Interviewer:
Today is February 5, 2015. We are in the studio for the West Point Center for Oral History, and we are speaking with Bob Stasio. Welcome.
Bob Stasio:
Thank you.
Interviewer:
Could you just spell out your name for the record?
Bob Stasio:
Sure, yeah, S-T-A-S-I-O.
Interviewer:
Excellent.
Bob Stasio:
Mm-hmm.
Interviewer:
So weâ€™re here today to talk about cyber, particularly cyber history. If you could just give me a little bit of background on your involvement with the United States military, and particularly the Army, and a little bit of history on your involvement with cyber issues.
Bob Stasio:
Sure. So I went into the Army. Initially my first engagement was with ROTC, the Reserve Officer Training Corps. I went to the University of Buffalo in New York, had a scholarship there. Studied physics and math, so kind of a more technical major. I always had an affinity towards that type of field, the harder sciences, and I branched Military Intelligence as an Officer. Didnâ€™t really know hardly anything about it, actually. I just thought it was something interesting. I remember when youâ€™re picking your branches for what you wanted to be as an Officer, Military Intelligence is a thing they talk to you least about, but thatâ€™s what I found the most interesting, so I kind of branched in that direction, and ended up getting involved in Signals Intelligence in a Tactical unit. I had the opportunity to stand up a program from really the Corps. I got to a unit in Fort Lewis, Washington, and there was nobody there. It was just me, really. And I ended up standing it up, getting all the soldiers, the NCOs, and having to [coughs] excuse me, and having to establish a training program and what we were going to be doing when eventually we were to deploy to Iraq. So it was kind of my initial involvement with the more technical field. After my tour in Iraq, I ended up getting pulled over to NSA on the Army side, Flight General Alexander. Helped stand up Cyber Command a little bit, and then worked in some Cyber Collection programs there.
Interviewer:
Okay. So how have you seen the evolution of cyber as a discipline within the Army over the course of your career with the Army, and after your time with the Army, in the NSA?
Bob Stasio:
Yeah. Itâ€™s been a pretty fascinating experience, actually. When I first got in, it was more of kind of a side job, a side hat, and I think we didnâ€™t really even use the word â€œcyber,â€ especially initially in my early days when I was a Lieutenant. It was more of kind of a discipline within Signals in college, and so it was kind of what you would call the top tier of Signals Intelligence. If you had maybe a pool of Signals Intelligence Operators, maybe the top 10% of those folks were actually dealing with cyber. I kind of saw cyber as a confluence between Signals Intelligence, maybe Signal and networking, so having an understanding of networking, and maybe a bit of forensics, too, so there was kind of those, a confluence of those three worlds, were really what I considered cyber. And we were doing those things, as a Military Intelligence unit in Iraq, and then I transitioned to do it more strategically. But then it became more of a solid discipline, probably around the time Cyber Command stood up, and there were more strategic thinkers that came in, some more Officers with pedigree and experience in policy that were trying to wrap the discipline into an official component of the Army, I would say.

Interviewer:
And so your time in moving from the establishment of Cyber Command, can you talk a little bit about your experience in being at the forefront of this movement?
Bob Stasio:
Yeah. Thereâ€™s a lot of political infighting, believe it or not [laughs]. I was very much a junior guy there. I was a Captain at the time when I was there, and I was working for a more senior Officer that was on the Commanderâ€™s staff, kind of. They called it the CAG, Commanderâ€™s Action Group. So it was really a great opportunity for me as a junior person to see this whole thing come together. It really started as a combination of working with DISA, the Defense Information Systems Agency, a part of NSA that was kind of the cyber component, and an organization called JTFGNO, which happened to be part of STRATCOM. And the whole concept was to unify the defense, the attack, and the exploitation side of the house, the espionage side of the house. And the vision I thought was pretty grandiose, and it made a lot of sense, but it ended up kind of meeting into the brick wall of reality as this thing stood up. And I think at first what I saw is it was more of an advisory staff, Cyber Command. It was, you know, a bunch of really smart Officers and staffers that could help try to facilitate the gap between the people who had the fingers on the keyboard and policy makers, and maybe the Pentagon and the DoD component, and bridging that gap. And I think thatâ€™s how it initially started out. And I really left that agency and Cyber Com before it became operational, and from what I can see now - not that Iâ€™m on the inside - but what I can ascertain is it seems to be becoming more operational. Theyâ€™re standing up these teams that have been out there in different variety, different aspects of cyber. I think thereâ€™s a defensive and offensive side. You know, it seems to be theyâ€™re actually becoming more operational, and doing the things that they have actually planned the policy for.
Interviewer:
Have you been able to notice a significant change in cultural behaviors or cultural attitudes towards issues such as cyber within the military from your initial period of being a Signals Officer through the time and now into the private sector?
Bob Stasio:
Yeah, thereâ€™s definitely a lot more emphasis on it. When I was a Military Intelligence Officer, the only kind of cyber training you could get as an Officer, official training, was this course you would go to at Fort Huachuca called the Signals Intelligence Electronic Warfare Course. So of course I took that at the first opportunity, and it was kind of a, I think they called it a sub-designator. It wasnâ€™t really your MOS. It was just kind of a, you know, you also do Signals, too. But you didnâ€™t necessarily get placed in an assignment based on that, right? So the HRC, the Human Resource Command in the Army, could really put you anywhere they wanted, even though you may have this very unique skill. I think at the time it was looked at as more of kind of some additional training you can go through, and from what I can see now, itâ€™s looked at almost as a discipline, as a profession, almost as a doctor or a lawyer, right? So something that you constantly have to train at. You have to go through a lot of schooling to figure out even just the baseline to get into this community, and then you have to learn how to be an expert over time. Much like a doctor has to go to a residency, and go through a fellowship, and continue learning in this discipline. And I think the Army, or the military in general, is starting to see it that way, and the private sector is certainly seeing it that way, too. Itâ€™s become this community of experts in this discipline that wasnâ€™t there, really, ten years ago.
Interviewer:
With the establishment of the Cyber Branch within the U.S. Army, do you feel that thereâ€™s going to be some sort of movement to further professionalize, to further establish? And do you think that is a movement in a positive way, or in a negative way?
Bob Stasio:
Absolutely positive way. Actually, I had just recently heard about the Cyber Branch being

established. I was in the military when they established the MOS for the soldiers, but there wasnâ€™t, you know, an Officer track, and there wasnâ€™t a branch that was completely segregated from all the other components of, you know, sub-components of this. This is absolutely the right direction to go. This discipline is so unique, and you really need to concentrate on it, and move throughout your career, and continue to advance yourself in this, and I didnâ€™t see that when I was in. That was one of the reasons I actually left the military, â€˜cause I really enjoyed this profession, and I wanted to continue doing it, and I had the option of transitioning to become an NSA civilian and really focus on it. And what I did, I could say that when I was 100% focused on this mission, I became a lot better at it, vs. I donâ€™t know, I was kind of doing it almost as a side discipline as a Military Intelligence Officer, and having to look at a track where I may not do that anymore. So I think not only should it - it is a good idea that this is established, but they should almost treat it like they treat the Medical Corps, or the JAG Officers in the military. You know, unfortunately, they have to make some type of dispensation to those types of soldiers. For example, my wife is a Medical Corps Officer. Sheâ€™s a surgeon, and you know, she doesnâ€™t do PT every morning. I think she may do PT twice a year [laughs]. You know, thatâ€™s not the greatest thing, but she has to concentrate so much on being a doctor. She has to work 16-hour days doing surgery, and going to conferences, and taking her Board exams, that thatâ€™s what sheâ€™s concentrating on. And I actually think that the Cyber Branch should be some - you know, we should swivel in that direction in the Cyber Branch as well, just because you really need to dedicate that amount of time to it.

Interviewer:

So youâ€™ve had three fairly dramatic different experiences, first as an Army Officer, then as an NSA civilian, and then having your own private firm, all within the same relative discipline. Could you provide any distinctions that youâ€™ve noticed over the course of these different aspects of your career that might highlight the trajectory of where cyberspace is, or where it might be going, in operational and just general national security terms?

Bob Stasio:

Hm. I would say, you know, over my career, it became less mission-focused, I guess you would say, as far as the community. So in the military, everybodyâ€™s mission-focused. They donâ€™t care about anything else other than the mission, and that was a great feeling. And you stand up these units, you train these people, and everybodyâ€™s focused on just doing the best they possibly can. And then as I transitioned to NSA, I think there was still a feeling of that. I think it was a little less. I think it had a little bit more - there was some more I guess youâ€™d call it politics involved, or maybe efficiencies of mission. You know, they couldnâ€™t do everything all the time - there had to be some decisions made. And then as you get into the private sector, there is just itâ€™s completely about money, right? At the end of the day, a lot of companies will only do what they absolutely have to in cyber security, based on what compliances have been put down upon that particular sector, and theyâ€™ll do the bare minimum. I think thatâ€™s starting to change. I think weâ€™re seeing that itâ€™s no longer just kind of cover yourself in the compliance method. Itâ€™s if you get hit, if you get hacked, thereâ€™s kind of far-reaching implications of that. We can see this in the Target example that happened, with Sony, itâ€™s in the news every day, so I think companies are starting to kind of go back to where the Army is, as being very mission-focused and dedicated to protecting their networks and protecting information at all costs.

Interviewer:

Having had your own private internet firm or computer security firm, did you take any lessons from your time as an Officer in the Army that helped carry your firm and make that firm successful? That really helped to develop the atmosphere and environment of that firm?

Bob Stasio:

Yes, thatâ€™s a good question. You know, I think whatâ€™s really interesting about being

an Officer in the military, especially an Intelligence Officer, I think, is from day one when you get to your training - and at the time, my training was called Officer Basic Course. I donâ€™t know what itâ€™s called now, probably something different. But when I went to my training, they really started to drill into you about strategy. Very much think about the core components of what you want to do first, you know. Even when I was in ROTC, we learned about the Army values, or when we did FM7-8 training, you know, you have to understand the very basics, the tenets of patrolling, or whatever that is - these core principles in everything you do. And when I got into the Intel field, they really trained you, even as a very young Lieutenant, how to plan, how to do MDMP, Military Decision Making Process, and how to apply that to what youâ€™re trying to do. And then after that, you started to lead people right away, so as a Platoon Leader I had somewhere in the neighborhood of 35 soldiers under me at one point. You know, I was a 22, 23-year-old kid. Thatâ€™s an amazing experience. And what I saw in the private sector is not many people get those opportunities. You donâ€™t really get the opportunity to think strategically until you get, you know, maybe 10, 15, 20 years into your career, if youâ€™re in the private sector for a long time, and you may not get the opportunity to lead people for a very, very long period of time. You really learn a lot of things when you lead people. I guess you could say I had the ability, the opportunity to screw up a lot when I was younger, so I can learn that when Iâ€™ve been older. So I think the way I approach things, and also my former veteran colleagues, approach it in a different way. They approach problems a little more strategically, I would say, applying principles to a problem and then creating the solution, vs. doing it the other way around. And they have the ability to really inspire and lead people a little better, from what I can see.

Interviewer:

So based on your wide scope of experience starting as a Signals Officer, moving into the private sector, and now at Bloomberg, youâ€™ve also been noticing the evolution of threat. And now the FBI, the various departments in the Federal Government, including the Department of Defense, have designated the cyber threat as one of, if not the, preeminent threat facing the nation.

Bob Stasio:

Mm-hmm.

Interviewer:

If you could provide your perspective on that evolution, and whether that is an accurate statement moving forward.

Bob Stasio:

Yeah. I think that if you would - thereâ€™s so many graphs and charts up there. If you were to look at how easy it is now to gain access - see, I guess the level, the threshold to get involved in cyber crime or cyber espionage is really lowered to quite a degree. And I think the reason for that is the prevalence of these things called â€œexploit kitsâ€ that have been out there for a little while, so you have people that are very intelligent that are kind of putting all their hacker skills, so to speak, into an exploit kit, and essentially commoditizing their knowledge of hacking and offensive cyber. And theyâ€™re putting it out there to the market, and you know, people are able to buy this, buy this technology, for under $1,000.00, somewhere in that range, and you too can become a cyber criminal if you were to buy that software. And somebody that doesnâ€™t have a very high skill level can then start to use that, so itâ€™s really weâ€™re starting to see that commoditization of cyber crime. Now conversely, on the defender side, on the good guy side, we have not seen the commoditization of cyber I guess expertise, if you want to call it, so the best technology, the best tools, and the best people that are able to fight this cyber crime still cost a lot of money. Really the top, if you look at the Fortune 200, maybe - kind of a bad way to think about it, but unfortunately, this is just how it is - the Fortune 200 have the money to spend on these tools, this technology, create these programs to actually fight this cyber crime, so weâ€™re kind of at opposite sides of the spectrum right now. Really, the best element

designed to fight cyber crime and cyber criminals is the government, as the Department of Defense, in my opinion, and NSA, because theyâ€™ve had to stand up these programs in the last 20, 30 years to protect classified information at all costs. And you know the government tends to spend a lot of money, and we have a lot of very smart people and put them through a lot of training, and theyâ€™re very good at doing this. So you know, we need to figure out how to bring that commoditization of that skill set down on the defender side, and start to bring the threshold for the ability to get into the criminal market up a little more, and bring that technology skill level up, I think.
Interviewer:
Great. So you led me into another question, so Executive Order 13636 -
Bob Stasio:
Yeah.
Interviewer:
Is the defining of critical infrastructure and helping to isolate the role of government -
Bob Stasio:
Yeah.
Interviewer:
In protecting national infrastructure as well as participating in general cyber security. Where do you see the role of government, both on the Department of Defense side as well as in the civilian sections of the government, falling within national cyber security efforts?
Bob Stasio:
Hm. Yeah, so you know 13636, really a lot of what has come out of that in subsequent I guess policy has put DHS in the leading role of a lot of these things. You know, kind of the point agency on a lot of these critical infrastructure components. My opinion is that DHS is kind of undermanned to complete this role. They have to help the commercial sector, all the dot gov components of the Federal government, state, tribal - I mean they have such a huge mission, and theyâ€™re really undermanned in their capacity to actually provide this information to that sector. Now, part of it is because DHS is new, and theyâ€™re growing, and one day theyâ€™ll be sufficient. But what I think is a huge disconnect is NSA and the intelligence community, theyâ€™re able to get some really great information and high fidelity information about cyber, or cyber threats, and really the only mechanism to pass it to the private sector is a relatively convoluted way, through either DHS or potentially the FBI or the Secret Service. And if itâ€™s the FBI or the Secret Service, itâ€™s generally after something has happened, so thereâ€™s warning or theyâ€™re telling this organization that â€œyouâ€™ve been hit.â€ Oh, great, Iâ€™ll know better for next time, but the damage is already done. I think DHS has the ability to maybe be predictive about these attacks and somehow connect the dots. Now, to work with DHS, I think the ISACs that have stood up, the Information Sharing and Analysis Centers, the kind of communities of interest that have gathered around different sectors, thatâ€™s actually probably the best way we have of doing this. Iâ€™ve worked with the financial sector ISAC, and theyâ€™re probably the most mature, and theyâ€™ve set up a SOC, a Security Operations Center, analysts, liaisons that work directly with DHS. So what we really need to do is build that connective tissue between the ISACs, DHS if theyâ€™re going to be the proponent agency, and the intelligence community, to build a bridge to get the highest fidelity information to the people who need it. You know obviously you have to be concerned about classification, sources, and methods. We have to be concerned about protecting the attribution, or protecting the liability of the companies that may be hit, and anonymizing them, potentially, and all those are solvable problems. But I think if we try to maybe push those things in the right direction, it can be very successful.
Interviewer:
So in recent years, particularly since the Edward Snowden releases, thereâ€™s been a very strong backlash against privacy violations and things. And since youâ€™ve had experience inside the government, outside the government, now in the media, where do you see this debate moving, and is the government culpable, or should it be considered

culpable, or does it have a greater responsibility to something larger than privacy?
Bob Stasio:
Yeah, I think thereâ€™s always that balance, you know, between privacy and security, and potentially it swung more towards the security after 9/11, and you had things like the Patriot Act, and the FISA laws were modified a bit, as been released by the government. Weâ€™ve talked about that. My personal belief is that I think we did a very difficult job at NSA in probably the best way we could in protecting peopleâ€™s privacy. There were a lot of safeguards put in place. I think itâ€™s potentially - Iâ€™m not sure about this - but itâ€™s one of the few elements of our government that have quality control and I guess oversight from the Judicial, from the Executive, and the Legislative Branch of government, so there was a lot of oversight. And it was done - you know, being behind the wall, I can tell you that if you were to do something that was wrong and illegal, you would be found out pretty quickly, and there were a lot of safeguards in place.
So not to say that those things couldnâ€™t happen, but I think we did the best we could with a very difficult mission, and I think we prevented a lot of bad things from happening. I think as more things get released from classification, youâ€™ll see that, the public will see that, and I personally think it was worth it. The debate over whether we should have more privacy or more restrictions I think is an absolutely worthwhile debate to have. Thatâ€™s why I love being an American, â€˜cause we can have these debates, you know, but thatâ€™s not my decision to make. I think Congress needs to have that debate, and they need to get input from the American people, what the American people want. From my perspective, the NSA and the intelligence community follows the directives and the laws of what Congress has put out and the President has signed. If those need to change, we should have that debate, and Iâ€™d love to participate in that debate any way I could. But itâ€™s just a really difficult thing that I think was done well, so.
Interviewer:
Since you now work with a company largely associated with media, where do you think the mediaâ€™s role in fostering an environment associated with either cyber security or concepts of how we protect the nation and things move forward from here?
Bob Stasio:
Yeah, I think with the media over the last few years has brought to light the problem a little more. I think thereâ€™s been more of a public interest in cyber, so youâ€™re starting to see media outlets have a lot more reporters that are dedicated to cyber, and people that are really doing a great job digging into the details of a story and not just looking at it at the headline level. I think we need more of that. I think we need to hear about some of these breaches as best we can. You know we donâ€™t want to throw any company under the bus necessarily when they get hacked, but we need to learn from these breaches, and we can learn from these stories, and I think they have a huge role in that, a key role. And if they do it well, and if they investigate it and get their sources right, that we can really learn from that.
Interviewer:
Having this wide background and all this experience, are there any final parting thoughts that you would have that you would try and impart from your experience, moving forward or predicting future actions that might be beneficial for audiences watching?
Bob Stasio:
Sure. I think that going forward, we should really try to focus on the public-private partnership, â€˜cause weâ€™re not going to do this in a vacuum and then silos. The commercial sector is not going to solve this problem in a silo, and the governmentâ€™s not going to solve this problem in a silo, and I think the government can really contribute by really setting the standards and setting the policies of what companies should be doing. They shouldnâ€™t try to burden companies too much with reporting regulations and requirements, but really setting the standard, I think. And then conversely, companies, private sector companies should be a little more open about sharing information about

things that happen to them into the wider community, and I think that could help everybody else. So that kind of collaboration and public-private partnership is really what should be focused on. Weâ€™ve really talked about that for the last five or six years or so, but not a whole lot has moved on that, and I think thatâ€™s something that I would like to see going forward mature a little more than it has.
Interviewer:
Okay. I think that brings us to a conclusion. Is that okay? Sorry, Iâ€™mâ€¦
Bob Stasio:
Thanks.
Interviewer:
Yeah. Thank you. Thank you for coming.
Bob Stasio:
Thank you.