SENIOR LEADER PERSPECTIVE: DANIEL HINGTGEN

NSCI's Lindsay Trimble recently had the opportunity to interview Mr. Daniel Hingtgen, chief of Information Assurance (IA) Policy, Programs and Training for U.S. Army Europe (USAREUR). Previously, Hingtgen was active duty in the U.S. Army, retiring in 2004 as a sergeant major. During his career, he was a program manager for multiple Army training initiatives and IA policy development, including developing the Army in Europe IA policy for 65,000 information technology users. In this interview, Hingtgen discusses the ways that USAREUR has adapted to meet the new threats present in cyberspace.
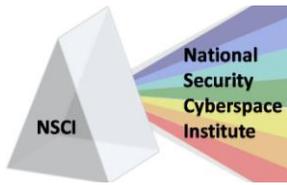
NSCI: What is U.S. Army Europe's relationship to other Department of Defense organizations supporting cyberspace operations?

DANIEL HINGTGEN: Our direct relationship is supporting Title X for Europe to support AFRICOM [U.S. African Command], EUCOM [U.S. European Command] and all subordinate tenants and major subordinate commands for the network connectivity. So we're the theater information grid, which is part of the global information grid. And of course owning it, managing it, safeguarding it and securing it are all critical and tied in. We have a lot of customers on our network that we rely on to ensure that they are doing their part to keep the network safe and that goes from the individual user being properly trained and certified to the computer user to the systems administrators and the enterprise administrators needing all the training and certification requirements for the Department of Defense as well as the Department of the Army.

My office focuses on the training and certification side for the AFRICOM and EUCOM workforce. The day-to-day operations are basically Army-run and owned. The people that I deal with for the Army in Europe's network (which covers Army in Europe's Area of Responsibility) are Army people – Department of Defense civilians, contractors and military members.

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

HINGTGEN: The most significant challenge is the constant bombardment of new information assurance vulnerability alerts, new directives, new challenges – both seen and unforeseen – that come down the pipe. These go beyond what you're doing in your normal duty day to safeguard security and making sure the information that meets our requirements and that people can trust it, but it's a very fluid environment with a very obvious threat from all sides. It's not just necessarily the wire threats, but also the physical possibilities of breaking into the network like someone walking into a building and gaining access. The challenges that are in the cyber world for corporate America or Britain or France are pretty

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 1**

much the same. We're strictly DoD, so we're a little bit more attuned to ensuring that the information is what it is and is not changed – that it's secure, available and that there's no question of integrity.

NSCI: How have these challenges evolved during your time at USAREUR – active duty and now?

HINGTGEN: There have been significant changes! When I did automation for the U.S. Army back in the 82nd Airborne Division, we had semi-vans with mainframe computers in them and security was not an issue on anything because we owned and operated our own network. Now, with the networking and being plugged into the world, there are significant challenges that go with that. It's been astronomical the changes that I've had the opportunity to experience in the automation and communication arena. It's pretty evident for high school and college students now – the way they grew up –my granddaughter is already using a computer, and I didn't use a computer until I was almost 25 years old! There have been significant changes – both good and bad.
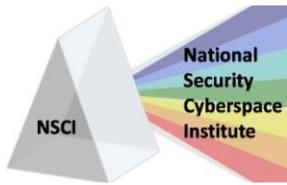
NSCI: How has USAREUR adapted to meet the new threats present in cyberspace?

HINGTGEN: We're constantly evolving and staying current with all of the directives that come from our higher-ups, trying to put in safeguards that are unique to Army in Europe that aren't necessarily happening in the continental United States. We have a significant amount of different posts, camps and stations – called a Kaserne over here – scattered throughout Europe, so we're not on a closed facility like a Fort Bragg or Fort Hood with all of us in one physical boundary. We're scattered and depend on the fiber and commercial networks to allow a lot of our traffic to pass through. We're just about there in completing our facility upgrades.

Another significant change is that – not that we have an undisciplined workforce – but we have a workforce that is using the company or government-supplied computer access to go and do different things on the Internet. This is also true in the corporate world and in the other military branches and government. If you get a good percentage of your employees doing that – whether it's for a few minutes a day or a considerable amount of time – it's taking away bandwidth that is supposed to be dedicated to the mission. That's a challenge everywhere. We've done studies and we've gotten a lot better because we've gotten people to understand that we are monitoring their actions on the Internet and on the network. Another action that has helped is that our users are trained and certified as computer users to know their specific roles and responsibilities.

NSCI: Many senior leaders have commented that trained cyber warriors are one of the most significant shortfalls we have right now. As the lead for Information Assurance Policy, Programs and Training, what programs have you initiated to prepare USAREUR soldiers for the fight in cyberspace?

HINGTGEN: The foundation for what we do is the policy and the law – the Federal Information Security Management Act (FISMA) and other directives. So what we have here in Army Europe is a dedicated training and certification program which is commercial certification for our elevated privileged users, such as our systems administrators, organizational unit administrators and our enterprise administrators. At different levels, depending on what they do on the network, we have the appropriate level of blended training – done online, prior with prerequisites and instructor-led training – which

110 Royal Aberdeen ⚫ Smithfield, VA 23430 ⚫ ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 2**

culminates in a commercial certification test to show that they are certified and that they have gained the knowledge needed in those positions. That's a DoD 8570 regulation, so we have all of the training in place to accomplish that.

We also do a lot of other training and certification for the Army in Europe workforce, which includes AFRICOM and EUCOM, and USAFE [U.S. Air Forces in Europe] if they want to buy-in to our program. We do project management, enterprise project management, enterprise architecture and information technology infrastructure library (ITIL). Not only do people have to attend to keep their positions, but we also allow for continued growth in the IT arena to become more professional and competent in your duty roles and responsibilities to safeguard and secure the network – both as a systems administrator or as a project lead for a group of systems administrators working a project.

Again, it's the policy that sets the foundation of what we need to do, why we need to do it, and where we need to focus our training energy and dollars to train and certify that set workforce. It's a combination of all three and then you tie in the IA programs already established in the Department of Defense and in the Department of the Army. Those are umbrellas over what we're trying to do. We use those systems to facilitate the success down here on the ground, for example the Army Portfolio Management Solution system, which helps with the management and day-to-day operations of our certification and accreditation actions of those systems on our network. We use that system for the recording, tracking, managing and moderating.

NSCI: How has this training improved cyber capabilities?

HINGTGEN: From my experience, it is a significant challenge to keep IT people in that set job because if someone is a systems administrator working here on an exchange server, but there's a staff position across the street with a promotion for their career field, people want to go for a promotion and better themselves – not only for the money, but for growth and professional development. They leave the technical arena and go for staff or management-type positions, and it can be a big hindrance to the IT team for those very competent and well-trained technicians to move into other positions. Before NSPS, the 2210s received additional money based on the fact that you were a technician. That takes the good people away. I'm not saying that more good people don't fall in behind them, but you can't replace somebody overnight that will fully understand the theater and network as well as the relevance for the role they have.

NSCI: What do you see as the next steps to providing the quality and quantity of cyber warriors senior leaders are asking for?

HINGTGEN: All the services have gotten smart enough to try to consolidate resources, servers and enterprise-type environments (versus a distributed environment like before). So we're consolidating and bringing things in and taking back the control of managing and operating the entire network. In my opinion, I believe that the end-state would be where the Department of Defense's DISA – Defense Information Security Agency – is the backbone and everyone rides off of one enterprise network. So all of our IT professionals are support staff to one enterprise, instead of having just the Air Force enterprise or the Army enterprise. We'd all be tied together and could use each other's resources and share the
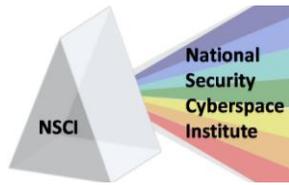
battle space for situational awareness. We're trying to get there and are making headway, but I believe that that would be the most significant thing that the Department of Defense could do to get all the IT cyber warriors working in the same direction for the same network. We have the theater information grid here in Army Europe, which is part of the global information grid. We should all be working in the same channel. And that may be the goal of the new cyber command that they are standing up. I believe that's where we need to head.

People become fearful of change and they get fearful of losing their jobs, but change and moving in the right direction leads to opportunity. The cyber warrior's goal is to ensure that the network stays available; that the information going back and forth has integrity, is sound, trustworthy and available 24/7; and that the network is fully supporting the mission requirement and its people are responsible for what they're saying on there…The synergy would be phenomenal.

NSCI: There has been a lot of discussion recently about the need to prioritize network defense efforts using a risk-based approach – we can't afford to protect everything to the same degree all the time, and not everything is equal in terms of mission assurance. What is USAREUR doing in this area?
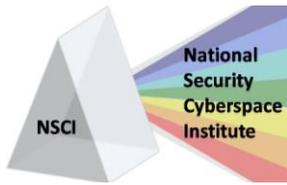
HINGTGEN: The priorities can come based on the threat. The threat is always there, but if something new comes up, of course the priority changes. For Army in Europe, the priority at the moment – as it is for the rest of the Army – is the deployment of data at rest, or mobile armor: products that we're implementing across Army Europe that will encrypt the information on your hard drive so that should your laptop or device be stolen, the personal identifiable information we don't want others to see cannot be easily looked at… That is a major initiative that is ongoing along with our pilots that we're doing for the FY10 Crypto-Modernization Program to upgrade all of our cryptographic-type devices throughout the network along with what we're trying to do with our network access control. There are a lot of major programs that are being pushed at the top as well as things we're doing at our own level, but they're all tied together. They all have different timelines and priorities.

The issue is things are changing at the same time you're implementing other changes. You might be going down one road and you might need to veer off and take a left turn because that has changed now and you think "let's go this way." That's a constant challenge also.

NSCI: What kinds of opportunities do you see for interaction with industry partners in training for cyber defense and offense?

HINGTGEN: Industry partners have a select role and we certainly need to work hand-in-hand with our industry partners because they're the ones that develop the products based on our requirements. ….It's industry that is the one that will facilitate meeting the requirements that we have. The UAV being able to communicate from CONUS when it's flying over Afghanistan is a perfect example of this because it's a

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 4**

wireless network, through satellite, down to a guy with headphones sitting in Colorado. It shows you the power of the wired and the wireless networks and the communications. I think that's one of the goals to have that same level of confidence in communication down to the soldier in a foxhole. If you're sitting in the Pentagon and want to talk to a soldier in a foxhole, you have the ability to reach out and "touch" him. That's where I think we're going. That takes a lot of smart people from industry to develop those types of products.

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

HINGTGEN: I believe that Army in Europe has the best training and certification. We have been recognized for it DoD-wide. Again, I've got to go back to my point about the policy setting the standards for us to follow, but having the resources, the people on the ground and the leadership support to make whatever program happen is essential. And based on the things that are going on in the world and now with President Obama's cyber command, the visibility of leaders at all levels is much better now than it has been in the past on the importance and how much we rely on IT.

There are some great videos out there – "What if" videos – asking "What if certain things happened?" It's scary how much we depend on our IT, our computers and our servers to manage, run and operate on a daily basis. What would you do if they were compromised and taken out of the net? It's a serious threat and it can have serious ramifications for people and lives. My hat's off to the president for moving forward with the cyber command.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 5**