THE MAGIC OF THE INTERWEBS

By Joseph Atkinson, Richard D'Angelo and Ron Granieri August 11, 2020
https://warroom.armywarcollege.edu/podcasts/magic-of-the-interwebs/

Ron Granieri: Welcome to *A Better Peace*, the War Room podcast. I'm **Ron Granieri**- professor of History at the Department of National Security and Strategy at the US Army War College and podcast editor of the War Room. It is a pleasure to have you with us. Public and private experience over the past decade have both taught many of us the possibilities and the challenges that exist in cyberspace. As we have taken advantage of the Brave New World of communication and connection, this podcast is itself only possible today thanks to a variety of cybertechnologies. Political leaders and military planners have tried to develop strategies for maximizing their utility and minimizing their risks, yet even the question of how the two can be separated from each other remains open. We all know that victory in future conflicts will depend on how well the combatants master the skills of cyber security and cyber warfare even as we might not know exactly what that mastery might mean in the rapidly changing cyber domain. Our guests today are two students in the War College Class of 2020 who have studied and worked on these problems, and they're here to discuss them. Lieutenant Colonel **Joseph A. Atkinson** of the US Marine Corps has wide-ranging and diverse experience advising commanders at the strategic, operational, and tactical levels. He served as a regimental Judge Advocate to a Marine Rifle Regiment during Operation Iraqi Freedom and Wing SJA during the Operation Enduring Freedom. He served as the legal adviser to the Deputy Commandant for Information as the Service Advocate for Intelligence Information Operations in Cyberspace. Lieutenant Colonel **Richard D'Angelo** of the US Army has 20 plus years of experience and expertise leading teams in cyber defense in network operations. Able to operate and succeed in dynamic and uncertain arenas that require team building across multiple stakeholders, he has served as Deputy Brigade Commander of the 11th Signal Brigade at Fort Hood as well as in several positions with USCYBERCOM at Fort Meade. He holds a Master's in Public Administration as well from North Carolina State University. Welcome to A Better Peace, gentlemen. It's great to have you both here. So I want to ask you both- what do you think is the most important single thing that you would want your colleagues at the War College and anybody listening in now to know about cybersecurity that they don't already know?

Richard D'Angelo: Ron, I think that the biggest thing is probably you are a part of it. If I could send any message to all of my peers, it starts with that. You cannot simply rely on someone that

has with the military has set aside for cyber expertise to solve all the problems. We're all in cyberspace all of the time, and as a leader in the military, you've got to adopt that and not be afraid of it.

RG: Right. Joseph, what do you think about that?

Joseph A. Atkinson: I agree with Richard, but I'll take it a little step further. I think we take for granted how interconnected we are today through social media to our smartphones, so I don't know if everybody truly appreciates how interconnected everything is and relies on cyberspace. So cyberspace for me is kind of like the glue that enables all these things to happen. It ties our critical infrastructure, health systems, financial systems, everything is interdependent on these systems working together. I don't know if we truly appreciate how vulnerable we can be to malignant actors that can easily get into that space and disrupt how we do business and how we live out our lives.

RG: And so Joe, how did you initially get into this whole question of cyber policy and cyber security?

JA: To make a long story short, I was serving as the Deputy Staff Judge Advocate out at 1st Marine Division in Camp Pendleton, California and my Commanding General then, Major General Dan O' Donoghue, the current J-7 on of the Joint Chiefs of Staff, was my Division Commander and we developed a good relationship for 2 years together. He then received orders to the Pentagon at the same time I did and a fortuitous meeting in the halls of the Pentagon where he was serving as the new Deputy Commandant for Information asked me to come work for him and to provide legal advice and help him steer all the different things that go on at the service level from, you know, contracting to business opportunities to operational type law matters as he was getting back into the information and cyberspace arena. So that was my foray into that world, and I served with him for a year until he left for the J-7 and the current Deputy Commandant and former Marine Forces Cyber Command Commanding General, Lieutenant General Lori Reynolds, is now did DCI. I served for her for the last year before I came to the War College.

RG: Interesting. And Richard, how about you? Not everybody ends up working at CYBERCOM, so how did you end up in this world?

RD: So as a traditional Signal Officer, generally I had not necessarily touched that side and when I got there to go to a Joint Command, it's similar. I listen to Joe, and it's similar. For me, when I worked for Admiral Gilday, who's now the Chief of Naval Operations, he was the Director of Operations for CYBERCOM, and I saw not just him, but several other leaders that didn't come from any kind of technical background and yet were the ones who are leading the

change, to be fair, in combination with people that had worked in the IT field previously. It was that combination of those two sides, and it proved to me the point that the expertise that already exists in the military as far as thinking about strategy it's all encompassed already. Cyberspace is-there's some new and unique differences about it, but the reality is that a lot of the ways that you prosecute warfighting still apply. You've just got to not be afraid of it and think about it and what makes it different, but then how do you still apply those same standards of making success and achieving the ends that you want.

RG: I was thinking about this as I was reading both of your bios and thinking about how you got interested in this. It strikes me that everybody when they entered the service starts doing something that they haven't done before, assuming that you didn't exactly spend your free time leading a rifle platoon before you became a Second Lieutenant. But do you think that there's something particularly interesting about the armed forces and cyber that you have a relatively small number of people who come from specific technical backgrounds but who are sort of drawn into this world based on there either interest or an aptitude that they didn't know that they had before they started?

RD: I think one of the things that makes it exciting to work it in cyberspace, for me as a Signal Officer, is it was the first time that I could actually be in the operations. No one looked at me a little bit different. If I find myself in a division in the Army, at best I'm a support staff guy. There is a real need for that, so I'm not knocking on that, but that's about as far as you can go. In the cyberspace environment, if you're in our Army Cyber, Marine Force Cyber, that actual USCYBERCOM, you can be anything. It doesn't matter. Are you a logistician? Are you a Signal Officer? It doesn't matter to me. Are you good at doing operations? And I think that's what probably made me so excited about that opportunity was this new space that needed new ideas and creativity and that some of my background was still useful. That's why I'll often talk about cyber defense and cyber operations, not necessarily the offensive cyber, because that's not where my expertise laid. But understanding the interchange and interconnectivity between all three of those is what was really exciting.

RG: I don't know if you have compared notes about this, but do you get a sense that there are different attitudes or different approaches to cyber policy between the Army and the Marine Corps? Joseph, what do you think about that?

JA: I think the approach is somewhat similar in a lot of respects. I think where we differ is how do we actually employ it? We had a good working relationship when I was at the Deputy Commandant, which I'll refer to as DCI. We worked very closely with Army Cyber out of Fort Belvoir, so several meetings, exchanging of information, notes, training, how do we implement this out to the operating forces? So I think we're all moving in the same direction, and despite

inter-service rivalries, the relationship between us MARFORCYBER and Army Cyber has been very solid to this point.

RG: This gets to the question of at what stage is there a real sort of joint cooperation in cyber? Is it at CYBERCOM or even between the services at other levels?
JA: For me, I think the jointness starts probably at the Combatant Commands. In the last couple of years there have been liaisons placed within a few of the Geographical Combatant Commands to actually work the cyber process on behalf of the operating forces, the combat commanders, then back to the functional Combatant Commander who makes the decisions on when and how cyber is actually going to be deployed after they do their leveling of bubbles with the Department of Defense and so on.

RG: When you came here to the War College and you brought with it your interest in these matters in cyber, how did you find the level of awareness or appreciation of cyber issues among what is otherwise a very distinguished group of upwardly mobile field grade Commanders- your fellow students at the War College?

JA: For me, I think it was about what I expected. Those that worked at the strategic service level who are exposed to the decision-making, and I'll say the churn surrounding how we're going to approach cyber, how we're going to make it more mainstream, how we're going to incorporate it into the operation or strategic level decision-making in operations. So those individuals having come from that world understood or had a better clarity on what cyber was and what it actually meant. Those that had not worked at the high operational strategic level did not quite fully embrace cyber. There was a lot of skepticism amongst our discussion, especially in seminar and in other forums. But as they got more introduced to it, the War College did a pretty good job of getting introductory-level classes and discussions in the seminar format that allowed them to kind of start to understand how that fits into the tactical, high operational, and even the strategic levels. So I think they turned it around, and just like anybody else would, when you don't know something or you're not familiar with something, there's a tendency to look at it with an eye of skepticism and not fully embracing a new capability that will be something that will be somewhat mainstream for it years down the road.

RD: Ron, I'd like to add on to that. The other observation- Joe and I were in the same seminar, Seminar 11, an awesome group- you could sense that everyone had the appreciation for the dangers in cyberspace, both public and private, but there's not a great understanding of how the military even organizes itself in cyberspace. And so to Joe's point about the War College doing a good job to educate I thought they did a great job of taking the time to say, "Hey, this is how we ourselves execute operations in our structure in cyberspace," but still, we're not doing such a great job at educating about the simple pieces and parts of what is cyberspace. When you think about how easy your average military officer can describe land features, sea features, it's rare to

find someone who isn't an Information Technology person or hasn't worked in a cyber unit who can talk about the physical layer, the logical layer, or the persona layer with any form of basic knowledge. And that becomes a concern because if you can't really think about it in the basic elements, then I don't know how you're going to lead it at the strategic or operational level.

RG: Because you are going to have to lead it when you get to the strategic level.

RD: Absolutely.

RG: It's going to be there. So Rich, you opened the door, so I'm going to ask. What are the differences between those levels that you just mentioned?

RD: I appreciate that. So those three basics?

RG: Right.

RD: The physical layer is everything that enables it in the sense of you have your hard drive, you have wires, you have undersea fiber optic cable, and satellites in the sky. That's a physical thing. As well as we're using the electromagnetic spectrum for those signals across. That's a physical thing, and physical things can be broken and they can they can get intercepted in different ways. Then you have the logical layer. All the things that make up cyberspace in the sense of your operating systems, your algorithms, software, those things, right? Then you have the persona layer which, real quick, is the two basic senses. One is you as a single person have several personas with in cyberspace. Your login to your work computer could be a persona. Your email address at another place could be another persona. So you would see an environment in which one persona can be operated by multiple people or one person can operate multiple personas. You add all those three together, and you get that sense of this thing we're calling cyberspace. All that helps you then see the advantages and the disadvantages of where the vulnerabilities might be.

RG: Whenever you deal with IT they talk about how most of the challenges occur between the keyboard and the chair, right? This matter of the person who doing the work, and it goes back to the point that you both made early on in this discussion that people need to realize that we are all part of cybersecurity, whether we know it or not, simply by virtue of the fact that we use this technology. But what do you think is the biggest hurdle that has to be overcome to help people better appreciate those basics so that, and especially to help future strategic leaders to understand the basics that will allow them to lead and manage cybersecurity and to engage thoughtfully in conversations about it?

JA: Yeah I'll jump in here, Ron. And I want to tail onto kind of what Richard was describing. It ties into the question you just asked, and I think the biggest hurdle is ensuring everybody understands that while cyber maybe a big unknown on how it actually all works and comes together, it's not witchcraft. It's just another capability that has now been placed in the Commander's tool kit to prosecute tactical and operational level operations. It's no different than when you're out there surveying a battlespace. You're looking for what is the key terrain, whether that's on the battlefield, but cyberspace has key terrain as well. So the terms and the concepts don't really differ all that much, and I think once people understand that it's just another capability that we use in our combined arms philosophy and how that can actually help and assist a commander make decisions or prosecute and successfully carry out his missions, then I think we'll have a better feeling and more comfortableness surrounding cyber, how it operates, and what it brings to the table.

RG: It's funny, your comment about witchcraft reminds me. There's a famous quote from Arthur Clarke, the science fiction writer and theoretician about the future. He said that any technology that's sufficiently advanced beyond the understanding of the observer is indistinguishable from magic. If I don't understand it, it might as well be magic. But that is the problem right? If I understand what you're saying, it's that people have to understand that it's something they can understand and that they should make the effort to try to understand it. Is that fair or not?

JA: Correct. Absolutely. What I'm kind of getting at here is it's part of that ever-changing idea that the character of War changes over time while the nature of War kind of stays constant. So you can look back through innovations throughout history and how it changed how we actually prosecute the war on the battlefield. Cyberspace is just the next evolution. It's the next changing characteristic in how we fight. Once we understand that, then it'll be an easier thing to embrace and to actually utilize, especially once you understand how you can employ it in timelines and efficiencies that it brings to the table and really benefit the Joint Force.

RG: We were talking earlier about cyber policy and cyber strategy and how they can be defensive but can also be part of the offensive. What does an offensive cyber strategy look like?

JA: We should be glad that General Nakasone pushed for the change to what he's calling persistent engagement. I was at CYBERCOM from 2013 to 2017 and at that time a lot of the focus was on deterrence and they utilized nuclear deterrence strategy. The idea was that we would hold back our greatest capability and use it in reserve and then said "Hey, we could use it, but we won't" hoping that nobody else would do bad things. And that didn't really work. It turns out in cyberspace you've got to be like a boxer and jab a little bit. You have to put the adversary in an uncomfortable position. Sometimes maybe you do use your upper cut and maybe sometimes that's in reserve, but you have to be out there jabbing and that's what he's calling persistent engagement. That provides an opportunity for some real synergy between all three

types of cyber operations. The military likes to say there's offensive, defensive, and then the actual just network operations. And it's really a legal definition of what the difference between offensive and defensive is as far as what type of effect and the permanence you have in the adversary and then you get the law of warfare which is why you did it. So if you have that persistent engagement and persistent presence from an intelligent standpoint, you've got the adversary in a position that you know they are less able to do what they want, when they want. You now have an opportunity to get cyber dominance when and where you want it, and then you could maybe take some different risks in how you do defense. So I'm a proponent that we should shift our strategy from being more perimeter security focused and defense in depth to data protection focused in the way we do defense in depth. Not to say that the perimeter is not important, but it's not as important in a resource-constrained environment as it is to actually protect the data. So there are ways to go after that in today's technology that we should change towards.

RG: Well, it gets back to a central paradox of information technology, right? The whole purpose of information technology is to make it easier for people to communicate what they are allowed to communicate, when they're allowed to communicate it. But also, the more available you make information to people who are entitled to see it, the more possibilities there are for people who are not entitled to see it to see it as well. I'm curious about the relationship between cyber policy and the older versions of questions of information security and intelligence. You want to read the other guy's mail, but you don't want him to read your mail. That's true whether you're talking about steaming open envelopes or intercepting packets of information. In what ways does current cyber strategy try to deal with the problem of wanting to make sure that it's easier to share information within the force, but also possible to protect that information from prying eyes?

JA: I think what you're getting at there, Ron, is kind of the business, private industry, innovation teamwork we're currently working with, at least when I left the Pentagon to come here to the War College. We were looking at industry leaders- some are big firms like Amazon, Microsoft, and Google- on how we could upload to things like the cloud to have secure repositories of information that would enable us to operate in the geostrategic environment. So in that industry partnership, we were working with them in order to try to protect our data by still giving us the ability to link in so that we can pass our own information. But as you're looking at intelligence in cyber world, again just to echo my points from earlier, we've been using intelligence to supply information since the dawn of warfare. All cyberspace does is just enhance it. It's mutually supporting. In some respects you're going to get intelligence that's human intelligence or through a human chain that can then be utilized in a cyber type operation, or you can gather intelligence through cyber capabilities that can then be used at the tactical in the truly kinetic sense, so they are mutually supporting endeavors or disciplines. Again, we shouldn't just think because it's cyber we're talking zeros and ones or that it's going to change the nature of intelligence work or intelligence fieldcraft.

RG: Rich do you have anything to add to that?

RD: On the other side of that is cyber norms. Right now, there are I guess you can say competing thoughts between some of our near peer adversaries, specifically Russia and China, who have with the Shanghai cooperation, SCO, they set up some ideas of cyber norms, but of course their version would be all about sovereignty and the ability to really control their people. And those aren't the kind of cyber norms that we would like, but that doesn't mean you can't have anything out there. The United States is pushing an idea of some non-binding voluntary norms, so sort of a middle ground where you just kind of acknowledge that we're all fallible. We might make some mistakes, and unfortunately in cyberspace, a mistake such as the NotPetya virus attack that happened a couple years ago and spilled into the civilian space and shut down several ports and caused a lot of damages and monetary effects. So you want to limit those kinds of things and when they happen, you have to call out whoever did it. If we're being persistently engaged, we might make a mistake. And if we do, we ought to be responsible for it and make up for it as we would in the world. When we see adversaries do things in ways that aren't acceptable, which could be "Hey, you can't use that third- or fourth-party person to do a nation-state attack. That's not okay. We caught you. Here's the evidence." The challenge is the willingness to show your intelligence to say "We caught you doing this bad thing that as a group of nations we don't think is okay." But when I do that, you might know how I found out, right? That intel gain/loss is so difficult in this environment. One more on the cyber norms is also internal. We have to look at our own set of authorities because we're finding ourselves in a place where the military might know through intelligence that an adversary is on a commercial entity's network. Sometimes it's even a defense contractors network. We the military might know that they're there stealing information, but we might not be able to do anything because it's not our space. It reminds me of the Coast Guard, right? If a drug dealer is moving cocaine through a submarine in the Atlantic Ocean and a Navy ship comes across it and they know exactly what they're doing, they can't do much about it unless they have a Coast Guard team on board because that's a criminal action the Coast Guard is authorized to take. Do we need to have a cyber type Coast Guard element that is that in-between the two? When you really think about the Coast Guard and what they provide not just for the criminal element, but also think of all the safety features. We accept the Coast Guard that says "Hey, you know what if you want to operate a boat, you have to follow the safety features. If you don't, you're not going to do that anymore and you lose your license and what not." So should we have a process that says "If you want to operate in American cyber space, here are the standards. If you don't, there's some sort of penalty or mark against you."? Obviously, it will take a lot of thought, but it's interesting we don't have that for cyber space.

RG: True. And it's funny, these days we see lots of examples of how it's very difficult for states to admit or want to admit that they might have released or not released a virus into circulation

that could have a negative impact on people. So, in an interesting way the same terminologies we use fits in cyberspace and in the physical world as well. I want to wrap this up- we're just about out of time, but I want to give you each a chance to say something specifically, you touched on it there, Richard, with your comments about some kind of a Coast Guard or some kind of norms. I want to ask each of you briefly to say is there a particular development or innovation in cyber strategy that you think would be important going forward for the future of US National Security, but also for global cyber security norms?

JA: I think what I'll end with, Ron, and I don't know if this will answer your question directly-

RG: That's alright. As I say in seminar, you don't have to answer, you just have to respond.

JA: Love it. Well I agree with some of the sentiments that Richard and you just spoke about on cyber norms and some of the innovations. I think I see it in my community, well not my community as Judge Advocates or legal advisers, but just this idea that authorities are very nebulous, and they don't give us the room to maneuver. What I think we need to realize is that is something between the executive and legislative branches of government to work out, so it's hard to be able to- when we see something in cyberspace like Richard was describing, affecting a corporation or another entity- how did we come about that? How far can we follow that trail? Does it violate Executive Order 12333 that prevents basically us looking at individuals here in the United States from an intelligence purpose? But you could qualify it as intelligence probably. So there needs to be some type of consensus, some kind of adjustment, or maybe it's an executive order with the blessing of Congress or maybe even some type of law that Congress can pass similar to the DSCA or defense support to civilian agencies where we can make some concessions in cyber realm in order to bolster US cyber security both from a national perspective and a private industry perspective since both are so intertwined in how we generate funding and how we generate capabilities to prosecute our defense forward. So I think that's going to be a collective effort that needs to happen at the highest levels of our government, and that the military can then benefit and provide assistance to civilian agencies and private industry.

RG: Great. Thanks Joe. Richard, final thoughts?

RD: You know Joe and I agree almost across the board on all that stuff, so I would say that he's right. In other words, it's the diplomacy and the information and somewhat the economic a little bit maybe on the penalty side, but it's the big diplomacy and big information power that leads the way, not the military. I think the military is doing the right things as far as we've established CYBERCOM and subordinate units, we're headed into persistent engagement. The military is creating its ability to defend itself and affect adversaries just fine, but we have to build those partnerships outside of us and as Joe was pointing out, it isn't just about military cybersecurity or cyber ability. Cyberspace is an international space. We've got partners like Brazil who need our

help just as much in determining how should they better do cyber operations and so as we use diplomacy and information to say “Hey, this is what's not right and it isn't in cyber norm sense,” we also need to use it to say “This is how to do it best.” I think we're on the right track with our national cyber strategy and leading the way and not allowing adversaries who would have cyberspace be used for things that just don't match American values. So in the end, America will defend herself in cyberspace. That's the overarching thing for everyone to understand and as always, that has to be said and then effectuated.

RG: Alright, well it's a good, thoughtful, and hopeful forward-looking way to end this conversation. I want to thank both Joe Atkinson and Richard D’Angelo for joining us for this conversation at *A Better Peace*. Thanks a lot, gentlemen.

JA: Thanks, Ron. It’s been an absolute pleasure, and you too, Richard.

RD: Absolutely. Joe and Ron, I appreciate it.

RG: You bet and thanks to all of you for listening in today on *A Better Peace*. Please send us your comments on this program and all of the programs. Send us suggestions for future programs, and if you subscribe to *A Better Peace* and why don't you subscribe to *A Better Peace*, please rate and review this podcast on the pod catcher of your choice so that other people can find it and subscribe and learn from these conversations. We're always interested in hearing from you, and we're always interested in growing our audience. Until next time, from the War Room, I’m Ron Granieri.