THE FIFTEENTH ANNUAL SOMMERFELD LECTURE[1]

THE STRUCTURE OF THE CYBER MILITARY REVOLUTION

PAUL ROSENZWEIG*

Thank you. Thank you, thank you very much for the introduction and thank you for the invitation. I must say, I am deeply, deeply honored

---

* This is an edited transcript of a lecture delivered by Mr. Paul Rosenzweig to members of the staff and faculty, and their distinguished guests, on September 3, 2013.

Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company, and a Senior Advisor to The Chertoff Group. Mr. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He is a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute. He also serves as a Professorial Lecturer in Law at George Washington University, as a Senior Editor of the Journal of National Security Law & Policy, and as a Visiting Fellow at The Heritage Foundation. In 2011 he was a Carnegie Fellow in National Security Journalism at the Medill School of Journalism, Northwestern University, where he now serves as an Adjunct Lecturer.

Mr. Rosenzweig is a *cum laude* graduate of the University of Chicago Law School. He has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography, University of California at San Diego, and a B.A from Haverford College. Following graduation from law school, he served as a law clerk to the Honorable R. Lanier Anderson, III of the United States Court of Appeals for the Eleventh Circuit.

He is the author of *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* and of the video lecture series, *Thinking About Cybersecurity: From Cyber Crime to Cyber Warfare* from The Great Courses. He is the coauthor (with James Jay Carafano) of *Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom* and co-editor (with Timothy McNulty and Ellen Shearer) of *National Security Law in the News: A Guide for Journalists, Scholars, and Policymakers.*

[1] Established in 1999, the Sommerfeld Lecture series was created at The Judge Advocate General's Legal Center and School to provide a forum for discussing current issues relevant to operational law. The series is named in honor of Colonel (Ret.) Alan Sommerfeld. A graduate of the 71st Officer Basic Course, Colonel Sommerfeld's Army judge advocate career was divided between the Active and Reserve Components. After six years of active duty, he became a civilian attorney at Fort Carson, Colorado, and then at the Missile Defense Agency. He continued to serve in the Army Reserve, and on September 11, 2001, Colonel Sommerfeld was the Senior Legal Advisor in NORAD's Cheyenne Mountain Operations Center, where he served as the conduit for the rules of engagement from the Secretary of Defense to the NORAD staff. He was subsequently mobilized for two years as a judge advocate for Operation Noble Eagle and became a founding member of the U.S. Northern Command (USNORTHCOM) legal office, where he served as its Deputy Staff Judge Advocate and then interim Staff Judge Advocate. He retired from the Reserves in December 2003.

to have been invited to give you the Fifteenth Annual Sommerfeld Lecture.

I am particularly honored because, of course, I am not a military lawyer. Indeed I am not a military man much at all. I practice in the national security sphere, but mostly from the civilian side. So it's quite an honor for me to be invited to speak with you, many of whom know far more about military law than I do.

I assume that the reason I was invited was to bring to this meeting a bit of an outside-of-the-box perspective on issues of cyber law and policy. I hope to honor that spirit by being at least a little provocative if not iconoclastic. My goal at the end of this discussion will be to have given you some things to think about, even if you don't agree with everything I say over the next couple of hours. If you walk away thinking, "Oh, yeah, he has a point there," then that will be a successful event, I think. My plan of attack is to talk for about forty-five or fifty minutes—we have more than that—and then have Q&A for as long as you guys like. If I say anything at all during this talk that is unclear, feel free to interrupt. I am not like an automaton or anything. So please, by all means, if you want to dispute something in the midst of this, you don't have to wait for the Q&A.

As I said, I am not a military man, but I have been to enough military briefings to know that the time-honored way to begin them is to give your audience the bottom line up front so that you all know exactly where I am going. So I have written this one down because I want it to come out exactly right. Here is my bottom line: Much of what the U.S. military is doing to prepare for conflict in cyberspace is misguided. We are, in effect, preparing to fight the last war against the last enemy. We conceive of the conflict as involving a contest against a peer nation states—China, for example. What we are systematically missing is something I would call the democratization of conflict in cyberspace. The capability of nonstate actors, ad hoc groups, and even individuals to compete on an almost level playing field with nation states and to do significant damage to our national security interests. If we do not reconceptualize how we are thinking about cyber security, policy, and conflict, we are going to miss the boat.

To illustrate the point, let me begin by asking you a question. I want you to think about the last ten years, and I want you to confine yourself to the cyber domain, broadly speaking, and ask yourself what has been

the worst U.S. national security failure in cyberspace in the last ten years? I would submit to you that there are really only two possible answers to that question. One possibility, one that fits the nation state model, is the systematic efforts by the Chinese government to conduct espionage against American national security and economic security interests. We have lost a boatload of intellectual property. The Commission on the Theft of American Intellectual Property says that it is on the order of $300 billion in value per year, which is really not chump change, even in the United States.

Meanwhile, the Defense Science Board has issued a classified report—and by classified, I mean it is only on the front page of the *Washington Post*—but a classified report on all of the systems that have been compromised in one way or another by ongoing Chinese espionage. They range from the F-35 fighter to something called nano armor, which I don't even know what that is, but it sounds really cool and I hope we have it, and I am upset that the Chinese are getting it as well.

So that is one area where we have systematically suffered a national security failure, and that is kind of paradigmatically what we have been talking about. If you have listened to President Obama and the Secretary of Defense, that is what they talk about when they talk about the conflict in cyberspace.

But the other answer, the answer that I think is actually more in your minds today, at least in my mind, would be Edward Snowden, right? A single individual who, through his own individual activities, or perhaps with a cadre of a few fellow travelers, has done immense damage to the American national security interests. Think of what has happened just by virtue of Edward Snowden's activities. We have suffered major diplomatic difficulties. There is a significant amount of anger at the United States amongst our allies and friends in Europe about what they perceive to be American spying on their national security interests. They sort of knew that we did it, but now it is out in the open, they can no longer deny it, and they are annoyed.

Even worse, the disclosures have given China and Russia the opportunity to create a false equivalence, if you will, between the nature of what they are doing, which is widespread rampant economic espionage, and what the United States has been engaged in, which by and large has been more traditional national security intelligence activities.

Edward Snowden's actions have disclosed our sources and methods to the great detriment of the United States. As result of this, we have already seen terrorist and other governments change their communication activities so that we are no longer as readily able to intercept their communications and understand their plans. That is major damage to the United States' national security interests. And then, of course, if you have been, oh, say, reading the newspapers you know that there has been a massive domestic political uproar. An amendment to defund completely portions of the NSA's intelligence activity programs, failed by only twelve votes in the House of Representatives just before the August recess; 217 to 205. When in the course of American history has a vote to essentially close down a portion of our national security apparatus come that close to success?

And if you think of that, you understand the scope of the damage that Snowden has done. Think of his contacts, though he is a lone wolf. He acted alone or perhaps with a few others. He had a lot of support from journalists like Lauren Poitras and Glenn Greenwald, and it appears as though he may have had some post-activity support from Russia or China. He is now, obviously, in Russia, and he is reported to have gone to the Russian Consulate in Hong Kong. But the bottom line is that he undertook this level of activity independent, essentially, of anyone else.

The latest report—one report that I saw—said that in a rather unguarded moment, Snowden admitted that he actually took the job at Booz Allen Hamilton for the purpose of collecting classified information with an eye towards eventually disclosing it. So that demonstrates the damage to national security interests that a single individual, or a small group of actors, like Snowden, can do. They are not affiliated with any nation state except perhaps after the fact. They have no sovereign interest that we can address or talk to. They are in essence a combination of political activism, ideology, criminality, and an adherence to some form of anarcho-libertarianism, if you will, and a great deal of narcissism.

So when I speak of the democratization of conflict, what I mean is simply that the tools and weapons of attack are now widely available throughout the globe and the use of force (and, if you'll permit me to say, information is a tool of force that we call information operations)—the use of information force, information power in this domain, is no longer the exclusive province of nation states. That, I think, is the reality of the

conflict in cyberspace, and that is the reality that I do not think our cyber strategy is coming to grips with.

My lecture today is titled *The Structure of the Cyber Military Revolution*. For those who do not know, it is a deliberate evocation of Thomas Kuhn's famous sociological book *The Structure of Scientific Revolutions*.[2] And for those who have not read that, here is a really short and necessarily incomplete summary of what Kuhn said.

Kuhn was asking, "How do we do science? How does something like science develop?" And he said that there are really two forms of science development out there. One form is what we would call normal science. Normal science is the kind of step-by-step accretion of new information. All of a sudden, we can measure something to .001 instead of .1. All of a sudden, we begin to know how much carbon dioxide there is in the atmosphere, and we can measure it as it increases. We have developed theories about what that might mean for global warming. And they can be right or they can be wrong, but normal science kind of starts from a basic set of premises and builds on that one step at a time in a slow accumulation of human knowledge.

The other type of science development that Kuhn talks about is what he calls paradigm shifts. Paradigm shifts are these avulsive yet discontinuous changes in thinking where all of a sudden everything you knew beforehand was wrong—what you thought was right is wrong, and everything that you know now or that you have just learned is a new reality.

The example he gives, the classic example of this, is from astronomy. Ptolemy thought that everything went around the Earth, and he had this whole idea of astronomy that was Earth-centric. Then all of a sudden, along came Copernicus, who made some new measurements and came to the conclusion that the Earth was not the center of the universe. That, in fact, the Earth went around the sun. The sun ran around the center of some universe elsewhere in the world. This was a huge disruption of the astronomy status quo. Nothing is less useful than a Ptolemaic astronomer after this sort of change, right? And that's why people resist them—they are too disruptive.

---

[2] THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (3d ed. 1996 Univ. Chicago Press) (1st ed. 1962).

Paradigm shifts are not limited to science. We see them in all sorts of human endeavors, including military endeavors. Take an example, Naval warfare. There are some Navy men in the room, right?

For 400 years, the entire scope of British strategy was based upon their view that naval supremacy was all that was necessary to rule the world. From the Spanish Armada in 1588 to 1940 in World War II, Britain ruled the waves. Many thought that this was an eternal truth that the Navy would always be the queen of combat and that nothing would ever change that. Then along came the Japanese. There is a very famous video taken by the Japanese after the British had sent the *Prince of Wales* and the *Repulse* out to Singapore as a response to growing Japanese power. The British Admiralty thought that this was enough to deter Japanese aggression in Southeast Asia. The Japanese, with a few very small torpedo planes, more or less, demonstrated that they were wrong. Aviation power was the new paradigm, and those who didn't make the change from a naval-centric power to aviation power were left with nothing but sunken ships on the bottom of the South China Sea.

We are in the middle, I think, of that same sort of paradigm shift in cyberspace. And the shift is the empowering of individuals to act with force in ways that were beyond our conception beforehand.

I would like to introduce you to Max Cornelisse.[3] Max is what I would call a happy hacker. He is a white hat, a Dutch hacker, who sees as his goal, using nothing but his iPhone, exposing flaws in Dutch cyber systems. Here we are in Amsterdam. All of a sudden, Max can turn out the lights. And just to show that he is not working alone—well, we will get to that in a second. I have seen him open drawbridges. I have seen him send mass text messages to everybody in a room hacking a cell tower. Here he is, proving that it is not a buddy in the basement: he does it in another building. So Max, as I said, is a happy hacker. He is a

[3] Since giving this lecture, I've come across some evidence that Max himself may be a fraud. *E.g.* http://ucnim.wordpress.com/2009/01/14/max-cornelisse-amazing-computer-hacker/. On the other hand, most of the capabilities he has exhibited on video have been achieved by real-world security researchers. They can hack into traffic control systems, *e.g.*, *Flaws Let Hackers Control Electronic Highway Billboards*, NEXTGOV.COM, http://www.nextgov.com/cybersecurity/2014/06/flaw-lets-hackers-control-electronic-highway-billboards/85849/, and medical devices, *e.g.*, Jerome Radcliffe, *Hacking Medical Devices for Fun and Insulin*, BLACKHAT.COM, http://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Thus, though Max is, perhaps, a flawed symbol personally, what he represents is the reality of the future.

good guy, a white hat. He does not mean to do any damage. Although, if I were working in the building on a last-minute assignment for my Judge Advocate Course, that would be kind of annoying. But he is not trying to do damage.

But what if he were bad Max or mad Max from Thunder Dome and this was not a random building in Amsterdam, but a hospital, or the New York Stock Exchange, or the Pentagon, or some other critical command and control node? Just as the video of Japanese attacks on the *Prince of Wales* signaled the paradigm shift in Naval warfare, this, I think, is a sign of the paradigm shift that we are in the midst of. Our military strategy, I think, is still fighting naval battles. Max, and other security researchers like him, are torpedo planes.

So let me step back a bit and kind of give you a little architecture of who these types of actors are. And for this I want to give some thanks—this is the product of a bunch of discussions I have had with a very brilliant fellow named Josh Corman who works for Sonatype and spends a lot of his time studying the hacktivist community.[4] So some of what I am about to tell you is the product of discussions he and I have had. So citation is the most sincere form of flattery, and I do not want to claim his ideas as my own.

Who are the combatants in cyberspace? They are not just nation states. They are not Russia and China. From Russia and China, we can expect some form of rationality. We can understand their motivations. We know why the Chinese are stealing intellectual property to jumpstart their economy. We can make some judgments about what would annoy them, what would not annoy them.

In the end they are rational actors just as the Russians were in the Cold War. But in this domain, the motivations of the actors are as diverse as the number of people who are there. And the closer you look, the more unclear it is. There are indeed many actors with many different motivations. I drop them into two different groups. Ones who are chaotic actors, and perhaps it is a little unfair to call them chaotic actors,

---

[4] Mr. Corman is the Chief Technology Officer for Sonatype. Previously, Corman served as a security researcher and strategist at Akamai Technologies, The 451 Group, and IBM Internet Security Systems. He co-founded Rugged Software and IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. *See* www.rsaconference.com/speakers/joshua-corman. He writes a useful blog called Cognitive Dissidents, http://blog.cognitivedissidents.com/.

but what seems to unify them is a disrespect for authority, for hierarchy, for structure, a dislike of it and an effort to work outside of it. And then there are those on the second level, who are more interested in creating terror and war, who are closer to something we would be familiar with and are more like nation states, though not quite.

I say that there are essentially three flavors in the top row of chaotic actors. Hacktivists or anarchist in the purest sense; vandals or criminals, who are spending most of their time breaking things or stealing things; and then most troubling of all for law and policy, people who are in that space for collective action, for free speech reasons, for protecting the freedom of the Internet. The challenge for lawyers and people it that it is really hard to tell the difference among all three of these.

Let's talk about the first group: Hacktivists. To my mind, they are cyber insurgents with a bit of an ideological twist. If you don't believe me—these are just some of the names of some of the people who are from some of the groups. If you don't believe me, here is Barrett Brown. Barrett Brown is the self-described cyber strategist for Anonymous, which is an ad hoc collection of generally anonymous cyber activists. Here is what he said: "It's a guerrilla cyber war, that is what I call it. It is sort of an unconventional asymmetric act of warfare that we are involved in."[5] If that is not enough, Anonymous has posted a manifesto online. You can Google it and pull it down and listen to it. This is what they say: "I declare the global space we are building together to be naturally independent of the tyrannies and injustices that you—that's governments—that you seek to impose on us. You have no moral right to rule others, nor do you possess any real methods of enforcement we have true reason to fear."[6]

This is tantamount to an insurgent's declaration of war. And if you kind of doubt that, you probably didn't know this, but we're at war. Anonymous has declared war on the United States. They did that in a manifesto published in February 2012, and they called on all of the citizens of the United States, that is all of us in the room, to rise up in rebellion. You didn't get that message did you? But that is what they

---

[5] Michael Isikoff, *Hacker Group Vows 'Cyberwar' on U.S. Government, Business*, Mar. 8, 2011, http://www.msnbc.msn.com/id/41972190/ns/technology_and_science-security.

[6] *Anonymous to the Governments of the World—Web Censorship*, YOUTUBE.COM (Apr. 25, 2010), http://www.youtube.com/watch?v=gbqC8BnvVHQ. Anonymous refers to itself in the singular, even though it is a collective group of people.

see as the struggle. It is eerily, to my mind, eerily similar to Osama bin Laden's declaration of war against the United States in 1998, or 1999, three years before 2001. So this is an insurgency group, and they use insurgency tactics. For example, they intercept communications.

LulzSec famously intercepted a conference call between the FBI and Scotland Yard, the topic of which was the prosecution of LulzSec and Anonymous members and then disclosed that capability as a means of sowing confusion and doubt amongst the FBI and Scotland Yard as to the security of their communications.

In recent months, the conflict between ordered liberty governments, like the United States, and cyber hacktivists has just ramped up in more ways than we can possibly imagine. Here are a few. Consider The Onion Router. The Onion Router (TOR) is an Anonymous browsing mechanism. The NSA tried to hack it. Why? Because that was how groups like Anonymous and LulzSec were communicating without being subjected to surveillance and tracing by government authorities. It was recently reported that the NSA hacked one end of a chain of that type of anonymous communication, enabling them to countersurveil anonymous groups like Anonymous and LulzSec.

The effort is not just limited to the United States—in Belarus it is a crime to own a map of the country. It is an authoritarian communist country, and they want to keep secret all of their government facilities. The social activists in Belarus opposed to this went on social media, pulled together all of the things that they could get from Google Maps, Instagram, Facebook, Twitter, and built a map of Belarus that is now publicly available outside of Belarus. How did Belarus respond? By making it a crime to access any website that is not a .be, that is the Belarus country code, .be website. That's punishable by life imprisonment, if not death. So this is the contest space between social activist in Belarus and the Belarusian government.

And if you think we are immune, I read a recent report that there are members of Anonymous in the military. A bunch of NCOs at Fort—I am going to say this wrong—Fort Huachuca. Huachuca in Arizona, which is one of our cyber bases where we do a lot of this. Apparently, several of the NCOs said that they are also participants in Anonymous. I don't know whether they are double agents on our side, or triple agents on Anonymous's side, but this has all the makings of an insurgency conflict between us, the United States, or Western governments

supporting ordered liberty, and this crypto-anarchistic kind of libertarian group over here.

But it's not a monolith, sometimes they'd trend over into criminality. We have seen a lot of criminal activity on the network, much of it is not ideologically motivated at all. Purely criminal groups like the Russian Business Network, RBN, and Ukrainian criminal groups are into nothing more than stealing money for their own private gain. But at the same time, groups like Anonymous and LulzSec, they tend to drift over into that realm when they get into vandalism, I would call it.

Recently, just basically as a joke, LulzSec started writing graffiti on the CIA's website. Not a significant or existential threat, didn't really do any damage, but it's like tagging it: "We were here. LulzSec was here." They did the same thing to the Church of Scientology. Apparently, the Church of Scientology is something that the anarchists really dislike, and so you can imagine why. But at the same time, they are also about Internet freedom, the idea that this new space is a place where political freedom, speech, new ideas, innovation—this is the good side, if you will, of the revolution.

For example, Anonymous gave some tools to the people who were behind the Arab Spring in Egypt, so that they could avoid the shutdown of the Internet by the Egyptian government. That actually sounds like something we would do, we would be in favor of as well. They, likewise, have given tools to the Falun Gong in China, which is a dissident group in China that is opposing Chinese authoritarianism. So we can't tell exactly where they are coming from. And some of the actors in this space are actually independent wild west sheriffs on the network who are trying to defend the network against people that they see, like Anonymous and LulzSec, who want to take it down.

One of my favorites is the Jester. The Jester is a former Army or Air Force Special Ops guy; nobody's quite sure. He is ex-military for sure. He has at least disclosed that. And what he does is he counterattacks the command and control centers of groups like Anonymous and LulzSec when they get too far out of line. He doesn't do it on orders. He does it as a hobby, if you will, or as his independent retirement activity. Some people retire from the JAG Corps and go back home and do county law; he retired from special ops and became the Jester, which is quite something. The Happy Ninjas is another such group that runs around the Internet wacking the bad guys—at least their perception of the bad guys.

And then, of course, some of the actors are kind of pseudo-state actors like Al Qaeda, the Russian Patriotic Hackers, and if you have been reading the news, units of the People's Liberation Army, PLA. Unit 61398 in China is essentially a top secret unit of the Chinese, and they sometimes look like Anonymous, and we can't tell the difference amongst all of the various actors in this space.

I did this slide three days ago, four days ago; if I had to redo it today, I would put the Syrian Electronic Army (SEA) up there somewhere. I am not sure where—probably down in the political motives group, but maybe up in the anarchistic group, in the middle; I do not know for sure. But the SEA have recently acted against American interests—and we aren't sure if Assad is behind them or not.

So now that we know who these actors are, what does that mean? So far, I have just been kind of descriptive. What does that mean for our policy? Well, first let me talk a little law because, after all, we are at a law school, and this is a conflict space, and you have just finished the section on operations law. You know a lot more about this than I do, guaranteed. You live, sleep, breathe *jus in bello* and *jus ad bellum*. Necessity and proportionality are by now, after how many weeks, four, three, coming out of your ears. The good news is that there is an emerging consensus that those laws, the international humanitarian laws, the laws of armed conflict, apply just as readily in cyberspace as they do in the physical, kinetic world.

Recently, a group of experts convened in Tallinn, Estonia and wrote something we call the Tallinn Manual,[7] which was an explication of how traditional laws of armed conflict, traditional rules from the Geneva Convention, would be applicable to nation states conflict in cyberspace. This is good. This is a wonderful achievement, and if you wind up being assigned after this to U.S. Cyber Command in the Staff Judge Advocate office there, you will imbibe the Tallinn Manual every day. We also saw, quite luckily, after four or five years at the UN, the Chinese government just made an announcement that they agreed that International Humanitarian Law (IHL) and the laws of armed conflict applied to cyber conflict.

---

[7] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge Univ. Press 2013), https: www.ccdcoe.org/249.html.

I don't know what would have applied if that hadn't applied, but at least we have an agreement amongst the nation states that that's the set of rules we are going to apply to cyber war.

But if you bought anything that I have said so far about the paradigm shift that's happening in cyberspace, you know that is barely the start of the story. What about conflicts with nonstate actors? International humanitarian law is reduced is defined by state-to-state conflict. There is a limited amount of international law that applies in non-international armed conflicts. Again, stuff you all know better than I do. Things like Common Article 3 of the Geneva Convention and things like that. But the fundamental question for operational lawyers in the cyber domain for the next five years—fair warning, this is great thesis topic area—is what sort of law applies to, say, our conflict with Russian Patriotic Hackers, or the Syrian Electronic Army. We have read—I have read—the *San Remo Manual*,[8] which is the equivalent for international law that applies to all non-international armed conflict. And I have to tell you, I have absolutely no idea, no idea whatsoever, how military lawyers are going to apply that law, which applies to non-international armed conflicts in the kinetic, in the physical world with boots on the ground—how that's going to be applied next year to a conflict in the cyber domain against a nonstate actor.

In that one space, there are literally five dozen subtopics that you can ask. What do the rules—what's a protected person? What is an appropriate weapon? What is a good targeting decision? How do you do that when the other guy is not a nation state actor? He is not wearing a uniform, and you are not even sure of his motivations. That is the fundamental question, and it is going to be a great specialty for somebody in this room. You write that paper now and two years from now, when we actually have to answer that question, the Army is going to look around and say who knows this stuff? And they are going to pull out your paper from the files here at the JAG School, and you will be the pocket expert. I highly recommend it.

Let me turn from that to give you some sense of what some of those questions would be; some of the policy issues that are going to drive the counterinsurgency in cyberspace conflict. Some of this I have said

---

[8] SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (12 June 1994).

before in an article I wrote for the Heritage Foundation.[9] And if citation is the most sincere form of flattery, then self-citation is an even more sincere form of flattery. I think that there are three factors that have to guide our cyber strategy that we are not necessarily paying as much attention to as we would like. The first is that asymmetric conflict is here to stay. Nonstate actors with near equal power to governmental actors are going to be the rule, not the exception, going forward. They can serve time as proxies as the Russian Patriotic Hackers do for nation states, but they aren't nation states themselves.

Second, currently, nonstate actor capabilities are limited. They can't take down the electric grid in the United States, but that's not a situation that's going to be around for very long. Five, maybe ten years at the outside before nonstate actor capabilities become almost equivalent to nation state actor capabilities. Max Cornelisse and people like him say that the time where our nonstate actor opponents are nothing more than kids running around playing war games—you know that old movie, right?—that's not going to last for very long. We have a window of opportunity to get our strategy right now, and we need to take it.

Third, attribution is the hardest part of the game. Knowing who the other side is and what their motivations are is the most difficult challenge of all. I saw an interview with the Syrian Electronic Army just the other day, in which they said they have got nothing to do with Bashar al-Assad: "We don't even like that guy. But we are on the side of the Syrian people, and if the United States launches weapons against the Syrian people, we are going to act on behalf of the Syrian people."

How do we deal with that? Who are these people? What are their true motivations? That's not something that we can fix technologically. In the end, we can get better at it, but it's not something where you are going to have the same confidence in identifying the enemy, or the opponents, as you do in the kinetic world where it's very clear that the tank was right over there, and you can shoot right back at him.

So my conclusion is that instead of technical fixes, what we need to do is to develop cyber counterinsurgency law and policy that uses all of the techniques in our arsenal to fight this kind of new opponent. This is

---

[9] Paul Rosenzweig, *Lessons of WikiLeaks: The U.S. Needs a Counterinsurgency Strategy for Cyberspace*, HERITAGE FOUNDATION, Backgrounder No. 2560 (May 2011).

going to be similar to the lessons we just relearned in Iraq, in a kinetic conflict. It's going to require not big disruptive military activity, but things like integrating the military and civilian activities, collecting intelligence, building host nations security, things like that. It's going to be military, intelligence, diplomatic, law enforcement, information, financial, and economic power, all of them will come into play.

Let me talk a little bit more about some of these elements in detail and try to identify some of the policy and legal challenges that are going to come about. If you accept my view that this is a counterinsurgency, the first thing we are going to need is to collect intelligence on our adversaries. And because of the technical difficulties, that's probably going to be human intelligence. That's probably going to be activities to try to infiltrate their organization so that we understand their motivations: so that we can learn who they are, foster a diplomatic campaign against them by naming them, and shaming them if we want to, so that we create divisions amongst them through misinformation if we have the opportunity.

I trust you can see immediately that that creates a lot of legal problems, not the least of which is that I do not even know whether any of the members of Syrian Electronic Army are Syrian Americans, residents here in the United States who have a political viewpoint that they are trying to activate through this action. I do not know if they are in the anarcho group, the political motive group, or if some of them might be in the Internet Freedom Group, and may be exercising protected First Amendment speech rights, or acting here in the United States in a domain where different sets of rules control military and intelligence activities. Nonetheless, in the absence of actual intelligence, we are not going to be in a position to be able to really understand what they want.

Second, we are going to have to build host nation cyber capabilities. In 2007, Russia attacked—Russian hacktivists attacked Estonia. Basically, they took the entire country off-line for a number of weeks. In response, the United States has provided a great deal of technical assistance to Estonia, where Tallinn is, and now they are one of the most cyber-capable nations in the world. Our network of Western actors—ordered liberty western actors, and that includes states like Japan and Australia who aren't in the West—is only as strong as its weakest link. The network is globalized and an attack that comes in through a server in France, before it hops over to a Department of Defense (DoD) server in

Germany, is just as dangerous as a direct attack against the German server itself. So we need to build that capability.

Likewise, we need to build public/private sector capabilities. Because 95 percent of the network is owned and operated by the private sector. Ninety percent of U.S. government military unclassified communications go over a civilian network right now. When you send an e-mail in the unclassified network, it goes through AT&T, or Verizon, or whoever the military server is. That's a problem for us. In addition, the civilian network is something we are critically dependent upon for everything else that supports the military function, like the lights in this room. Even though we are dependent upon these lights, the military has no real formal role, domestically, in protecting—what's the name of the local energy company—Virginia Electric Co.? Dominion? in protecting Dominion against cyber attack.

We need to deny the cyber insurgents safe haven. Max Boot just wrote a wonderful book on insurgency in general called *Invisible Armies*.[10] One of the things that he said was a key to the success of an insurgency was its physical safe havens. Vietnam, think Laos and Cambodia for the Vietcong. The Taliban had the Federally Administered Tribal Areas (FATA) in Pakistan. There are cyber-safe havens out there right now in China, and in Russia, and in the Ukraine. And we need to exercise either military, diplomatic, legal, economic, financial tactics to convince those countries to cease being cyber-safe havens where cyber insurgents can stay.

We need to recognize that some of this, the Internet freedom part of this, is actually a legitimate political viewpoint. I mean, it's quite simple. We need to think about how to win the hearts and minds of that group of people. We need to know how to break off the Internet freedom people on the left from the anarchists and the criminals on the right. The U.S. government is, unfortunately, seen in that space as an exceedingly authoritarian institution that wants to restrict the freedom of information and free speech.

Aaron Swartz is a quite famous case who was involved in what's called the Freedom of Information Movement. He wanted all of the journals, scientific journals, to be freely available to everybody. He was

---

[10] MAX BOOT, INVISIBLE ARMIES: AN EPIC HISTORY OF GUERILLA WARFARE FROM ANCIENT TIMES TO THE PRESENT (Liveright 2013).

charged with a crime for stealing them, and he committed suicide. His name is a *cause celebre* in the Internet and information freedom space, amongst the people who should be our natural allies. I am not going to argue the merits of his criminal prosecution, but through a very underhanded sort of set of activities, we essentially drove a number of people who might be like-minded to us in general away from the United States' point of view, at least for little bit of time.

We need to build resiliency. When you build—when you have an insurgency in Iraq, one of the first rules that I learned was rebuild the road so that the insurgents can't claim a success in disrupting the economy of the area. We need to have the cyber equivalent to that. And you will read every strategy in the U.S. government, military or civilian, and you will not find a single mention of resiliency as an important factor in the cyber domain. But we should be striving for a world in which the Syrian Electronic Army, who recently took down the *New York Times* for two or three days, can only take it down for an hour, or 30 minutes, where we can bring it back up as quickly as possible.

And then, finally, I could go on, but we need a theory of offensive of action. The general theory of kinetic offensive action against nation states is one of maximum destruction of the enemy's forces. You want to eliminate its factors of military production. In insurgency warfare in the kinetic world, the physical world, that's very different. You want to find key havens, capture and kill key leaders, and isolate the enemy in domains away from where the civilian population is. We need to build the same sort of targeted cyber tool capability in the cyber domain. Again, another classified leak in the *Washington Post* suggests we are trying to do that, but we are doing it on the intelligence side, not at U.S. Cyber Command.

Finally, we need to do all of this consistent with our own values, the rule of law, and appreciation of dissent in the First Amendment. By contrast, we don't want to be like Belarus, where the response to social media innovation is a lifetime imprisonment or the death sentence.

One more critical point I'll make, and this is one not of strategy but of structure. Five years ago, I wrote an article about the organization of American government in cyberspace calling for more centralized federal

government control.[11] I wanted a really strong cyber czar who had a budgetary authority and directive authority over as much of the government as we could to centralize a response.

I was wrong. I repent and regret those words. This is the most distributive dynamic domain that I know of. There are more than two-and-a-half billion people and more than a trillion things connected to the network across the globe. It changes on a, literally, hourly or daily basis. The advanced, persistent threats that are intruding on the DoD's .mil computers today did not exist six months or a year ago. They are newly built, purpose-built for that thing. The last thing we need is a centralized hierarchy that is going to go into conflict with a diverse, multifaceted, morphing opponent in a battle space that changes every day. If I am right, that the cyber conflict is a paradigmatic shift, the last thing we need to do is build a hierarchy with a top-down structure.

Now, we are here at the Judge Advocate General's School, it is part of the big Army. The big Army does a lot of things great, but one of the things it doesn't do well is turn quickly. The Army's turning radius is the same as that of an aircraft carrier, not of a Corvette. We are in the process of building, at cyber command, big cyber. It's a sub-unified command that reports to STRATCOM, and there's already proposals to turn it into an independent command of its own. And you know exactly what that means in Pentagon structure. We are going to have a big hierarchy with lots of rules, reporting to the top, acquisition rules, staff judge advocate who drives rules all the way down. In this battle space, I think we need a cyber force that's much more akin to special operations. Something that's lean, quick to react, flexible, with flat administrative structure and, essentially, the equivalent of an "A" detachment in the special ops branch.

Think about where we are right now. President Obama is in the midst of thinking about a physical attack on Syria. What's going to be Syria's cyber response? The Syrian Electronic Army has already told us they are going to counterattack. What do we know about their capabilities? Nothing. We don't have anybody on the inside. What are

---

[11] Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*, *in* NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (National Academies Press 2010).

their likely targets? We don't know, because we don't have any sense of what their capabilities or any intelligence on their targeting methodologies or what they think are our soft points. Do we have targeted weapons that can find the Syrian Electronic Army's command-and-control servers and take them out without taking offline the entire Syrian electric grid? I don't know, but I suspect not. Do we want to take down the entire Syrian electric grid? No, because that's what the rebels are also using for their command and control and that's what the civilians are using to ameliorate the horrible effects of the chemical warfare that they are undergoing.

What response and resiliency measures do we have in place here in case the Syrian Electronic Army does attack? I don't know, but very little I suspect. In short, the entire paradigm of the cyber aspect of our anticipating kinetic attack on Syria is really a counterinsurgency response to what we see as potential counter activity by the Syrians.

Let me make two final points very quickly. The first is I have left out of this discussion completely one other set of important actors out there, corporations or the private sector. If you don't think that Facebook, Google, Microsoft are big players in this space, think back to January 2012. I don't know if you remember, but the entire Internet was blacked out for a day by these companies in protest of a bill that they didn't like that was being considered in Congress.

If an Iranian had done that to us, we'd call that a cyber intrusion or possibly even a cyber attack. But when Google does it to itself, what do we call it? And imagine if they decide tomorrow that even if Congress authorizes an attack against Syria, they don't like that idea, so they say they are going to blackout the network anyway? Because the means of our communication are in their hands, they have an important role here.

The other final point I would end with is an admonition to humility. Nobody who works in this environment has any real certainty. Oliver Cromwell is reported to have said back during the War of the Roses to churchmen in Scotland: "I beseech you in the bowels of Christ, think it possible you may be mistaken."[12]

Now, I have got to think about that. Perhaps China really is the main threat and my worry about Anonymous and LulzSec is wrong. Perhaps

[12] Letter to the General Assembly of the Church of Scotland (Aug. 3, 1650).

nation states will, *ala* Belarus, crush Anonymous and LulzSec. But as long as the United States and the West are limited by our respect for the rule of law, I do not think we are going to undertake the types of activity against those groups that would be successful in crushing them. The Russians might, but we would never do that.

So what I see is that the change is real. Max Cornelisse and his ilk are a harbinger—power and force are being democratized, and we are not ready for it. So that is my bottom line. In my judgment, we are in the midst of a Kuhnian paradigm shift from a time when nation states have a monopoly on the use of significant force to a time when destructive potential in cyberspace is being increasingly democratized. If I am right, then our current military strategy in cyberspace is focused on the wrong enemy at the wrong time, using the wrong tools and with, I think, the wrong hierarchy. And that almost certainly means we are setting ourselves up for a failure of a sort that I cannot even imagine.

Again, I have overstated the conclusion somewhat for rhetorical effect, but the outlines of the problem are there for anyone to see. I think it is just that we are not looking.

So with that, I thank you for the honor of being invited to give you this lecture. I very deeply appreciate it, and I will look forward to speaking with you and answering your questions.