David Gioe

Today is December 18, 2014, and we are here at the West Point Center for Oral History with Colonel Greg Conti. Welcome, sir.

COL Greg Conti

Itâ€™s my pleasure to be here.

David Gioe

Before we get started, can you please spell your last name for the transcriber?

COL Greg Conti

C-O-N as in November, T-I.

David Gioe

Thank you very much. Well, letâ€™s start at the beginning. Can you tell us something about yourself, where youâ€™re from?

COL Greg Conti

Well, I grew up in the Hudson Valley, so West Point was always looming large on the Hudson River, and Iâ€™d say I consider myself a hacker of the old school, going way back. And for the record, I would say I use that term not as a malicious hacker that breaks into things, but someone who likes exploring technology and pushing it in directions the designer did not intend.

David Gioe

And can you tell us your current assignment right now?

COL Greg Conti

Currently Iâ€™m Director of the Army Cyber Institute at West Point, which is a new entity that was created about two and a half years ago by the Chief of Staff of the Army,

COL Greg Conti

the Secretary of the Army, and Commander, U.S. Cyber Command, and Commander, U.S. Army Cyber Command.

David Gioe

With that as our end state, letâ€™s work backwardsâ€”

COL Greg Conti

Okay.

David Gioe

A little bit, and start from a younger Colonel Conti, growing up in the Hudson Valley. What year did you graduate from West Point?

COL Greg Conti

I graduated in 1989, studied computer science. And what I find interesting is my class, â€˜89, is the last class to not be issued computers, so it was the class of â€˜90 that was first issued computers. They were Zenith 248s, 8286s, I believe, and what I would do as a cadet, because I didnâ€™t have a computer and I was a computer science major, there were plentyâ€”this was a newfangled technology at the time. Many people didnâ€™t use their computers.

COL Greg Conti

So I would rent one from a class of â€˜90 person for $50.00 a year or something.

COL Greg Conti

And as it turns out, we would later find out, Mooreâ€™s Law, that renting a computer for a couple of years, a $2,000.00 computer for $50.00 a year until it was no longer useful anymore. For the three years it was quite helpful.

David Gioe

Youâ€™ve used Mooreâ€™s Law in other contexts. I wonder if you can just take a second and define what Mooreâ€™s Law is.

COL Greg Conti

So Mooreâ€™s Law is the general idea that the density of transistors on a computer chip doubles every roughly 18 to 24 months. And itâ€™s held since the 1960s, and really had been an indicator of increases in computing power over that time, and what computers have been able to do. So basically it means that every 18 months or so you have a doubling capacity of what computers can do.

COL Greg Conti

And oftentimes, a halving in the cost, so itâ€™s fueling exponential growth, although currently weâ€™re feeling like weâ€™re getting at the end of the run of Mooreâ€™s Law.

COL Greg Conti

Although that might change if thereâ€™s a new technology that can take it further, which has historically happened.

David Gioe

Speaking of historical events, for instance, West Point did not have an information technology major until relatively recently, although it did have a computer science major even going back to the â€™80s. Was that something that was relatively new, or was that something that was established by the time that you became a Cadet?

COL Greg Conti

The computer science major? It was established. West Point transitioned from everyone receiving effectively a general engineering degree, which I believe class of â€˜86 or thereabouts was the last class, plus or minus, that did that. From that point forward, people could declare majors.

COL Greg Conti

I think that was a major step forward.

David Gioe

And reflecting on your time as a Cadet, the 47-month experience, with the benefit of a long Army career and successful career and hindsight, how did your time as a Cadet prepare you for your future responsibilities, either leadership or Officership?

COL Greg Conti

Well, I think the program here is actually very well thought out, and typically you donâ€™t necessarily appreciate it as a Cadet. Itâ€™s something that as you graduate you draw back on the lessons learned. Like layers of an onion, youâ€™re peeling layers back, and drawing more and more from that experience, everything from the courses youâ€™re taught, the lessons youâ€™re taught outside the classroom during the summers by your Tactical Officers, all of those things.

COL Greg Conti

And then later on, you find yourself drawing upon those, and even years later Iâ€™m finding that itâ€™s that network of contacts from that time.

COL Greg Conti

Years later, itâ€™s a strong bond, and it gives you people that you can reach out to, and help the Army move forward in a way that would be more difficult if you werenâ€™t connected that way.

David Gioe

Another sort of network.

COL Greg Conti

Itâ€™s another network, yes.

David Gioe

Your path from West Point to being the Director of the Army Cyber Institute has had a variety of different assignments. Can you take us through a couple that were particularly either meaningful for you, or significant in the development of your career?

COL Greg Conti

Sure. My first assignment was to Fort Stewart, Georgia, the 24th Infantry Division. I was there for six months. I branched Military Intelligence, and was there for six months.

COL Greg Conti

And Saddam Hussein invaded Kuwait, and we immediately deployed and went over. It was a very stressful time because he was poised, couldâ€™ve invaded Saudi Arabia. We were literally unloading tanks in the port. If he had decided to keep going south into Saudi Arabia with only the 82nd going against multiple Armored Divisions, it wouldâ€™ve been a battle for the history books, the fighting from the port.

COL Greg Conti

It was a very stressful time, but it was a condensed learning experience that seven months I was in the combat zone pushed you in ways. You lived, breathed the Army in a way that you never get on a normal garrison schedule. From there, Iâ€™ve always beenâ€”like I said, Iâ€™ve always considered myself a hacker, and fascinated by technology and computing. I was always trying to steer towards that in my career. I had a break at the Advanced Courseâ€”which is now the Captains Career Courseâ€”that I wanted into this area as close as I could get.

COL Greg Conti

I was able to get into a program called National Systems Development Program, which allowed me to get to Fort Meade and study signals intelligence in depth. I did a full set of assignments there. Itâ€™s kind of a closed community, so once I was in, I really felt like I had found an area where I could really contribute and what I could do would be appreciated. And that led to a next assignment, which was Company Command and Deputy Division Chief at another place in England, so it was a really nice follow-on.

COL Greg Conti

Iâ€™d always wanted to come back here to West Point because this is one of the few places, at least at the time, in the Army where you could do what is not being called Cyber. I had started a Masterâ€™s at night at Johns Hopkins. The Army let me spend a year finishing it up full-time, and then came and served on the faculty at West Point.

COL Greg Conti

At that point I ran into Dan Ragsdale, who was running the Information Technology and Operations Center, and really laid the groundwork for the Information Security Program we have today. He inspired me, rolled me into his efforts.

COL Greg Conti

I went to DEFCON, which was a hacker conference in Las Vegasâ€”really a game-changing experience for me. I really liked what I was doing. Applied to come back, and was accepted to go get a PhD. I went to Georgia Tech, which has a real solid information security program, and then applied for a permanent position called Academy Professorâ€”allows us to stay here for long-term. Upon return, I went to quickly became director of the ITOC, which became the Cyber Research Center, which is focused on information security, and led that from 2007 till 2014, just a couple months ago.

COL Greg Conti

And then finally in 2012, we were minding our own business, and we received a note that came down from the Chief of Staff of the Army, and I was informed by General Trainorâ€”we were in the libraryâ€”had me sit down, and said, â€œOkay, the Chief of Staff of the Army wants to create the Army Cyber Institute at West Point.â€ And I was charged with doing that, and EECS and I helped incubate it since June of 2012. It was dual-hatted as CRC Director and ITOC Directorâ€”Iâ€™m sorry, CRC Director and Army Cyber Institute Director, and then transitioned to full-time Army Cyber Institute Director late September 2014â€”so just a couple months ago.

David Gioe

It seems like everything has pushed you on this path, and the culmination is a very positive

one. You couldnâ€™t have seen that, of course, in 1989, where you mentioned that you branched Military Intelligence when it would have been possible to branch Signals as well.

David Gioe

Can you take us through that decision process?

COL Greg Conti

Well, at the time, youâ€™re making decisions based on a relatively small sampling of information as a Cadet, and oftentimes Cadets will have role models or mentors that they gravitate toward to make those decisions. At the time, I didnâ€™t even really know that Signal Corps was a place where you could do computing. I think that West Point does a better job of communicating that today, learning about the branches. Iâ€™d done a summer experience with the Air Defense Artillery and had a really positive time, and there was the Air Defense Artillery Officer here in the Department of Military Instruction was veryâ€”I really liked him.

COL Greg Conti

So I listed Military Intelligence, which I just thought would be the neatest thing to do, followed by Air Defense Artillery. And I believe Signal Corps was my third choice.

COL Greg Conti

I donâ€™t regret it. It turns out that the things that really attracted me to computing, the idea of information security was really vibrant in signals intelligence, and I was able to put those skills to work in places like NSA that wouldnâ€™t have been possible otherwise.

David Gioe

Can you describe in an unclassified way what you mean when you put skills to work?

COL Greg Conti

Well, I can say that NSA has two main missions. Itâ€™s kind of a well-known collection mission, and a defends-the-network mission, and itâ€™s a community that respects technical expertise. So when I first showed up there in 1994, I found an environment that truly respected the skill set that I had, and an environment that would allow me to develop my skill set further. For example, they had a robust self-paced learning program,

COL Greg Conti

that frankly I think the Army still isâ€”you know, as we build this Cyber branch that weâ€™ll probably get to later in the discussion, you could literally on your desktop continue your work.

COL Greg Conti

So I spent, I donâ€™t know, eight hundred hours over my two and a half, three years there, doing off-duty hours development, taking different courses and things like that, because it was a very fertile environment for those things.

David Gioe

You mentioned the significance not only of the Army Cyber Institute but of the Cyber

branch as a distinct branch from Signals and MI. Yeah, I think now would be a good time to go into that. What was the need for that? What was the impetus?

COL Greg Conti

Well, I think the need from the Army perspective is they needed expertise in these areas, people who could perform offensive cyber operations and defensive cyber operations,

COL Greg Conti

and that your typical Army career paths werenâ€™t conducive to that. The typical Army career path has a very well-mapped track of leadership development experiences, assignments that youâ€™re supposed to follow. And if you were able to, lucky enough to get into a cyber-type assignment, it would really be for one tour. And if you tried to get two and were able toâ€”and typically you had to fight very hard to stay to do more than oneâ€”it really was potentially a career-ender to do so.

COL Greg Conti

So I see thenâ€”so you fast-forward to the present, and I know many peopleâ€”taking a step back, I know many people that fell by the wayside because they were really passionate about doing this work. But the largerâ€”and I would joke the immune system of the Army would kill off cyber people, because it was foreign, it was different.

COL Greg Conti

So that kind of mindset, righting the ship and helping create a path that allowed people to go through 30 years of development, length of college degrees, you know, for pre-commissioning, straight into a career path for 30 years, that would be game-changing.

COL Greg Conti

I would look atâ€”I served with General McCaffrey, whoâ€™s the Division Commander of the 24th Infantry Division, during the Persian Gulf War, and he knew everything. To a Second Lieutenant, he knew everything. And he would get in front of his staff, and heâ€™d ask them the best questions, and had them kind of squirming sometimes because they didnâ€™t have the answers. And I came away truly impressed with what 30 years of development can do, and the Armyâ€™s quite good at that for Division Commanders.

COL Greg Conti

My goal, then, was to think through how do we do that 30-year development for people in Cyber, â€™cause thatâ€™s how you grow a truly professional world-class force?

David Gioe

You mentioned that you went to Georgia Techâ€”

COL Greg Conti

Yes.

David Gioe

And received a PhD. Is that part of what can be expected in terms of growing Cyber leadersâ€”some sort of advanced education, and if so, in a STEM-type discipline?

COL Greg Conti

I think whatâ€™s expected of Cyber leaders is continual learning, a passion for the discipline, because if you just rely on the traditional Army model, which is quite good, that youâ€™d go to school for six months to a year, do an assignment, you know. And then go as a Captain, you spend six months to a year getting more schooling, and then another three to four, five years, and go to the Commander General Staff College.

COL Greg Conti

Really robust programsâ€”unfortunately, they are insufficient to keep up with Mooreâ€™s Law.

COL Greg Conti

The technologyâ€™s changing so fast that I struggle to keep up, and I love this stuff. So I spend almost every waking minute working on this area, because itâ€™s what I do, and so I think thatâ€™s a requirement. Going back to your question, where weâ€™re trying to get with the branch is that fundamental training as a baseline, and thatâ€™s really the minimum standard, and then finding people that are passionate about this, that will then drink deeply from the well, and help feed that, whether itâ€™s allowing them to take additional training along the way at various points in their career.

COL Greg Conti

But also people thatâ€™ll go home, will build networks at home, will read books, will write papers, will watch the movies about this, and will just continue their development.

COL Greg Conti

And importantly, read current events and developments in technology. I think youâ€™ll see graduate school at least to the Masterâ€™s level be part of that. A PhD, weâ€™re still sorting through what that means, because you want to use that skill set wisely, and itâ€™s a long time away from the larger force.

David Gioe

In hearing you describe drinking deeply from the wellâ€”

COL Greg Conti

Yes.

David Gioe

Really having a passion, maybe now would be a good time to talk about the future of the Cyber branch. You just returned from an Assignment Branching Board trying to consider what the next talent poolâ€™s going to look like, and it sounds like youâ€™ve described several of those attributes. Is that a fair statement?

David Gioe

And if so, what do the next branch of junior, or the bunch of Second Lieutenants, look like?

COL Greg Conti

I think that is a fair assessment. Weâ€™re looking at people who are passionate about technology, that are self-learners, that have the ethical foundation so that they wonâ€™t abuse the skills, the powerful skills that theyâ€™ve learned and will continue to learn. I think itâ€™s also important to have an adversaryâ€”the ability to have an adversary mindset. Itâ€™s something I learned in Military Intelligence, that as the 2, as the Intel Officer, you need to be able to project yourself on the adversary youâ€™re facing, get in their head, and figure out how would they respond to this, and then predict what thatâ€™s going to be, and you get good at that.

COL Greg Conti

Itâ€™s the same thing. You need to think like a hacker to say, â€œHow would I break into these systems?â€ and then defend against it.

COL Greg Conti

I think we do a good job of that here with the Cadets. Frankly, what weâ€™re talking about is just my anecdotal experience in what those attributes are, and weâ€™re trying to do research to formally define what those are, what those should be, and then share them. Because ultimately it canâ€™t be a â€œweâ€™ll know it when we see itâ€ modelâ€”we need to define it, so then we can tap the full power of Human Resources professionals to then help us identify them, or at least prescreen those folks.

COL Greg Conti

So one of the things weâ€™re working on is to define what that should be.

David Gioe

Perhaps youâ€™ve hit everything, but if not, how should young people, maybe even pre-Cadets, maybe folks, high school students or students in a Junior ROTC program, or anything, even the Boy Scouts.

David Gioe

You know, if they want to be the Director of the Army Cyber Institute 25 years or 30 years from today, what would you encourage them to do? Where would they start?

COL Greg Conti

Well, I would say not to shy away from technologyâ€”not to shy away from studying hard subjects in school. And things like mathematics are progressive, so if you kind of arenâ€™t committed to it early on, youâ€™ll find yourself behind, you know, continually. So that would be one, not to shy away. Male or female, you need to be interested in that and dig in and put the effort in. It does get easier. You get beyond the kind of fundamentals into what I consider much more fun aspects. And I think leading.

COL Greg Conti

I think programs like the Boy Scouts, seeking out leadership positions in school, trying to behave in an ethical way, all of those things are important. I think coding, learning to program early is helpful, because much of the world is run by code. In the Army historically itâ€™s all been a very human activity, but increasingly, aspects are becoming more and more automated. Itâ€™s really this human and machine symbiosis that occurs, and I think over time, weâ€™re going to see more and more aspectsâ€”that thereâ€™s going to be increasingly more automated pieces.

COL Greg Conti

Think robots on the battlefield, automated weapons systems like the Phalanx systems on the ships, where youâ€™ll just have a human in the loopâ€”or human on the loop to monitor whatâ€™s going on. So those things you can do in school to help prepare you for that, that kind of world, would be a powerful way to start.

David Gioe

Youâ€™ve mentioned ethics twice. Certainly, when you say hacker you were quick to note the good kind, and we often hear of hacks in malicious terms. Is there something distinctive about the cyber domain that requires a special emphasis on ethics, or are there distinctive threats or temptations or lures that would tempt young people in ways that maybe we wouldnâ€™t want them to go?

COL Greg Conti

I think so. I mean you have a great deal of power that can be vested in a single person in terms of cyber capabilities and what you can do with that. If misused, that can be dangerous.

COL Greg Conti

When I think of a Private with a rifle on the battlefield, the worst they can do is, you know, shoot into the sector next to them by accident or something. But in terms of what a rogue service member could do, it could resonate around the world. They could accidentally shoot the wrong country, if theyâ€™re not careful.

COL Greg Conti

Thereâ€™s second and third-order effects that are very subtle in terms of, you know, cyber operations that can be very damaging to national securityâ€”could quickly become an international issue. Weâ€™ve hadâ€”but at the same timeâ€”so thatâ€™s the concern. But at the same time, you want people to have that playful aspect and explore technology, and West Point isnâ€™t exactly known for its open mindset with such things. So one thing we did is we built actually a couple of labs that are air-gappedâ€”that means theyâ€™re not connected to the Department of Defense networkâ€”that will allow people to explore technologies in ways.

COL Greg Conti

Itâ€™s a safe place to explore really potentially dangerous technologies, and have their fun using these tools without, you know, attempting to do so on Department of Defense networks, which is a bad thing.

David Gioe

How do you envision the Army using, or how would I say it, using, maneuvering, exploiting, existing in cyberspace in the future?

COL Greg Conti

Well, I mean thatâ€™s the question, right? Youâ€™ve gotâ€”I tend to think of cyberspace and the DoD recently declared cyberspace as an operational domain, alongside air, land, sea, and space. But it has unique characteristics. Itâ€™s man-made, in particular. The laws

of physics apply, sort of.

COL Greg Conti

I mean fundamentally, surely they apply. But at the same time, many attributes of that space are man-made and controlled, so you can kind of define half the laws of physics, how it behaves. Our adversaries can do the same.

COL Greg Conti

Commercial technology, commercial off-the-shelf technology races ahead of what the Acquisition and Procurement systems do. I mean some of those programs are two to ten years long, so our adversaries can be very agile. So amidst all that, I think in terms of planes. Youâ€™ve got a geographic plane where kinetic warfare has occurred, and all those rules still apply. But now you have a cyberspace plane on top that interacts with the two, so you can have operations ongoing in cyberspace and engagements, and then engagements going on in the physical world, and synchronizing those and allowing, you know, to support objectives on the ground.

COL Greg Conti

Ultimately trying to defeat an adversary or change their will, overcome their will, and behave as youâ€™d like them to behave.

David Gioe

Thereâ€™s a lot of terminology. You mentioned offensive cyber operations, or OCO, defensive cyber operations, DCO, networks, domains. You hear most often people talking about active defense as distinct from either a reactionary defense or an offensive capability. Can you help us understand where we need to place the majority of our emphasis on, if these terms are even the right ones?

COL Greg Conti

Well, I mean weâ€™re creating this from scratch in many ways, all these. Traditional military doctrine is well-established. It dates back hundreds and hundreds of years, and itâ€™s highly refined.

COL Greg Conti

Really what weâ€™re doing is creating something from scratch, and trying to figure out how you fight conflicts in cyberspace, so really weâ€™re defining as we go. And Mooreâ€™s Law in particular is challenging, because it isnâ€™tâ€”like the evolution of a traditional military doctrine is every five to ten years, maybe, we relook it. But cyberspace, it changes so quickly.

COL Greg Conti

New technology could appear thatâ€™s game-changing and needs to be adapted very quickly. So specifically in terms of computer network defense, as it stands today, much of it comes down to what youâ€™re legally allowed to do. And you are legally allowed to â€“ I am not a lawyer. I am not a lawyer, for the record.

COL Greg Conti

Youâ€™re legally allowed to do more on your own network that you control, both in terms

of the laws of physics that you can define, as I mentioned, but legally, you have greater authorities to operate and do certain things.

COL Greg Conti

Part of it is you have potentially a god-like ability to look into your own networks and find adversaries and hunt down adversaries in your networks, the hunt mission. But the more responsive, active defense could involve really a spectrum of activities. Maybe some would say it could be hacking backâ€"someone attacks you, you attack back, and so youâ€™re basically responding in kinds. It could be crafting the network that there are trip wires and sensors in various places.

COL Greg Conti

You could have documents that, once stolen, beacon back home.

COL Greg Conti

And these are all unclassified examples. So creatively, since you own that train, you can shape it, define it, to behave in ways that support your defense. It hasnâ€™t been done previously, but itâ€™s useful. I mean historically networks have largely been relatively straightforward and similar amongst wherever they were deployed. But now you can craft that domain to control it, make it more defensible, and then add mechanisms that allow you to be more aware of whatâ€™s going on, and shut down operations, or potentially attack back.

COL Greg Conti

A classic problem, though, of attacking back, one, will the lawyers will largely say itâ€™s illegal, and two, its attribution problem.

COL Greg Conti

That an adversary might come in through the network through multiple proxies, and you have to walk that backwards to ultimately try and find the actors responsible, and even from there, you have to then find out, well, who? Are these actors acting on their own accord? Did someone put them up to this? Did a nation-state put them up to this, and theyâ€™re acting as a proxy for someone?

COL Greg Conti

So itâ€™s actually quite hard, because and it also ties back to whether itâ€™s a law enforcement issue. If itâ€™s an online criminal group, itâ€™s probably a law enforcement issue. If itâ€™s a foreign nation-state, then itâ€™s a bigger issue.

David Gioe

It seems that youâ€™ve described many ways in which cyber operations are distinctive from conventional operations. I wanted to just pause on your last comment about law enforcement versus, you know, large national mission forces, some that even involve the national command authority.

David Gioe

How can we conceptualize the threats? In a normal battlefield, you might have another sort of peer, as it were, in the conventional realms, but in the cyber realm, you could have a

state-sponsored group of hackers, an independent group of hackers, a special interest group of hackers.

David Gioe

It seems the Army has so many different front vectors, not all of which are nation-states. How can we make sense of that?

COL Greg Conti

Well, thereâ€™s actually been some I think pretty good thought in that space, and Iâ€™ll try and remember. Iâ€™m just taking some notes to make sure I approach it appropriately. The first is I think in terms of attack service. What is out there and what can be attacked, and then defendingâ€”you know, figuring out where the enemy is likely to go, the adversary is likely to go, and defending against it.

COL Greg Conti

And that resides in theâ€”I gave you two planes in terms of the physical plane and the logical plane, the cyberspace plane.

COL Greg Conti

But really, if you think more closely about it, thereâ€™s the physical plane, where boxes and computer machines sit, tanks sit. Then thereâ€™s a physical plane which, for the people whoâ€™ve studied networking, itâ€™s like the zeroes, the electrical impulses over the cabling and things like that. And then working up through the various types of software, the network layers, to the applications running, and then it keeps going up until you hit like the personas, the online identities of people. Then for example you might have three online identities.

COL Greg Conti

If you are using Facebook, you could have three different user names and passwords to log into that social media site.

COL Greg Conti

Then on top of that, there might beâ€”thereâ€™s physical people behind those online identities, there are command and control structures behind those identities. So adversaries really can operate on any of those planes, probably multiple planes at the same time to do what I was mentioning before, the battlefields youâ€™re trying to take in cyberspace, and you know, the physical space, and make them interact.

COL Greg Conti

So adversaries are doing the same up and down that stack of planes. Much of what we see is asymmetric, too, because the bureaucracyâ€”well, it torments me on a day to day basis. It isnâ€™t necessarily a bad thing. It allows for efficiencies of scale thatâ€”it allows for efficiencies of scale that allow you to create large, powerful groups, and large numbers of people capable to do things.

COL Greg Conti

However, it takes a long time to create that, to overcome the inertia and the friction that would make that possible. Our adversaries do not necessarily possess that friction.

COL Greg Conti

They can quickly form, develop some code, take some existing code, and probably not constrained by laws all that much, operate very rapidly. And an example of that might be as a Lieutenant, a friend of mine was asked toâ€”we were having a big simulation exercise, where the Division was fighting multiple enemy Divisions. And they chose a Military Intelligence Lieutenant to be effectively the Commanding General of the adversary corps that we were facing. And it turned out he beat the pants off us.

COL Greg Conti

Effectively with one or two other people, he beat the pants off an entire Division staff and all the subordinate staffs, because his OODA loopâ€”Colonel John Boyd from the Air Force described the OODA loop of Observe, Orient, Decide, and Act, which is basically your decision-making process. He was operating very, very rapidly. He could just look and decide, okay, Iâ€™m going to move this here, blam. For us to come to that same decision it might take two to three hours, and ran the pants off, and ultimately they had to stop the exercise and tell him to basically start losing.

COL Greg Conti

We have that asymmetry going on today. And more specifically in terms of adversaries and their capabilities, there is a hierarchy that we understand today, that at the low end you have the lone or small groups of malicious hackers, and it goes up from there that you have, say, current phrase is hacktivist groups.

COL Greg Conti

They might form around a given cause and do some sort of online activities. At a higher level, you have online criminal groups. Maybe you have terrorist groups, but although weâ€™ve seen terrorist groups really being more interested in fundraising and spreading ideology than actually doing attacks.

COL Greg Conti

But the online criminal groups haveâ€”you see increases in resources in terms of money and people they can throw at the problem. An online criminal group has illicit sources of income that allows them to perhaps resource what they do at a higher level. Then as you go up, you have potentially nation-state capabilities, smaller nation-states all the way up to large nation-state capabilities. Sometimes you see those nation-states helping actors further down, maybe to avoid attribution.

COL Greg Conti

Or those less capable groups may care a lot less about doing something if they have the will, but they donâ€™t have the capability, so if thereâ€™s a pairing between a nation-state and one of those groups, thatâ€™s particularly concerning. And then outside of that spectrum, some things we forget are that traditional spectrumâ€”insider threat, that sometimes the enemy is usâ€”we saw that with Edward Snowden and Private Manningâ€”to a great deal, damage can be someone on the inside. Iâ€™d also think in terms of depending on how you define adversary that certain large businesses are quite capable.

COL Greg Conti

And theyâ€™re collecting tremendous amounts of personal information on us from our search queries, emails we send, and really for the purpose of largely targeted advertising.

COL Greg Conti

So you have all these actors in play.

David Gioe

You mentioned the insider threat, particularly Snowden and Manning, and of course their cause has been taken up, you mentioned hacktivists, then journalists, you know, documentary movie makers, and thereâ€™s a lot of noise about the U.S. governmentâ€™s efforts in cyberspace. What would you say to people about the United States government operating in cyberspace? What do they need to know about the cyber mission force or the mission generally, and how can they make sense of all of the other competing inputs that theyâ€™re hearing based on the two events that you mentioned?

COL Greg Conti

Well, so thatâ€™s actually quite a loaded question, and a challenging question.

COL Greg Conti

I would say that Iâ€™ve seen on both sides of that question an intense amount of passion. On one side, you have folks thatâ€”it often can come down to the trade-off between privacy and securityâ€”that if youâ€™re not careful, you can threaten the democracy which weâ€™re trying to protect. Iâ€™ve been on both sides of that, and I see both groups absolutely believing what theyâ€™re doing.

COL Greg Conti

I think the answer is probably dialogue and transparency when possible, trying to find solutions that there doesnâ€™t have to be a trade-off between privacy and security in all ways. You can find solutions that increase privacy and increase security. I do know that the people in uniform are trying to provide security.

COL Greg Conti

Theyâ€™re very dedicated folks. Theyâ€™re not glib about it, and theyâ€™re doing their best to do so, and itâ€™s a very difficult time.

COL Greg Conti

Because right now, I mean my understanding of the law is that youâ€™ve got individual companies fending off, you know, adversaries, potentially nation-state level adversaries, and you have a military thatâ€™s charged to protect the nationâ€”theyâ€™re wanting to help accomplish that mission. Itâ€™s difficult. Itâ€™s very difficult, because if youâ€™re not careful, you can challenge, you can undermine our freedoms while trying to increase security, or trying and may or may not be actually succeeding, in increasing security.

David Gioe

Youâ€™ve been doing things cyber before they were perhaps called cyber, for over 20 years, in uniform.

David Gioe

I wanted to ask you about your perspective on the evolution of cyber as a threat, or as a domain. How has cyber changed, cyber operationsâ€”how has that changed over the course of your career as a Cadet, or as a Commissioned Officer?

COL Greg Conti

Well, like you said, a lot of this occurred, a lot of the development occurred before we really understood the full potential of what it could bring, and I wonâ€™t claim we understand the full potential today. But I think we have a much greater understanding. So it was an evolution, and at first, people raced to build great new things with the technology that was available. Security was an afterthought. It really wasnâ€™t an issue early on.

COL Greg Conti

And by the time we became increasingly dependent on it, where we are today, weâ€™ve built fragile houses of cards that are often hard enough to keep working on their own, let alone when thereâ€™s a determined adversary trying to break them or knock them over. As far as I see it maturing, that much of what was probably initially done was building and operating like I said, and designing new technologies, and there have always been intelligence collection activities. I think youâ€™re seeing more and more public face of that.

COL Greg Conti

The intelligence community has always been kind of hampered in the game to tell their story, because much of what they do is classified and it only comes out years and years later. I see a maturing in terms of a career path forming, a cyber mission force formingâ€”a recognition of the types of people that we want to grow and nurture, and not kill off by the system.

COL Greg Conti

All of that I see happening, so itâ€™s an exciting time.

David Gioe

Letâ€™s keep going with that themeâ€”

COL Greg Conti

Okay.

David Gioe

In terms of trends. What do you think is on the cyber horizon, and the near term may be five years, or ten years, or even in a generation or so, by the time todayâ€™s Cadets who are seeking to branch Cyber, by the time theyâ€™re Colonels, what is the cyber domain or cyberspace, what is that going to look like for them?

COL Greg Conti

Well, right now weâ€™re going through an era of cultural change within the Army, so in the near-term weâ€™re going to continue to do that, and itâ€™s not a done deal. I mean the Army, the DoD I think largely appreciates it, but we have a great deal of progress to be made, a great deal of education to help inform people about what it is, what it isnâ€™t, what its real capabilities are, what they could be.

COL Greg Conti

So I see that occurring in the near-term. In terms of technology, I mean weâ€™ve created something thatâ€™s a fragile house of cards, that if you try and bolt security on after the fact that can be very problematic and expensive.

COL Greg Conti

But at the same time, the incentives, particularly in industry, are not to design security in, because itâ€™s a rush to get products to market first. Now, but we see this countervailing force of well, if your business gets attacked in a major way, like weâ€™ve seen the attacks against Sony where movies have been released that theyâ€™ve worked on for many years, and much of their personal information has been dumped to the internet.

COL Greg Conti

I think weâ€™ll see maturing of thatâ€”that thereâ€™ll be greater and greater awareness on the pipeline of people with expertise in this area who will come in and help mature the discipline, and hopefully we can build security in from the beginning. Weâ€™ll have raised awareness across the country and around the world. As far as technologies, certainly mobile is what weâ€™re transitioning from desktops and PCs to mobile, to our mobile devices, things like cellular phones. And then the buzzword today is the internet of thingsâ€”that every device will be connected to the internet, or many devices will be connected to the internet.

COL Greg Conti

I think back of Isaac Asimovâ€™s story of, you know, We Robots and others. I remember one particularly about a toy that was this intelligent toy that the child became attached to, and parents I think took it away.

COL Greg Conti

I think weâ€™re entering that era for those of you right now. For those of you in the future, we have our cellular phones, and thereâ€™s an artificial intelligence agent called Siri that we can talk to and will give us information, but basic information. But thereâ€™s a personality there.

COL Greg Conti

I mean we see the glimpses of what that artificial intelligence can become, and I think youâ€™ll see that embedded into the internet of things, and increasingly intelligent corporate entity, corporate AI is coming. I think weâ€™ll see implants as people try to extend their lives and increase their functionality with new technology implanted in our bodies, things like cellular phones and locators. And if you push me farther out, I would say that weâ€™re going to see direct neural interfaces, kind of the â€œhello worldâ€ or the initial example of that would be you wonder what time it is, and the chip in your brain tells you what time it is, right?

COL Greg Conti

I think thatâ€™s comingâ€”donâ€™t know the timelineâ€”25 years from today, maybe. With that comes a whole host of challenges. If you think about the malicious software getting onto your computer, Iâ€™m very concerned about malicious software breaking past the firewall and getting into our brainsâ€”so yeah, exciting times. As a security professional,

you tend to see the glass is half-empty. Others will try and sell you these technologies because theyâ€™re cool, and we may repeat that cycle all over again where the bright, shiny new technology outraces the security.

David Gioe

It seems that Admiral Rogers, the Commander of Cyber Command, recently testified before Congress, and he said that a traumatic cyber event was not a question of if, but a question of when.

David Gioe

It seems that as a security professional youâ€™re also sort of seeing the dark side of the otherwise neat opportunities. But what keeps you up at nightâ€”if thereâ€™s one thing that you could put your finger on that really has you most concerned?

COL Greg Conti

So the true answer is there are things that literally keep me up at night. I wake up at 3:00 in the morning. It isnâ€™t so much the threat aspects. Itâ€™s more trying to take care of the people, and feed the myriad senior leaders. Weâ€™ve got some great champions, so providing the information they need in a timely way, and interacting with higher levels, highest levels of the Army, is actually very demandingâ€”for example, Iâ€™m briefing the Chief of Staff of the Army in early January.

COL Greg Conti

And to do so, I have to brief a Council of Colonels.

COL Greg Conti

I have to brief a one to two-star General Officer Steering Committee. I have to brief a three-star General Officer Steering Committee, all in preparation to brief the Chief of Staff of the Army. Before even briefing the Colonels, I had to brief the Superintendent here, and then before that, prepare slides, PowerPointâ€™s. Iâ€™m sure thatâ€”look it up in Wikipedia. For the future audience, look up the military communicates by PowerPoint, so you have to polish the PowerPoint slides and your briefing, pre-brief it, pre-brief it, pre-brief it, pre-brief it, and ultimately, brief the boss.

COL Greg Conti

Great, great championsâ€”you know, General Odiernoâ€™s been a great champion. Secretary of the Army McCune has been a great champion of this. They get it.

COL Greg Conti

But a lot of effort goes in. The second is thereâ€™s a lot of well-intentioned people kind of in the intermediate layers, and just trying to slowly adjust and keep things in lineâ€”largely take care of the right people and allow them to thrive. So thatâ€™s usually what keeps me up at night.

David Gioe

What do you look forward to when you hit 30 years and you can finally leave the PowerPoint and the pre-briefs behind? What future challenges after your career in uniform do you afford to?

COL Greg Conti

Iâ€™ve had the luxury for a few years at least, while Iâ€™m on the faculty and running the Cyber Research Center before it turned into the Army Cyber Institute, to think and write. I suspect after I graduateâ€”after I graduateâ€”after I complete 30 years, and Iâ€™m at 25-1/2 years in the Army now,

COL Greg Conti

that if I can make it work, I will spend some time trying to capture these thoughts and put them down. We could haveâ€”thereâ€™s a lot to be said about this period thatâ€™s moving so fast.

COL Greg Conti

Seems like we have weekly historic change occurring, that one day itâ€™s the Cyber branch is created, the next week weâ€™re creating the Cyber branch insignia, a couple of weeks later weâ€™re defining criteria to choose the first West Point Cadets going Cyber, the first ROTC Cadets going Cyber. And this all involves like a week at Fort Knox to go through files. Itâ€™s all very time-consuming where weâ€™re laying the groundwork, I think, down the road, that institution that is the Army will take place. So all of that, I would like to capture that.

COL Greg Conti

Thereâ€™s so many areas we could dig into in terms of books and writing and advising that are hard right now.

COL Greg Conti

Weâ€™re putting a lot of energy into building the airplane. Iâ€™d like toâ€”building the airplane, building the infrastructure, building the organizations. Iâ€™d like some more time to stay in the discipline. Like I said, going back to day one, this is what I love doing. Right now Iâ€™m in a position of helping people do what I love doing. I want to hopefully buy back some time to continue to do it myself.

David Gioe

Well, I think if Amazon.com still exists in the year 2020, weâ€™ll look for your best-selling cyber memoirs. But in the meantime, let me again thank Colonel Greg Conti, ACI Directorâ€”thanks very much for your time.

COL Greg Conti
My pleasureâ€”thanks.