructive* attacks. We witnessed the Iranians in February 2014 conduct a data deletion attack against an American casino. And then in November, Sony Pictures was attacked by the North Koreans. So in a period of 10 years, nation-states progressed from exploitation, to disruption, and finally to destructive attacks against us in cyberspace.

But now we're seeing what many call a *corrosive* threat, which is the ability to weaponize information in order to conduct influence campaigns, steal intellectual property, or leverage someone's personally identifiable information. We've seen our adversaries doing this in places like Iraq, Syria, Ukraine, the 2016 elections, and the hack of the Office of Personnel Management. The question then becomes, "What does a state do to defend against that?"

Thus far, our responses against adversaries who have penetrated our networks or stolen our data or defaced our Web sites have not worked. We've learned that if we're going to have an impact on an adversary, we have to *persistently engage* with that adversary, we have to understand that adversary, we have to be able to impose cumulative costs on that adversary, and we have to be able to understand where that adversary not only is but also where he is going.

JFQ: *A number of years ago, the original concept of having a cyber command was primarily defensive in nature because offensive operations were really not what we are about. But I think the more the public understands about cyber, the more they think we can't just sit back and take punches. How does U.S. Cyber Command see this issue?*

General Nakasone: The Department of Defense [DOD] has an important role to play in the defense of the Nation in cyberspace. We enable both the Department of Homeland Security [DHS] and Federal Bureau of Investigation [FBI] with information and intelligence to more effectively work with the private sector. USCYBERCOM has developed strong partnerships with DHS, the FBI, and sector-specific agencies for select critical infrastructure and key resource sectors. We are doing this purposefully, in partnership with DHS and private-sector leads. It is critical that we develop these partnerships prior to a possible crisis.

JFQ: *We have heard a great deal about Russian interference and misinformation in the U.S. election process, which you noted a moment ago. What other problems are you concerned about from the Chairman's "2+2+1" challenges: Russia and China, Iran and North Korea, and violent extremist organizations? How do they compare to each other, and how are the responses different?*

General Nakasone: I think it is wise, as we look at the alignment of threats, to realize that we're in a period of great power competition. The National Security and National Defense strategies clearly stated that over the past 10 years, any advantages that we had—to include in cyberspace—have eroded as our adversaries have caught up. As we look at near-peer competitors, China and Russia clearly are at the top of the list because they have capacity to operate across the full spectrum of cyberspace operations. Behind China and Russia are the Iranians and North Koreans, who are unique in demonstrating both capability and intent to strike us in cyberspace. We pursue varying strategies to address all four of these nation-states. Additionally, as we have learned in combating [the so-called Islamic State] in cyberspace, we must maintain visibility on nonnation state adversaries as well in this domain.

JFQ: *Cyberspace is now a growing security industry dedicated to find and neutralize state and private cyber attackers and tools. How is this affecting military operations? Is your command able to deal with the weaponization of information? How does that fit in the more conventional military role of operations?*

General Nakasone: The National Defense Strategy outlines that partnerships are one of the three key elements we must possess to compliment and enhance our warfighting capabilities. Partnerships are fundamentally something that we must do in cyberspace. In fact, one of our priorities is to build strong, reliable, and resilient partnerships because this is a domain where 90 percent of the networks—the critical infrastructure—resides in the private sector, not in the public. This is primarily a private industry-driven domain.

Think of the antivirus community and how it has grown in the last few years. What do they have? They have global presence, and the ability to collect an enormous amount of information. They have strong analytic capabilities. The products they produce often rival what we see being done by the Intelligence Community. These partnerships—and particularly with private industry—are

Cyber warfare operators serving with 175th Cyberspace Operations Group of Maryland Air National Guard monitor cyber attacks on operations floor of 275th Cyber Operations Squadron known as Hunter's Den, December 2, 2017 (U.S. Air Force/J.M. Eddins, Jr.)

critical for what we're doing in cyberspace today. We have a number of different initiatives that are reaching out to the private sector because we know that a lot of the cutting-edge technology that's being used today in cyberspace resides within private industry.

JFQ: *How difficult is it for the military to compete with the private sector?*

General Nakasone: This is a common question—a good question given the competition for talent across government, private industry, and acadamia. We think of this competition across the recruitment, training, and retention of a force. In recruitment, the Services do a tremenous job of attracting young men and women to join our teams. Why do the Services get top talent? Because young people want to join and do this type of work. Second, we have a strong training program. In fact, it is so good that not only do we train them, but we also have the opportunity to earmark those who are the top talents. Once we have earmarked the top talent, then the question becomes, "How do we retain them?" The retention problem is not a macro problem—we have proved we can retain the overall numbers of Servicemembers to maintain our force. The challenge is ensuring we retain our very best. Those very best are often exponentially better than their peers—10 or 20 times better. They're coders, they're forensic and malware analysts, they're developers, they're operators who are *x* times better than those to their left or right. Those are the folks we must ensure we retain. They are the ones we are in fierce competition to keep.

JFQ: *You've spoken in other forums about the concept of "persistent engagement" and even mentioned it earlier. In relation to your mission, can you describe what you mean by that phrase and how it relates to the National Defense Strategy?*

General Nakasone: *Persistent engagement* is the concept that states we are in constant contact with our adversaries in cyberspace, and success is determined by how we *enable* and *act*. In persistent engagement, we *enable* other interagency partners. Whether it's the FBI or DHS, we enable them with information or intelligence to share with elements of the CIKR [critical infrastructure and key resources] or with select private-sector companies. The recent midterm elections is an example of how we enabled our partners. As part of the Russia Small Group, USCYBERCOM and the National Security Agency [NSA] enabled the FBI and DHS to prevent interference and influence operations aimed at our political processes. Enabling our partners is two-thirds of persistent engagement. The other third rests with our ability to act—that is, how we act against our adversaries

in cyberspace. Acting includes defending forward. How do we warn, how do we influence our adversaries, how do we position ourselves in case we have to achieve outcomes in the future? Acting is the concept of operating outside our borders, being outside our networks, to ensure that we understand what our adversaries are doing. If we find ourselves defending inside our own networks, we have lost the initiative and the advantage.

JFQ: *When I was interviewing Admiral* [Michael] *Rogers, he was in the process of building teams to stand in the early days of cyber. How is your progress in getting to where you want to be to have all your teams in place to accomplish your mission?*

General Nakasone: One hundred thirty-three teams are built and trained to a joint standard, and that is complete. Our focus has gone from building teams to making sure they're *ready* teams, making sure the teams, whether offensive or defensive, have the capabilities, have the manning, have the tradecraft, have the experience to conduct the missions that I talked about earlier. It's our primary focus. One of the things that we have going for us is that we have some pretty active adversaries. Whether it's countering adversaries who are trying to impact our elections; whether it's opposing adversaries in places such as Iraq, Syria, Yemen, or Afghanistan; or whether it's working to ensure that our defensive teams are assisting in the protection of our weapon systems—we are ready.

JFQ: *U.S. Cyber Command is a relatively new organization, even in its recent elevation to command status. How have the capacity and capability of the command grown over time to meet your missions? Has jointness been a benefit to how the command operates?*

General Nakasone: Jointness has been a tremendous benefit to our cyber mission forces. In the early days of USCYBERCOM, the leaders decided on an important point: there would be only one training standard, a joint training standard determined by USCYBERCOM. That's helpful for any commander who gets a Marine team, Army team, Navy team, or Air Force team and knows that whatever Service team he receives, missions will be executed to a single joint standard. We have a number of different missions with a number of different elements, so jointness is essential for us.

Looking back on the development of the force, there's been a series of different acts in the history of the command. Act 1, was standing up the command in May of 2010. Act 2, in 2012–2013, was the decision by DOD to build 133 teams—6,187 people (both military and civilian)—for 4 years in order to build capacity and capability across this command. Act 3 was the employment of these teams, both with Joint Task Force Ares, focused on the defeat of the [so-called Islamic State] in virtual space, and the recent Russia Small Group, which was a USCYBERCOM/NSA partnership to assist in the securing of the 2018 midterm elections. Across all these activites or acts, the concept of jointness has been fundamental to our thinking and our success.

JFQ: *How do you leverage partnerships at home, and internationally, to the command's benefit? What is your relationship to the various other places you may have forces, or how are you related to other commands globally?*

General Nakasone: When we take a look at our partnerships with other commands, we begin with geographic combatant commands. These are easy partnerships that we formed immediately. There's a known threat: there are known challenges to their networks, data, and the way they do business. We have also been the beneficiary of the DOD desire to stand up cyberspace operationally integrated planning elements. These elements are personnel who have cyber experience, who have gone to the commands to work within the J3 and J5 shops to provide the planning and subject matter expertise that was necessary. Moreover, we've been the beneficiary of ongoing operations in northern Iraq, Syria, Afghanistan, the Philippines, and Yemen to perfect a lot of our tradecraft with these supported commands. Then there are the functional or global commands. I appreciate both U.S. Special Operations and U.S. Strategic commands for pulling USCYBERCOM in and saying, "We are global commands, we need to think about this differently. We have shared areas that we have an ability to provide greater support to the Nation." That's appreciation for access and appreciation for a wide range of options. These are things that we among the [global commands] started talking about, and I think this would be among the big steps that USCYBERCOM and other commands will be able to offer the Nation in the years to come.

JFQ: *As these threats and responses evolve, what is your view of the long-term conflict in cyberspace? What changes in operational structures and technology do you think are necessary?*

General Nakasone: As we look to the future of competition in cyberspace, one idea comes to mind. The concept of persistent engagement has to be teamed with "persistent presence" and "persistent innovation." Persistent presence is what the Intelligence Community is able to provide us to better understand and track our adversaries in cyberspace. The other piece is persistent innovation. In the last couple of years, we have learned that capabilities rapidly change; accesses are tenuous; and tools, techniques, and tradecraft must evolve to keep pace with our adversaries. We rely on operational structures that are enabled with the rapid development of capabilities. Let me offer an example regarding the need for rapid change in technologies. Compare the air and cyberspace domains. Weapons like JDAMs [Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When

More than 800 Servicemembers and civilians enhance readiness during Exercise Cyber Shield 18 at Camp Atterbury, Indiana, May 2018 (Indiana National Guard/Jeremiah Runser)

we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict. Thus, we will need formations that have ready access to developers. Also, developers who understand how to complement the work of our operators in a rapid, agile manner.

JFQ: *I imagine your loop for acquisition has to be almost infinitely fast, lightspeed somewhat, say, compared to trying to develop an F-35 or some other kind of conventional or traditional system.*

General Nakasone: We have created programs for building capabilities in cyberspace. However, to your point, one of the very helpful things is that we have some acquisition authorities, and we have acquisition money that we are able to touch, so we've started doing that. The construct of operating and rapidly developing in tandem within this domain is one of the areas that makes this domain unique. Operators must work closely with developers, and the developers must work in partnership with our operators.

JFQ: *Obviously when U.S. Special Operations Command* [USSOCOM] *was set up under Goldwater-Nichols, it got a certain chunk of authority under Title 10 that the other commands do not have. In the future, do you foresee a need for asking for that kind of capability for U.S. Cyber Command since you're somewhat different than the other kinds of commands?*

General Nakasone: We are still at the point of building our infrastructure and capabilities and the development of networks, but once that's done, I think we will look for increased USSOCOM-like authorities. What underwrites success in cyberspace is the need for speed and agility. This will likely lead us to evaluate those authorities—whether it is in acquisition, joint force training, or joint force provision—that ensure we can operate rapidly with unmatched lethality.

JFQ: *What is artificial intelligence* [AI] *and what does it mean for the future of conflict in general and for the future of cyber security in particular?*

General Nakasone: When we talk about cyberspace, I think that the early instantiation of AI will be on the defensive side. We are experimenting and developing "self-healing networks," where we see a vulnerability and the vulnerability is recognized rapidly and patched or mitigated.

Yet AI will likely be part of future offensive capabilities as well. Currently, access development is our most time-consuming and difficult element of developing offensive options. I suspect that AI will play a future role in helping us discern vulernabilities quicker and allow us to focus on options that will have a higher likelihood of success.

JFQ: *I'll leave you some space for things that you think we may have not covered here and that you think are important to talk about. We touched just briefly on jointness. How have you seen jointness come to develop itself and where do you see it going from here? Not necessarily specific to U.S. Cyber Command, but as a member of the elite within the joint world, what does jointness mean to you as a commander?*

General Nakasone: I was commissioned in 1986, so my experience with jointness has taken place over the last 20 years. I have seen first hand the advantages of joint formations—whether it's been in combat or stateside. I operate comfortably within the joint world given several tours with the Joint Staff or within joint commands. It's natural for me to understand how to do joint planning processes. I believe USCYBERCOM has benefited tremendously from a joint construct. We operate as a joint force *habitually.* We will be even more joint in the coming 5 years given the power of being able to bring a "best athlete" approach across the Services to a problem. When we evaluate problems, we do see specific Service advantages, but that advantage has to be teamed with capability and capacity that other Services can offer. I see bringing our best operators, developers, and analysts across Services to solve tough problems as a large part of what the future is going to hold for us. We will always have Service equities in terms of what we're going to defend and be able to do, but increasingly our networks will be joint. Our training is moving much more toward a joint flavor than a specific Service flavor. USCYBERCOM in many ways will be at the cutting edge of this new and important movement toward jointness.

Venetian resort hotel casino, owned by Las Vegas Sands Corporation, was hit by Iranian cyber attack in February 2014 (Courtesy Bert Kaufmann)

JFQ: *Your teams are made up just as Service teams, or . . . ?*

General Nakasone: The Services man, train, and equip our teams, but we operate regularly as part of joint task forces. This includes our major operations supporting the defeat [so-called Islamic State] campaign and the recent efforts to secure the midterm elections.

JFQ: *What is your greatest challenge?*

General Nakasone: Our greatest challenge—also our greatest opportunity—is recruiting, training, and retaining a world-class force. The Services continue to recruit high-caliber military and civilian personnel to man our force. We have developed a training pipeline that trains all to a common, joint standard. Our retention of top talent is a critical component of future success. We track this closely and work with the Services to identify opporutnities to improve retention. We must continue to build our recruiting and training successes along with a strong focus on ensuring we retain our best military and civilian personnel. The competition for talent is not getting any easier.

JFQ: *Thank you so much for your time.*

General Nakasone: Let me add one final point. We have a tremendous amount of momentum to build on in the coming months. The guidance resident in the National Security Strategy, National Defense Strategy, National Intelligence Strategy, National Military Strategy, National Cyber Strategy, DOD Cyber Strategy, and DOD Cyber Posture Review give us a clear vector to move us forward. This, coupled with clear policy guidance and the 2019 National Defense Authorization Act, ensure USCYBERCOM can operate at the speed of relevance to effectively accomplish its mission and bring greater capacity and capabilities to DOD and the Nation. **JFQ**