



SENIOR LEADER PERSPECTIVE: GENERAL GENE RENUART

NSCI's Lindsay Trimble recently interviewed General Gene Renuart, commander of the North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM), headquartered at Peterson Air Force Base, Colo. He entered the U.S. Air Force in 1971 and was commissioned through the Officer Training School in 1972. Renuart assumed command of NORAD and USNORTHCOM in 2007.

NSCI: USNORTHCOM's mission is to "anticipate and conduct Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect and secure the United States." How has the increase in cyberspace operations affected this mission? How has your organization adjusted its defense systems to include monitoring for potential cyber attacks?



GENERAL GENE RENUART: We are constantly taking actions to protect our networks by applying anti-virus and software updates to reduce network vulnerabilities, increasing network monitoring and expanding information sharing with US-CERT [U.S. Computer Emergency Readiness Team] and coalition partners. Clearly more needs to be done within the government and private sectors to ensure uninterrupted access to our critical network infrastructure, such as nationwide implementation of smart sensors that can quickly identify and stop malicious cyber activity; and real-time nationwide cyber common operational picture that will enhance situational awareness and decision-making.

Also, malicious cyber activity across the public and private sectors has pushed USNORTHCOM to explore and codify its role in providing cyber support to civil authorities. We are working with DHS and other stakeholders to characterize possible and probable cyber assistance requests in the event of a national cyber incident.

Over the past year, NORAD and USNORTHCOM have made a number of adjustments to improve the defense of our networks. Within the headquarters, we established a robust 24/7 Network Operations and Security Center (NOSC). This NOSC works with our network maintainers, subordinates, components and other DoD [Department of Defense] entities to keep open our lines of communication with our NORAD partners and all of our USNORTHCOM Interagency partners. Our Cyber Domain Watch Officers provide leadership the required awareness of "the good, the bad and the ugly" activities occurring both within our headquarters' networks and within the area of operations/area of responsibility. We are also expanding our relationship with DHS [Department of Homeland Security] to improve our situational awareness and understanding of their unique cyber requirements.



Keeping Cyberspace Professionals Informed

NSCI: When you say “clearly more needs to be done,” do you mean efforts are in progress or NORTHCOM would do more if it had the funding and manning?

RENUART: Certainly, funding and manning will always allow you to be more active in any area, but I want to be careful not to say “we are not able to be successful because we’re limited in that regard.” It’s important to understand that in most areas, we’re not an initiator, but we’re a consumer of the capabilities that really reside and exist in other areas and other organizations. USSTRATCOM is really the principle player for the Department of Defense. DHS is the principle player for the whole of government and then there are a number of private sector areas involved in this that we don’t drive or fund, and yet we’re very much dependent upon their support.

When I say “clearly more can be done,” it’s really gathering the various partners to work on a progressively-tougher set of questions. I’m pretty comfortable where we are. We can always use more money and more people, but it would really be to help us continue to partner with STRATCOM and DHS, in particular, and really expand into the private sector over the coming days and months to create common cyber defense capabilities that reduce vulnerabilities in both the classified and unclassified networks we use.

NSCI: Would you tell me a little about the cyber arrangements and authorities between USSTRATCOM, USNORTHCOM and the DHS?

RENUART: Within our area of responsibility, USNORTHCOM – along with USSTRATCOM and DHS – have teamed to shape the cyber security efforts by improving information exchange and expanding relationships with the government and private sector cyber community of interest.

USNORTHCOM has the specific responsibility for Defense Support of Civil Authorities (DSCA) and Homeland Defense (HD) within the continental United States. Regarding DSCA, the DHS has outlined key cyber responsibilities for the DoD in the National Response Framework, Cyber Incident Annex. These responsibilities are shared between USNORTHCOM, USSTRATCOM, USCYBERCOM and the DoD’s intelligence and law enforcement organizations.

USNORTHCOM leverages the cyber capabilities within DoD through USSTRATCOM in executing its DSCA and HD cyber responsibilities. The standup of USCYBERCOM under USSTRATCOM will not change this arrangement. We regularly meet with DHS and USSTRATCOM to discuss current cyber activities and efforts to enhance future mutual support.

Our cyber authorities are derived from a number of sources. The Unified Command Plan assigns DSCA and HD to USNORTHCOM. The National Response Framework established the whole of government, all hazard response construct. HSPD-5 [Homeland Security Presidential Directive] Management of Domestic Incidents establishes a single, comprehensive approach to domestic incident management. HSPD-7 Critical Infrastructure Identification, Prioritization and Protection details the approach to protecting the Defense Industrial Base. HSPD-8 National Preparedness is the foundational document for



prevention and response to threatened or actual domestic terrorist attacks, major disasters and other emergencies.

NSCI: To illustrate these relationships, can you summarize the sequence of events and agency involvement if a government or military network were to experience a major cyber attack?

RENUART: First, I'd like to hope that we've developed these relationships in a way that if NORTHCOM suddenly discovered an intrusion or a vulnerability that was being exploited, then nobody else would know that. As we've networked together in operations and security functions, I would hope that within the STRATCOM structure and the Cyber Command structure, we hear information on our networks in real-time. The alert giving us word of this intrusion might well come through one of them to us before it actually gets into our enterprise. But we do have the ability to detect and determine threats immediately if they come to us; we don't know if anyone else is aware, we make them aware and we make the folks at STRATCOM aware of this issue. Sometimes, it might come to us through a Service enterprise, and then we would collaborate immediately with the Services.

It's a collaborative process, and I think we're at a point now, where we all know around the same time – or pretty close, in real-time – so that it's not a command-and-control process. Some of the fixes to those intrusions may be better initiated at a more global level. So, DISA or JTF – Global Network Operations will initiate those efforts on behalf of the many other users that may be affected. But we also do have the ability to do some self-protection of our own enterprise within the command.

It's cumbersome to describe it as a chain of command because it really is an interactive environment where most of the players are in that space simultaneously, especially within DoD.

NSCI: From a USNORTHCOM perspective, can you discuss a few of the key challenges regarding cyberspace operations?

RENUART: Our mission partners transcend traditional military coalitions, thus our cyber interests expand well beyond DoD networks. As such, NORAD and USNORTHCOM view our access to the Global Information Grid and the broader Internet as critical to successful homeland defense and civil support missions.

Key challenges for NORAD and USNORTHCOM include a secure, available, interoperable and reliable cyber environment that will enable us to effectively execute our missions. To address these shortfalls, we require improved cyber situational awareness and defense tools, improved training for cyber professionals and interoperable standards with our DoD and non-DoD mission partners.

USNORTHCOM is the single entry point for all DSCA missions to include cyber. This construct simplifies requests for assistance from civil authorities and ensures unity of effort for DSCA operations.



Keeping Cyberspace Professionals Informed

The bottom line is that USNORTHCOM, USTRATCOM, USCYBERCOM, DHS and the public and private sectors must do everything we can to build resiliency and redundancy in our networks to assure successful execution of our homeland defense and civil support missions.

NSCI: You mentioned the need for improved training of cyber professionals – a topic that comes up often in this growing field. Does the technical nature of cyber defense ever make it difficult for NORTHCOM and its partners to acquire the resources and training they need from lawmakers?

RENUART: We tend to approach network security/cyber security in “islands” – that’s my way to describe this. We let Service network operations and security centers deal with their networks. We do this, not quite in isolation, but as more discreet entities. As a result of that, we didn’t really create a common training construct among all of the Services and, increasingly, among other government organizations to be able to operate.

This network – this enterprise that we live in – is all-inclusive and simultaneous across a variety of spectrums and in what I would call “network speeds.” We’ve had to adjust and improve the training programs. For example, the Navy has kind of become the lead agency to provide more aggressive training for cyber professionals and the Services are all beginning to pile onto that. But it is a capacity problem; you can only go so fast and training someone to be a systems administrator is very different from training someone who can operate in a defensive environment in cyberspace – where the threats, attacks or intrusions can come from a whole variety of different arenas. We’re growing in that capacity and we need to continue to do that. As Cyber Command comes aboard, they will begin to drive those key elements of training that all of the Services will be compliant with. It’s going to take us a little while to increase sheer capacity in this area.

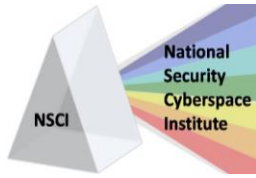
NSCI: How will that affect the overall budget?

RENUART: I think that General Chilton is pretty comfortable with the current budget projections that we have. We have sufficient funding to continue, maintain and sustain those training programs. I think that the cyber arena is one where the more you learn, the more you figure out there’s more to learn. This is going to be a living, breathing environment that we’re going to have to operate in and extend our capacity over time. I’m not sure we yet know all that we need to know. At just about the time you think you’ve defended an enterprise, some other vulnerability may pop its way in.

NSCI: You’ve been commander for USNORTHCOM and NORAD for more than two years now. Have there been any specific cyber successes since 2007 that you’d like to highlight?

RENUART: Yes, one aspect we’ve been successful in is our work in providing fidelity for cyber support to DHS and other government agencies to mitigate the impact of cyber incidents.

NORAD and USNORTHCOM also sponsored cyber-specific exercises that have improved relationships with DoD and non-DoD cyber mission partners. These exercises are intentionally designed to “stress the system” by challenging our equipment, tactics and personnel.



Finally, the establishment of a robust 24/7 Network Operations and Security Center has enhanced our situational awareness and response to malicious cyber activity that could adversely affect our operations.

NSCI: Is it ever difficult to quantify success in this field because “no news (successful attacks) is good news?”

RENUART: Success comes in a variety of areas. I think we can quantify the success as we defend our enterprise against specific intrusions: you see that you’ve identified it, you’ve defended against it, you’ve negated it, you’ve ensured that it can’t come back to some degree. But I think the pervasive nature of cyber is that it can move from one target to another pretty quickly, so you may not necessarily know that you’ve solved a problem for a bit longer.

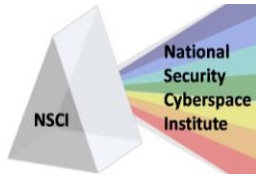
You made the comment that “no news is good news.” I guess we don’t have publicity for the successes, but on the other hand, some of the threats we see are designed to lay dormant and only become a threat later on down the road. So we shouldn’t say “Nothing’s happened, so we must be doing great.” In fact, you can make the case that if nothing’s happening, you should be suspicious because the intent of those that would manipulate the networks or enterprises continues to remain constant. It’s born out of the intelligence we see; it’s born out of the fact that young kids are trying to get smarter with computers and do cute things every day. That intrusion intent is present in a variety of different areas. I would suspect that even industrial competition drives a certain amount of intrusion into networks for a competitive edge. So we ought not to assume that “no news is good news.” We ought to assume that if we’re not seeing something, somebody may be figuring out a better way to get access and we need to dive deeper.

NSCI: USNORTHCOM and NORAD recently held the Ardent Sentry 2009 exercise in various sites across the country. Did this exercise incorporate cyber defensive and/or offensive tactics?

RENUART: We incorporated numerous cyber defensive tactics that exposed areas where we need improvement, but also brought to light areas where we’ve made significant progress due to our investments in technology, training and people.

NSCI: Did the exercise provide any insight and/or lessons learned you’ve been able to leverage in support of USNORTHCOM cyberspace operations?

RENUART: Yes it did. Without going into specific details, there were several lessons and insights we’ve taken for action. The staff, particularly the J6, is currently working on the results that will enhance our cyber security posture.



NSCI: You mentioned that NORTHCOM has sponsored cyber-specific exercises. Would you tell us a little about that?

RENUART: USNORTHCOM participated in the Cyber Storm exercises, hosted by DHS. We look forward to the opportunity to work with DHS in the next Cyber Storm. Further, we routinely participate in USSTRATCOM-sponsored exercises. Finally, we've held several internal table-top exercises exploring various cyber scenarios and greatly increased cyber activity in all exercises.

In addition to robust cyber elements in our exercise program, we've allowed the J6 to conduct spear phishing exercises within the headquarters that directs "offenders" to phishing-specific training. We've also conducted mandatory cyber security training and awareness sessions for all personnel.

NSCI: What opportunities do you see for other collaborative projects with defense organizations and/or industry partners?

RENUART: NORAD and USNORTHCOM partner with Allies; Federal, State, local and tribal governments; and the private sector to reduce cyber vulnerabilities and defend against infrastructure attacks.

DHS is giving USNORTHCOM the opportunity to take part in developing their first Quadrennial Homeland Security Review. This provides an additional venue for us to further refine our role in providing cyber assistance to DHS.

Other collaborative projects include ongoing development of the DHS-led National Cyber Incident Response Plan which will enhance the nation's ability to respond to a national-level cyber incident with a whole-of-government approach. The stakeholders supporting this effort are government and non-government organizations.

NSCI: Has the multi-national partnership between the United States, Mexico and Canada enabled USNORTHCOM to have a broader perspective on the global effects of cyberspace?

RENUART: We are building a relationship with Canada Command and the Canadian Forces Network Operations Centre to facilitate information sharing of cyber-related information. This will enhance mutual situational awareness and offers the potential to synchronize cyber response to a major event.

Mexico and the U.S. have common security objectives that can be mutually supported through increased intelligence sharing, interoperability and collaboration. Recently, we had discussions with the Mexican military to develop interoperable communications solutions within the cyberspace domain.

NSCI: Is there anything else you'd like to add?

RENUART: USNORTHCOM experiences many of the same threats that non-DoD organizations address on a daily basis. To help mitigate these threats, more collaboration is needed between private and government sectors.



CyberPro

September 10, 2009

Keeping Cyberspace Professionals Informed

Recently there has been significant activity concerning cyberspace: the President's 60-Day Cyber Policy Review, the updating of the National Cyber Incident Response Plan and the stand up of USCYBERCOM. Given its Homeland Defense and Civil Support missions, USNORTHCOM – along with STRATCOM and USCYBERCOM – are prominent players in synchronizing and shaping DoD's role in securing our national interest in cyberspace.

Thank you for this opportunity to discuss USNORTHCOM's significant involvement in shaping the future of cyberspace activities both within DoD and with our external mission partners. NORAD and USNORTHCOM mission success is predicated on robust, reliable access to both classified and unclassified mission systems. Our efforts in the cyber domain, throughout the whole of government, are vital to ensure our homelands are defended, protected and secure.

H@cker | Halted TM **USA 2009** **Miami | Florida**
Sep 20 - 22 | Academy
Sep 23 - 25 | Conference

FREE TRAINING
Worth **\$599!***

Intriguing . Provocative . Informative

Get certified and obtain new technical skills.
Understand the state of information security.
Stay updated on latest threats and countermeasures.
Network with infosec professionals from around the world.
Be part of the world's largest reunion of Certified Ethical Hackers.

Bonus !

Register for the Conference, and attend one of three special one-day full fledged training workshops (Sep 25) led by EC-Council Master Instructors.
Identifying Threats & Deploying Countermeasures | Incident Response: Principles of Incident Handling | Virtualization: Threats Exposed.

Hackers Are Ready. Are you?

Register Now !

w w w . h a c k e r h a l t e d . c o m
*Terms & Conditions Apply