David Gioe:
Today is December 18, 2014, and weâ€™re here at the West Point Center for Oral History with Captain Brent Chapman. Welcome, Brent.
CPT B. Chapman
Thank you. Good to be here.
David Gioe:
Before we get started, could you please spell your last name for the transcriber?
CPT B. Chapman
Sure. Itâ€™s Chapman, C-H-A-P-M-A-N.
David Gioe:
Thank you very much. Well, letâ€™s start at the beginning. Tell me a little bit about yourself, where youâ€™re from.
CPT B. Chapman
Sure. I was born in Georgetown, Guyana. Itâ€™s just a little country in South America, on the northern coast, in the early â€™80s. Later on, my family and I immigrated to New York City, and so I spent my formative years in the city, going to school in the city. Graduated high school, tried college for a little bit, it didnâ€™t work out, so I enlisted in the Army as a Signals Intelligence Analyst. It was my first opportunity to leave the New York bubble. I got to travel the world, see Oklahoma and Texas and strange places I never thought Iâ€™d be, so that was neat.
And then I got a calling back to New York when I became a Cadet at West Point.
David Gioe:
Can you just quickly tell us how you went from going to Oklahoma and Texas and other places to getting an appointment as a Cadet here at West Point?
CPT B. Chapman
Sure. So I was assigned, Iâ€™d just gotten to my first duty station at the Medina Annex at Lackland Air Force Base as a Signals Intelligence Analyst, and began the conversation with the Admissions Department at West Point. And I found out that there was a component of the admissions effort focused on recruiting enlisted, so I said, â€œThis is interesting.â€ I promised my mom Iâ€™d go back to college, and it worked out.
David Gioe:
What is your current assignment now? Letâ€™s fast forward a little bit.
CPT B. Chapman
Sure. So Iâ€™m currently assigned as a Research Scientist with the Army Cyber Institute, and also as an instructor in the Department of Electrical Engineering and Computer Science.
David Gioe:
Otherwise known as the EECS Department.
CPT B. Chapman
The EECS Department.
David Gioe:
What does it mean to be a Research Scientist at the Army Cyber Institute?
CPT B. Chapman
So my particular area of focus is in education research, so Iâ€™m in the Education Research Division. But for me, itâ€™s really a chance to well, really, get paid to do things I want to do. And so cyber has been a personal interest of mine for many years, before it was really called cyber or really given its title. Exploration, breaking things, hacking things, if you will, has always been a personal interest of mine, so now I get to find out ways to improve my techniques, but also package it up so that I can teach it to others, and so they can learn.
David Gioe:
Okay, going back to West Point for a moment, I just want to take a few minutes to talk about your experience here and how that prepared you for your futureâ€”

CPT B. Chapman
Sure.
David Gioe:
Responsibilities. Letâ€™s get the chronology right. What year did you graduate?
CPT B. Chapman
So Iâ€™m a 2009 graduate.
David Gioe:
Okay. And then over the time from your enlisted time up through your appointment, being a Cadet and then graduating in 2009, looking on the totality of that experience, how did the Cadet, and I guess even Junior Officer experience, prepare you for your current responsibilities at the ACI, or in general?
CPT B. Chapman
So whatâ€™s interesting is that of course there wasnâ€™t a Cyber when I was a Cadet, and certainly when I was enlisted. But when I arrived to West Point, and then later on to my Department as a Cadet, I was an IT major, one of the first IT majors here at West Point.
David Gioe:
Information Technology.
CPT B. Chapman
Information Technology, yep. We had received accreditation that year, and so it was sort of a very exciting time to be in the Department. And I was able to form really great relationships with some of the instructors and they have become mentors, folks that I keep in contact with to this day. And I noticed that they had the same level of enthusiasm about the subject as I did, which I thought was kind of unusual, that this old guyâ€”this guyâ€™s an Officer, you knowâ€”heâ€™s as thrilled about this as I am.
And so that sort of got me thinking that maybe I could do something like this and make it a career, and maybe impact others in the same way as they did me. And that sort of started my love affair with teaching, teaching cyber specifically, and then hopefully getting back to West Point to do this before I go.
David Gioe:
Before we get too far down the cyber path, how does being an Academy graduate impact your duties as an instructor? So in addition to ACI Research Scientist position, youâ€™re also an instructorâ€”now that youâ€™re on the other side of that fenceâ€”
CPT B. Chapman
Yeah.
David Gioe:
What does that look like, and how has that molded you?
CPT B. Chapman
So it was a little strange. I had arrived in the summer for my assignment, and I still had that feeling in the pit of my stomach coming through the gate as I did when I was a Cadet, and I thought it would never go away. Itâ€™s gone away now, but with that in mind, Iâ€™ve noticed that in the classroom I can connect a little quicker with the students Iâ€™m teachingâ€”freshmen primarily. And I see theyâ€™re sponges. Theyâ€™re ready to soak up all the info Iâ€™ve got to fire at them. But theyâ€™re also scared. For many of them, this is the first time in the Army.
What is this? What is this new experience, what is this new place? What is the Academy? So I like to take a break sometimes and just talk about what life is like as a Cadet, and say, â€œHey, itâ€™s okay. Itâ€™s good, you know? Things turn out.â€ â€™Cause I was in that position not too long ago.
David Gioe:
Although youâ€™re a fairly recent graduate, I think itâ€™s worth exploring your path from the time where you Commissioned to your current position here at the Army Cyber Institute.
CPT B. Chapman
Okay.

David Gioe:
Where did that path take you, what did it look like?
CPT B. Chapman
So since I was, as I mentioned before, enlisted in Military Intelligence, but I didnâ€™t want to Commission into the Military Intelligence Corps, so instead, I went Signal, figuring that I would get more of the technical experience. Get hands-on on switches and routers and all the technical things with the blinky lights. How true that was, I reallyâ€”itâ€™s not as true as Iâ€™d hoped, certainly. But the exposure with customers, with the war fighters, with those that we support, is something I didnâ€™t anticipate getting, but has been so beneficial for me.
To understand where these services, where our efforts are going, and how itâ€™s impacting operations on a daily basis, so it was a very positive experience, one I didnâ€™t expect to get going Signal. And eventually I becameâ€”Iâ€™m technically now still a Functional Area 24. Iâ€™m a Network Engineer, so I made the decision about a year and a half ago to just go Functional Area, which means that I do more of a technical job. I do a technical job more often than if I were just a regular Signal Officer.
David Gioe:
Why donâ€™t we skip ahead to talk about branch, and you mentioned that you branched Signal, but now the Army has stood up its own Cyber branch. What does that mean for you as a Signal Officer, and then also what does that mean for the Army or for the nation, you know, big-picture?
CPT B. Chapman
Sure. So for meâ€”Iâ€™ll start with me, itâ€™ll be sort of easier to answer. I put in my request for a transfer to the new branch, so Iâ€™m waiting along with many others for a decision to be made. So Iâ€™m crossing my fingers, and I wanted to do cyber before it existed, and so the Cadets I get to mentor, for example. I live vicariously through them, and their enthusiasm coupled with mine, and then also coupled with the Army sort of momentum towards this new branch, I think is great and is what we need. At a time when the Armyâ€™s downsizing, itâ€™s kind of tough to stay focused. But again, the Armyâ€™s realizing that cyber, you know, and it can be described in many different ways depending on who youâ€™re talking to, should be a priority. So getting to the Armyâ€™s level, Iâ€™m thrilled and very pleased to see that the Armyâ€™s putting so much effort into making sure that weâ€™re approaching it the right way. It seems that although we werenâ€™t the first to get, to get after cyber, if you will, I think our slower, methodical approach is going to pay off. We, as in the Armyâ€™s, methodical approach is going to pay off, really identifying what requirements are, maybe seeing cyber in a different way than Senior Officers are used toâ€”those are all very critical tasks and points that we need to address.
David Gioe:
You mentioned to do cyber, but what does that mean to you, to do cyber?
CPT B. Chapman
So it means so many things to the audience, so to the nation, to the Army. So to some itâ€™s strictly the zeros and ones in our networks. To others, it may be thereâ€™s maybe some physical component to it, whether that physical component is power or the spectrum. For me personally, I think itâ€™s all of it. I think itâ€™s where zeros and ones meet, the physical world, because we have real threats in that area. I see industrial control systems, for example, all sit on a SCADA. That certainly is cyber, because although weâ€™re not using kinetic means to deliver those actions, the results are very real and very physical. So for me, cyber is the zeros and ones, and exactly where it meets the physical world, and how IT services and IT infrastructure supports making things easier for us. And thatâ€™s all cyber to me.
David Gioe:
What do you think your interface is between the cyber warrior and the conventional war fighter? Where do those domains meet, if indeed you think cyber domain is its own domain? Where do they overlap, or how do they overlap, if at all?

CPT B. Chapman
I think they overlap in sort of two areas. The first is that we use cyber, we use IT, if you will, as really the infrastructure to support all the things we do. These systems are built into our vehicles, our weapons systems, our communication systems, so in that sense cyber is very much tied in to what we do on a daily basis. But we could also use cyber as a means to deliver effects itself. In the same way that cannons and bullets achieve a certain physical affect, we can also use cyber to achieve a certain effect.
And so we have on one hand cyber used as sort of a support, an infrastructure, and on the other, cyber used as the effect vehicle itself.
David Gioe:
In the Cyber branch, which you mentioned that youâ€™re hoping to re-branch, if thatâ€™s the right termâ€”
CPT B. Chapman
Sure.
David Gioe:
What experiences have helped you to understand what your goal in that branch might be, or what have you learned in your career thus far that you want to bring to Cyber branch?
CPT B. Chapman
So I think one of the most difficult aspects of cyber, whatever it is, is that for many Senior Commanders, there is just no realâ€”thereâ€™s no full understanding of what can really be achieved. In many cases, some Commanders expect almost fantastic effects from our computer systems, and these are just not realistic. And so I hope to bring that level of realism, that technical background, the technical expertise, to really fully inform Senior Command, and so Senior decision-makers, on whatâ€™s really possible, and maybe make them aware of things that they didnâ€™t think were possible.
Things that may perhaps save some lives, reduce work, ease your way of doing things, in much the same way that IT is already doing.
David Gioe:
Is it possible to give us an example of some of the fantastic things that thereâ€™s a perception that cyber can do? Sort of just flick a switch or press a button, then you have a desired end state?
CPT B. Chapman
Well really, thatâ€™s exactly it. We have movies showing us that in three minutes on a keyboard, this super-elite hacker can take down an entire power grid. Although not completely out of the question that one can do this, itâ€™s not happening in a matter of seconds, and itâ€™s not that easy to get these people to begin with. And so itâ€™s exciting to think about and itâ€™s really sexy, but thereâ€™s a lot that goes on behind it in order to support whatâ€™s really possible.
David Gioe:
How do you get across whatâ€™s truly possible to Senior leaders in the Army, or even broadly, in business or in government? How does that conversation take place, or what does that look like, between people with your skill set or who are in your branch, and then more Senior folks who might not be as familiar with on-network operations?
CPT B. Chapman
So I think the ACI, you know, is actually doing a great job of that. In fact, one of the primary core functions of the ACI is outreach. And thatâ€™s outreach to communities in the Army, communities in academia, communities in industry. And by just very basically forming these connections and starting conversations, we build relationships where these things can happen, where these conversations and this sharing of ideas is happening.
And that takes, of course, a bit of effort on everyoneâ€™s part, and a bit of interest, but what ACIâ€™s doing is weâ€™re facilitating these bridges being built, and it looks like itâ€™s very successful so far.
David Gioe:

Is there anything in that method or in that undertaking that young people, whether Cadets, or ROTC, or even JROTC, or young people generally, can they prepare themselves, either through, you know, some engagement with the ACI or some other similar type body, to prepare for a career in your field?
CPT B. Chapman
So at West Point we have the Cyber Leader Development Program, and this is really just for the Cadets right now. And this is a framework that weâ€™ve built to help identify interested Cadets, and really set them up for success in terms of making sure they take the right courses, theyâ€™re majoring in the right things. And this doesnâ€™t necessarily have to be Computer Science or IT or Engineering. This can be Math, or it can be something in the Humanities. But making sure that they are in the right path, theyâ€™re taking the appropriate summer courses, the internships.
At West Point we call them AIADs, Advanced Individual Academic Development, and these are really internships at some of the places that West Pointâ€™s already very well connected into, some of the agencies. The NRO, the NSA, for example. And again, this is voluntary for the Cadets, and what we want to get is that it takes some effort on your part. The path is there, and weâ€™re going to help facilitate that as much as possible, but itâ€™s really about interest. And if they are interested, they take these internships, they major in the right things.
They perhaps spend their summers or their free times doing something that their friends arenâ€™t doing. Maybe they go to a few security conferences.
David Gioe:
It seems logical that IT or STEM type majors would be either interested or involved or branch Cyber, but you threw the Humanities in there. To your mind, what could someone whoâ€™s majoring in the Humanities offer to the Cyber Mission Force?
CPT B. Chapman
So many years, so maybe two decades ago, when computers were first coming on board as part of our culture, you really had to be a computer scientist to even use the thing. You had to understand how it worked to really get anything useful out of it. But nowadays computers are everywhere. Theyâ€™re in fridges, theyâ€™re in phones, theyâ€™re in cars, and you know longer have to have a technical background or even an understanding to use these things. So this introduces many more interesting dynamic aspects to the whole world of computing, what is computing, because itâ€™s so tied into so many different things. So I think itâ€™s incredibly useful, for example, to have an economist, or someone who is focused in the social science things, looking at these problems that occur in cyber, because it brings a whole new perspective, a rather fresh perspective to these problems, tackling these problems. And coupled with the guys with a technical background, I think this more comprehensive approach produces better results.
David Gioe:
It seems that youâ€™re talking really about the accessibility of technology on a lower barrier to entry for others to understand. Is that a widely shared sentiment, or is there a sense that itâ€™s really the hard engineering or hard sciences that are going to drive the branch forward?
CPT B. Chapman
Hmm. Iâ€™m not sure how widely shared the sentiment is, but from my experience in the ACI, for example, I think the ACI being a multidisciplinary organization shares that same approach to it. And donâ€™t get me wrong, there are certain levels of technical understanding that certain jobs should have. An operator should have a very solid technical foundation. But someone whoâ€™s analyzing, perhaps, some type of activity doesnâ€™t necessarily need to have that. So it may depend on the job, and I think thereâ€™s a space for just about every discipline in this very dynamic and new world of cyber.
David Gioe:
In your experience, has there been a person or a mentor or an experience or an

assignment that has shaped who you are, and what you think that you are bringing to the cyber domain wearing an Army uniform?
CPT B. Chapman
So outside of the Army, when I was in middle school I had a lion teacher who would later become a close family friend that really opened my eyes to the fact that learning could be fun, and could be a lifelong thing. And for me, fortunately, thatâ€™s sort of rather early on, and so I think that love of learning, the love of the fact that she told me that I shouldnâ€™t be afraid, or I shouldnâ€™t be ashamed of the fact that I liked to break things and try to figure them out, really stuck with me. So that love of learning, that sort of embrace of my destructive hacker side, has really paid dividends for me.
In the Army, Iâ€™ve had several mentors here at West Point, at the Military Academy, and theyâ€™ve really shaped my outlook tremendously. Those include the current Director of the Army Cyber Institute, Colonel Greg Conti, other individuals serving throughout the Cyber Mission Force. Lieutenant Colonel John Giordano, for example, taught me while I was a plebe in Freshman IT, and that was like the first sort of â€“ he was the first real person I could reach out and grab, and say, â€œHey, thatâ€™s a cyber guy.â€
It wasnâ€™t cyber at the time, but he had a background in the Military Police and Transportation. I saw, hey, heâ€™s led this very interesting life, but in the end of the day, at the end of the day, heâ€™s doing what he loves to do, and I said, â€œHey, maybe I could do the same thing.â€
David Gioe:
It seems that youâ€™re talking about things that are cyber in nature before we were calling them cyber, so youâ€™ve been tracking these things for a while now. How have your perspectives about the threats in particular, or the opportunities, that the cyber domain both affords in terms of opportunities, but also the threats that the cyber domain presents to us as Americans. Howâ€™s your thinking on this evolved over your time either in the Army, or even before that, as a Cadet?
CPT B. Chapman
So clearly, more folks are connected to the networks, connected to each other now as there are more devices that are connected. Computers are getting faster. So this presents all types of challenges, but what I found, and reinforced now that Iâ€™m instructing, is that education is the numberâ€”should be a priority for those with very technical backgrounds, and those not, who are just users. In fact, many folks using just donâ€™t know the simple ways they can protect themselves. How easy it is to have data taken from you.
So by starting with education, we can branch out to more advanced aspects in using or defending yourself in terms of the cyber threat. But it starts with education, I think, so then in my class with the freshmen, I get them nice and early. We spend a whole block of instruction time on cyber, and I introduce them toâ€”I open their eyes into whatâ€™s possible.
David Gioe:
What does that look like when the bulb finally goes on for a freshman?
CPT B. Chapman
Well, itâ€™s a great feeling. Personally, I like to introduceâ€”I begin with perhaps some pieces, some clips from the news, and I say, â€œYouâ€™re hearing about these breaches and youâ€™re hearing about all these destructive things. But hey, look how easy it is to protect yourself. Watch out for these signs. Watch out for these attempts to get your information.â€ And once they see, either through demonstration or through a lecture, how easy it is, you can sort ofâ€”they feel more confident themselves to take that next step.
I have a phone, I know how to use it at the very basic level, but if I change these settings, Iâ€™m that much more protected. And from there, they can sort of branch out on their own and get into it as much as they like.
David Gioe:
How do you then scale that from, you know, IT 105, the freshman course, to the United

States Army?
CPT B. Chapman
Well, thatâ€™s a challenge, right? Itâ€™s really tricky. You have folks in the Army, soldiers, are not justâ€”theyâ€™re not all from the same generation, so you canâ€™t approach it the same way. We as advisers and as educators, for not only the Academy but for the Army, we have to be aware of everyoneâ€™s background, where theyâ€™re all coming from. We have Senior leaders who didnâ€™t have computers, didnâ€™t have a computer in their pocket in the form of a phone. We have Junior Privates who knew nothing about connectivity.
So itâ€™s a more difficult job for us, but itâ€™s one that we embrace, and we have to be more creative. Sure, thereâ€™s certain tests and thresholds that they should meet, but to really get those points home, I think we have to be creative in the way we approach itâ€”and Iâ€™ve seen some pretty effective things going on so far.
David Gioe:
If you were in charge of the Cyber branch, and you could wave a wand and pick whoever you wanted, what sort of mix would you choose between digital natives and people who youâ€™re referencing who donâ€™t always remember having a computer or a smartphone in their pocket?
CPT B. Chapman
I think that regardless of the accessibility of IT and all these products, I think that someone who loves learning something new all the time, and really goes out of their way to do it, is who Iâ€™m going after, because theyâ€™ll be able to pick a new technique up rather quickly because theyâ€™re interested in seeing how these things work. So I always love engaging with folks who do things, who do cyber, or do exploration, or do hacking on the side, because itâ€™s a personal interest, because they sort of share the mindset that they really want to understand how this works. And they want to perhaps bend the rules of the system and see what happens, see how the system reacts, and see what they can get away with. And in doing so and in learning about these things, they can better protect themselves from adversaries who want to use it for darker purposes.
David Gioe:
Letâ€™s talk about those. Letâ€™s talk about adversaries and darker purposes, and also the mission of Cyber branch in the U.S. Army for our purposes. How do you envision the Army using cyberspace in the future, either in an offensive or a defensive capability?
CPT B. Chapman
So letâ€™s seeâ€”the Armyâ€™s sort of been doing cyber for a while under different names. But I think what weâ€™ll see, and what I hope to see, is that we improve our defensive posture, because again, weâ€™re seeing more connectivity, more folks willing to do us harm. So I think our first priority should be to improve our defensive posture, and thatâ€™s a tough job. Offensive is kind of easyâ€”we can score all the timeâ€”but trying to react to someone attacking us, understanding what theyâ€™re doing, first of all, having the skill set to react, and then actually defending is a really tough job.
And Iâ€™m happy to see with this new Cyber branch and the creation of the Cyber Protection Team, for example, that the Armyâ€™s taking a real hard focus in establishing places and people whose sole responsibility is going to be this defense. So I think our priority should remain in this sort of this active defense, if you will. Not just sitting back and relying on some settings to do the job, but really taking a look at our networks and seeing whatâ€™s going on, understanding it from a technical point of view, and then take action to both prevent it, and then to make sure it doesnâ€™t happen again.
David Gioe:
It seems that cyber operations are one realm that the Army is decidedly either fearful of or acting against. Not just nation-states, but organized criminal networks and other things that we donâ€™t maybe envision the Army taking a hard look at. Can you talk about some of the differences in the threat between a nation-state or a terrorist group or organized criminal group, and how can the Army prepare itself to deal with the myriad of threats that

are coming at it?
CPT B. Chapman
Well, I think that one very effective way that we at the ACI try to help the Army deal with this problem is through our partnerships. So the Army, so the Cyber domain is shared. Industry shares this domain. You know my mom and dad share in this domain. And the Army, weâ€™re working in the same areas, so we all share the same interest in protecting it, whether itâ€™s for defense purposes, whether itâ€™s for industrial purposes, the economy, recreation. So by getting everyone involved, and not just saying, â€œHey, itâ€™s just the Armyâ€™s problem,â€ everyone should be concerned because itâ€™s everyoneâ€™s shared resource.
Yes, the Army, we have the training and the manpower behind it, and weâ€™re certainly doing our part. But I think establishing these partnerships and sharing best practices with the titans in industry, for example, is the right way to go, because they have talented folks, too.
David Gioe:
What does partnership look like? What does a best practice look like for someone watching this interview, if they want to know what a best practice would be, or an example of government or the army partnering with industry, can you explain what that looks like?
CPT B. Chapman
Sure. I mean a partnership can be as basic as the Chief Security Officer of an organization meeting with perhaps a Commander, a Cyber Commander, and talking about, â€œHey, how do you react to breaches on your network? How do you react to threats? How do you react to insider threats?â€ And really, the behavior and the mechanisms are quite similar. The networks are protected for different reasons, and the networks are there to facilitate folks doing something, and the ways we react to threats on the network are very much the same.
So, by sharing, really, TTPs, techniques on how one would react to this type of reaction, this type of breach, or this type of threat, and just maybe sharing the manuals. â€œHey, what software do you use? How do you configure your appliances on the network?â€ It can be as simple as that.
David Gioe:
Is that one way that we can help in terms of partnership, we can help improve cyber security? And if so, are there other things along those lines that we either as a state or as an Army, should be doing to continue to improve cyber operation or cyber security or cyber effectiveness?
CPT B. Chapman
So to sort of reference the previous point about education, thatâ€™s also something else that we share in our efforts with those in industry, is that often, quite often the users on the networks areâ€”they donâ€™t have a technical background necessarily. You canâ€™t assume that, and in many cases, they are sort of that weakest link. And so the Army has a certain approach to it in that you have users of all backgrounds, and so does industry, so perhaps sharing techniques on how you educateâ€”what type of training should folks go through to even get on the network, things like that, tend to be effective.
And put us in a better posture to stop these cyber threats before they even get a chance to develop into something more dangerous.
David Gioe:
I think youâ€™ve hinted at this a couple times, but just to make it explicit, can you explain some of the ways in which cyber operations might differ from a conventional operation? When we think of conventional warfare thereâ€™s certain things that come to mind. How is cyber different and what makes cyber operations distinct from when people think of the Army conducting an operation? Whatâ€™s different? Whatâ€™s distinctive?
CPT B. Chapman
So I like to think of the analogy of sort of a chess board. In conventional warfare, you have

your side and the opponentâ€™s side, and you know what the battlefield looks like. Itâ€™s well-delineated, and you know civilians donâ€™t come onto the battlefield. You donâ€™t have other players playing in your chess game, for example. Often, you can see the enemy as he moves around the battlefield, maneuvers into a position to get some advantage over you, perhaps. And then you have some time to therefore think about your move, and what youâ€™re going to do, and perhaps a few moves ahead. But in cyber itâ€™s a little different.
You donâ€™t have a standard sized chess board. In fact, you donâ€™t know how large the board is. In fact, you might not even be able to see the opponentâ€™s playersâ€”thereâ€™s a fog over it. There are other players in the game. You have civilians, right, in the cyber space. I mean we have those in infrastructure, you have educators, you have academia. So youâ€™re blindfold, and you have to make this determination of where was that shot fired from? Well, I donâ€™t know, because I canâ€™ t see what the enemy even has, so itâ€™s tricky, and how do we get over it?
We improve ourselves from a technical point of view, and be prepared for the unknown. Itâ€™s easy to sayâ€”itâ€™s very, very difficult to achieve
David Gioe:
It seems that you canâ€™t really pull a war plan off of the shelf and address a contingencyâ€”
CPT B. Chapman
Yeah.
David Gioe:
Because you donâ€™t knowâ€”
CPT B. Chapman
Exactly.
David Gioe:
What that would be, so how do you prepare? You talked about intelligence a little bit. How can you prepare for a key terrain when the terrain can move, or be different, or change? What does the planning process look like in order to stay one step ahead in the chess analogy?
CPT B. Chapman
Well, I think itâ€™s again, if I were in charge and I wanted to recruit cyber guys, thatâ€™s what I would look for: folks who are flexible, and folks who think outside the box, and folks who donâ€™t necessarily go into an engagement with a plan and stuck on that plan. Sort of a Beowulf, if you will. They are ready to be flexible, theyâ€™re ready to adjust when they have to, because they know that their plan isnâ€™t going to survive that first contact, especially in the cyber world, and they need to have something else in mind. And just know that theyâ€™re going to have to change what theyâ€™re doing, and then perhaps also have that technical background to know whatâ€™s really possible.
David Gioe:
How do you do that? How do you, in the Army culture that emphasizes momentum, and taking the initiative, it seems like youâ€™re describing something thatâ€™s sort of reactive, and may be uncomfortable for Army soldiers that want to go out and seize the initiative, or seize that key terrain. Youâ€™ve described a reactive type process. Does that mean weâ€™re looking for new kinds of soldiers, or weâ€™re looking for soldiers to think differently?
CPT B. Chapman
I donâ€™t necessarily think that itâ€™s reactive. In many cases we do find ourselves in a reactive posture, which is hopefully something that we get out of. But we want soldiers who do think differently. And does it go against the existing culture of the Army?I think to some degree it does, because in the military, you have clearly delineated everything, right? You have a uniform, you have a place to be, you have formations. And thatâ€™s not to say that somebody who is free-thinking and sort of thinks outside the box canâ€™t fit in there.
But often you find that itâ€™s not as easy to find those types of personalities and folks with

those skill sets in the Army, unfortunately. So I think that the Army needs to perhaps make it clear and really focus their efforts on identifying, in whatever way, individuals like that, because those I think will be the most successful.
David Gioe:
Unfortunately, the Armyâ€™s not alone. Youâ€™ve got the other branches of the service alongside, who are also creating their own cyber forces, even if theyâ€™re not called branches. What do you see as the future of the Joint Cyber Force? What does joint-ness look like in the cyber realm?
CPT B. Chapman
I think Joint is good. Diversity is good. Diversity of thought is good, and diversity of background, and diversity of studies, as I mentioned before. This interdisciplinary approach to it seems to work best, and I think sort of the joint approach might be similar, having this holistic point of view, very comprehensive point of view, and identifying what cyber really is to begin with, what the threats are, and how perhaps we should approach these is good. Especially when youâ€™re coming from branches who are used to only dealing with a threat in a certain way, whether itâ€™s Navy, Air Force, or Army. Having this joint approach is an excellent way to go, and perhaps it might be the future of how we see cyber.
David Gioe:
Speaking of the future, what are the most relevant trends in the cyber domain, if youâ€™re looking out maybe even one year or five years, ten years, or even a generation? What do you see coming down the pike in the cyber domain that we need to position ourselves for now?
CPT B. Chapman
Well, in terms of the threat, I guess there are two things that sort of keep me up at night. The first is a threat to our industrial system. I mean we use IT to make our lives easierâ€”hopefully, right? And so with having everything so connected, that introduces all types of problems in terms of our industrial systemsâ€”our water systems, our power systems, our traffic systemsâ€”so any type of exploitation of those systems could really bring this very immediate, very high-impact results.
So I think we should, knowing that we want to keep this standard of living as high as it is, we should protect these systems that rely so heavily on IT, and we should make that a priority. So thatâ€™s sort of my number one concern, and thatâ€™s a concern now, and I think itâ€™ll be a concern over the next five to ten years. My second concern is sort of more of a long play. It would be a very systematic undermining of our financial system.
I think thatâ€™s part of the reason why ACI, for example, partners so much with the financial world, is that we have the sameâ€”of course weâ€™re in the same domain, but we also have the same concerns and the same interest in protecting our system. So if an adversary were to undermine our financial system, in the long-term it could really have effects, not only in the financial world, but nationwide, to include our defense.
David Gioe:
The Commander of U.S. Cyber Command, Admiral Mike Rogers, I think just said something very similar to what you did in terms of national traumatic event caused by something originating in the cyber domain, but that has real-world implications. He said, â€œNot if, but when that happens.â€ Thereâ€™s a lot of debate about how big the threat is vs. how likely it is to happen, and the scale of impact, and how do we prioritize resources to deal with that? Where do you come down on that, that debateâ€”sort of alarmist, or realistâ€”where do you see yourself?
CPT B. Chapman
Well, itâ€™s part of, again, why education is so important. I mean we shouldnâ€™t be afraid to the point where weâ€™re not living our lives and getting things done. But we should be educated and knowing whatâ€™s really possible. And you know one would be surprised at how simple it is to protect, you know, on a certain level, protect yourself from a

certain type of cyber threat. But this collective approach to it, if everyone does his part, I think will make our overall posture so much better. So I would say that we shouldnâ€™t be afraid.
I mean technology is there to help us. But we should take care to educate ourselves to whatâ€™s really possible, and to know that itâ€™s out there, the threats are out there, and take steps accordingly to mitigate those.
David Gioe:
Youâ€™ve briefly referenced the internet of things, and how interconnected everything is. Are there any parallels that we can take for the U.S. Army as a network of soldiers, or every soldier a sensor, or some of these other buzzwords? It seems that one day your refrigerator will talk to your toaster, and itâ€™ll talk to your smartphone. What about from an Army perspectiveâ€”is there an analogous view of the Army as a networked body, and if so, what does that look like?
CPT B. Chapman
So the internet of things is kind of an interesting concept to me. I donâ€™t know if I think itâ€™s necessary. I donâ€™t think itâ€™s necessary to have everything connected, because what benefit does that really bring you in the course of your day, to have your toaster connected? So in a similar light, does it make sense to have every soldier connected, or does it make sense to have only the Platoon Leader or the Commander connected? We still need those leadership skills. We still need that interface, and I think we should embrace it.
We should use IT to the point where itâ€™s making money for us, but I donâ€™t think itâ€™s necessary to force it down to every level if itâ€™s not really bringing us any distinct advantage, â€™cause I donâ€™t necessarily think thatâ€™s the case. I think itâ€™s still important to have people interfacing with people, and doing things the traditional way on the battlefield, and you know, in real life.
David Gioe:
Where do you see yourself going professionally? Youâ€™ve had a time as an enlisted soldier, now time as a Cadet, and then time as a Junior Officer. With the creation of the Cyber branch, and the Armyâ€™s willingness to be flexible and meet new challenges in this way, how do you fit into it?
CPT B. Chapman
Yeah, so one of myâ€”so whatâ€™s kept me in the Army is that the Armyâ€™s sort of put me where I want to go, where Iâ€™ve requested to go, and gave me the jobs that I wanted throughout my career. And I think thatâ€”excuse meâ€”I think that as long as this continues to happen, Iâ€™ll stay in. What I have been very pleased about is that when I first Commissioned, I saw some potential areas for frustration in terms of well, there not being a job or branch or domain that I was really interested in, so I picked something pretty close to it.
But now that the Armyâ€™s sort of opened up this new branch and really put some significant resources behind it, Iâ€™m pretty happy in where the Armyâ€™s going, and I feel like Iâ€™m privileged to be a part of it. So Iâ€™m pretty excited to stay on board and see how it develops over the next foreseeable future.
David Gioe:
Captain Brent Chapman, thank you very much for your time
CPT B. Chapman
All rightâ€”thank you.