THE BROOKINGS INSTITUTION

FALK AUDITORIUM

CYBER WAR WILL NOT TAKE PLACE, OR WILL IT?

Washington, D.C.

Monday, September 9, 2013

PARTICIPANTS:

Moderator:

PETER W. SINGER
Senior Fellow and Director, Center for 21st Century Security and Intelligence
The Brookings Institution

Featured Speaker:

THOMAS RID
Reader in War Studies
King's College London

Panelists:

IAN WALLACE
Visiting Fellow
The Brookings Institution

JASON HEALEY
Director, Cyber Statecraft Initiative
Atlantic Council

* * * * *

P R O C E E D I N G S

MR. SINGER: Hello, I'm Peter Singer, director of the Center for 21st Century Security and Intelligence at Brookings and we're delighted that all of you are joining us here for this important event.

I'd like to begin with a quote. "Be it resolved by the Senate and House of Representatives of the United States of America and Congress assembled, that the state of war between the United States and the government of Bulgaria, which has thus been thrust upon the United States, is hereby formally declared." This June 5, 1942 text describes the last time that the United States actually declared war.

This declaration covered the minor axis powers who were feeling left out after the first post-Pearl Harbor vote to go to war against Nazi Germany, Japan, and Italy.

Now, in the years since, America has sent troops that places that range from Korea to Iraq, we've launched air strikes in places that range from Yugoslavia, Cambodia, Pakistan, maybe even soon, Syria, but the United States has not formally declared war on another state since 1942.

Now, wars have been declared on various other things such as President Johnson's 1964 "Nationwide War on the Sources of Poverty" or Nixon's 1972 "War on Drugs". Now, notice the date, 1972. We were

willing to declare war on drugs, but not on Cambodia. And what more recently some conservative leaders have claimed as a secret "war on Christmas".

Now, the disconnect between an actual state of war and the far more frequent uses and misuses of the concept of war is important to keep in mind when discussing a term like cyber war. War is used to describe an enormously diverse set of conditions and behaviors, from a state of armed conflict between nations, like World War II, to symbolic contestations, like recently New York City's "war on sugar".

Now, as for cyber war, the term has been used to describe everything from a campaign of cyber vandalism and disruption, like the "Russian-Estonian Cyber War", to an actual state of warfare using cyber means. Indeed, in 2010, *The Economist* ran a cover story on "Cyber War," which portrayed it as everything from military conflict to credit card fraud.

So, the key question of cyber war may not be what it's good for, absolutely nothing, say it again if you want to, but rather, what is cyber war and whether it will happen.

Now, as many of you are aware, the Brookings Center for 21st Century Security and Intelligence has been making a dedicated effort to raise the level of discourse and research in this important new area of

technology and politics. Now, at the start of summer, we had the pleasure of hosting General Dempsey, who spoke on the full range of cyber issues that he was dealing with as Chairman of the Joint Chiefs in a way that previous chairmen weren't having to face.

And in that session I asked him on his view of when a cyber war would start and how would he even know. And the answer he gave was, "I think that the decision to declare something a hostile act and an act of war is certainly one that resides in the responsibility of our elected leaders, with my advice, but to your point about a cyber war, I do think that there are capabilities out there that are so destructive in nature, and potentially that they would, it would be very difficult not to see them as acts of war. We haven't experienced one, but I know the capability is out there."

Now, Brookings is a place that takes great pride in convening views from multiple perspectives, something I think has become all too rare in the think tank world today, and so we're here to launch a new book in the field that in many ways acts as the other side of that question.

First we're going to hear from Thomas Rid, who is author of that book, *Cyber War Will Not Take Place*. He's worked at various research institutions, including the German Institute for International and Security Affairs, the Woodrow Wilson Center, RAND, and is now a non-

resident fellow at Johns Hopkins SAIS and a reader in the Department of War Studies at Kings College, London.

His new book has been described by *The Financial Times* as "A well timed bucket of cold water on an increasingly alarmist debate."

After Thomas we'll hear from two experts who are ready to put that argument back into hot water. Jason Healey started his career at the U.S. Air Force where he was the founding member of Joint Taskforce Computer Network Defense, the world's first joint cyber war fighting unit. Now, notice it's interesting, we get these bios, so we have everything from *Cyber War Will Not Take Place* to a member of the first cyber war-fighting unit. He has degrees from Air Force Academy, Johns Hopkins, and James Madison University. He went on to work as director for Cyber Infrastructure Protection at the White House, and with Goldman Sachs, where he helped respond to cyber attacks and manage crisis response and business continuity.

He's currently the director of the Cyber Statecraft Initiative at the Atlantic Council, currently editing the first ever history of cyber conflict, *A Fierce Domain: Cyber Conflict 1986 to 2012*.

And finally we'll hear from Ian Wallace, who's had a distinguished career with the UK Ministry of Defense, including as team leader for financial and requirement scrutiny of air, maritime, and nuclear

programs, political advisor appointments in Iraq and Kosovo, and most recently as defense policy and nuclear counselor at the British Embassy where he served as a key liaison with the U.S. government on these issues.

He's now out of UK government service and he's with us here at Brookings as a visiting fellow in cyber security issues focusing on the international dimensions of cyber security, including especially for military forces and the public and private sector.

So, it's a great line up for an important debate and we're really delighted to have them join us and you joining us as well. Tom?

MR. RID: Thank you, Peter, for this very kind introduction.

When I was hired in the Department of War Studies about two years ago, my Head of Department, at the time, Mervin Frost, introduced me to colleagues and others as "This is Thomas Rid. He's our cyber war expert," and I always cringed when he did that because, you know, you have to remember that the persons also working in the Department of War Studies study the First World War, the Battle of the Somme, the real thing, not the metaphor.

So, the spirit of this book was really to educate my boss in order not to introduce me as the cyber war expert, by trying to find a way to distinguish between, as Peter pointed out, between the metaphor and

the real thing, because obviously there are cyber capabilities that can be highly destructive and they may deserve the label “weapons of war” -- of course there are capabilities that deserve to be called “cyber weapons”, if you like, but the key challenge is to find out what is a cyber weapon and what is an act of -- a use of force in cyberspace and what is not.

So, the book starts out by asking the question, really, what is war, and going back to classical, strategic theory that is time tested. And then the answer is, well, war, first of all, has to be violent, or at least potentially violent. If it’s not violent, then we’d be using a metaphor, like the War on Drugs, as it were. The second feature is that war has to be an act of war, the use of force has to be instrumental in the classic expression that force -- an act of war is using force to compel an enemy to fulfill our -- to change his or her or their behavior. So, it has to be instrumental. And the third feature is that an act of war has to be political in the sense that somebody claims credit for it. And that, of course, is hinting at the attribution problem.

Now, the attribution problem, of course, is on our mind in these days and weeks in a rather different context, in the use of chemical attacks in Syria, which in historical terms is the exception. It’s very rare that sophisticated weapons systems are used in conflict, in war, and nobody claims credit for it. Usually, I mean, almost always it’s the other

way around.

Of those three characteristics, violence, instrumentality, and its political feature, the violent aspect is by far the most interesting one if we are talking about the use of cyber capabilities. Why? Because if we carefully look at the empirical record, at the history and at the technological possibilities, and that, by the way, is the spirit, the underlying motive of the entire book. I think we have enough speculation and near fictional scenarios in this debate already, we don't need even more.

So, contrary to its title, I'm actually not talking about the future, I'm talking about the past, and what we've seen, and the technical possibilities.

Using cyber capabilities is not producing more violence, as this label of cyber war would lead us to think, that's the core argument, it's not producing more violence, it in fact takes -- oftentimes takes violence and physical risk out of the question. So, I'll very briefly give you three reasons, three illustrations of this argument, and I think then we should already move into the discussion.

First, perhaps the most consequential use of computer attack is sabotage. Attacking a system, and when I say system, it can be all sorts of things, in order to degrade its efficiency or possibly damage the system -- sabotage, that's sort of where sabotage comes from in the early

20th century, withdrawing efficiency from a system.

In previous times, if you sabotaged a system, say, by throwing a monkey wrench -- that's the American equivalent to the sabot, the French wooden shoe that strikers would throw into machines, if you like -- if you throw sand or mechanical devices into a machine in order to sabotage it, in that classical context, then you would damage the machine, you would damage property. You would actually, if you like, do something violent because it damages something mechanically, physically.

Today, in the context of cyber attacks, it is easier to distinguish between violent sabotage, because for violent effects you would have to weaponize the target system, like Stuxnet did, with very arcane payloads. It's easier to distinguish violent sabotage from nonviolent sabotage. So, for instance, the Saudi Aramco attack in 2012 and the Saudi oil company was sabotaged, was entirely nonviolent, but it was highly effective, of course.

So, that is an interesting distinction to make that nonviolent sabotage has become possible and probably also easier. Violent sabotage may have become more, shall we say, intelligence intensive. That's a point to be discussed, perhaps later. Second, very quickly, intelligence operations, espionage operations, here also I think in this day and age, as we are learning as a result of the ongoing revelations post-

Snowden, intelligence operations and espionage in the 21st century can exploit this new technical environment in ways that were practically unimaginable only a generation ago. (Inaudible) before the Internet was already impressive, but with the Internet the possibilities of (inaudible), of extra trading information from a target, without the target noticing, are drastically increased.

So, again, the same thing, in order to exploit espionage in the cyber context, if you like, you can --probably you have to take less risk, you may not even have to infiltrate physically -- you may not have to infiltrate a target to plant bugs, you may not have to recruit agents in order to help you on the ground. It can be done remotely. Not always, but often. That also makes it easier -- it, in a way, takes out physical risk, takes out potential violence, not adding more to cyber operations.

And very quickly, the third feature if you look at subversion, is undermining political authority. Here we've also seen that a new communication environment can be used to undermine authority effectively without first resorting to political violence, without going to use terrorist tactics in order to undermine the legitimacy of a government that's very much taking us into the realm of counterterrorism and really counterinsurgency theory, but you can use -- you can influence public opinion even if you're not a powerful media organization, in more effective

ways today. That's an entirely separate problem, subversion.

Now, here also violence becomes more problematic blurred. This, in a nutshell is the book's core argument that violence changes its shape.

Let me, perhaps, close my short opening remarks by responding to an argument that I know from experience at least ten people in this room now have in their head. They think, well, maybe we should adapt the notion of violence, maybe we should adapt the notion of what counts as war, as a use of force, to the 21st century, maybe we have to -- why use Clausewitz? The guy's been dead for 130-something years. Shouldn't we be a little more progressive here? To which I would respond, we have not updated our notions of what is violence, what is war, with the rise of air power, which hasn't been around when Clausewitz was around. We haven't updated our notion of war with the arrival of nuclear weapons, necessarily.

Ultimately, and I appreciate that some of you here in this room may have served in warzones, who experienced political violence in other contexts. I think, and I say this as somebody also who is teaching in the Department of War Studies, we have to respect violence, we have to respect war in a fundamental, existential way. So, exfiltrating data, even crashing an entire company's network, and physically disabling data, is

different from hurting, injuring, and killing human beings, even a single one, and I think that's a fundamental philosophical distinction that we have to keep in mind, I think, and we owe it to those who have had that experience, in a way.

When Secretary of Defense -- outgoing Secretary of Defense Panetta introduced the medal for cyber operators and drone operators, there was an outcry among veterans because it was in the hierarchy of medals initially thought to be more important than the Purple Heart, and there was an outcry, rightly so, I think, and their decision was repealed.

So, I think I'll close by saying we need to respect time-tested principles here. Thank you.

MR. SINGER: Jason, would you like to respond?

MR. HEALEY: Yes, thank you. How much -- do I have the full rest of the hour or --

(Laughter)

MR. HEALEY: Okay, thanks. So, I want to start -- I mean, I know everyone's looking for lots of argument and lots of sharp edges. As I've been talking to Thomas about this, we realized that we do have a bunch of overlap, but I did want to start with a good jibe, and I want to say that our book, the cyber conflict history book, *Fierce Domain*, has more

pages and is less expensive.

(Laughter)

MR. HEALEY: But it actually does cover a lot of the same ground in similar ways as Thomas does.

So, if you look back at the 25 years that we have of cyber conflict, so, we avoid the word war for many of the same reasons that Thomas does, but we can still say, look, we've been having these things that are understandable as national security conflicts since 1986, and that includes everything from espionage to some of the things that Thomas describes as sabotage, to high-end attacks that don't cross into war. We still don't see that anybody has ever died from a cyber attack.

So, I absolutely agree with Thomas that it's an odd kind of war that's never had a single casualty, but there is this conflict that's happening at the technology level with these very strong national security implications that we can take a look at and that we can learn from, and most importantly, can help us understand what might be happening next, because Thomas has been great at underlying this point and saying, the discussion on this has been very flat. There hasn't been much thought about what we mean by war, about what kinds of war.

Frankly, we're continuing to be pulled back by people talking about the digital Pearl Harbor, and we realized in this book, we've been

talking about digital Pearl Harbors for 20 of the 70 years since the actual Pearl Harbor. So, there's obviously some kind of dynamic going on that we're not understanding if we're getting that wrong so much.

I'll cover just some of the main lessons that we've been looking at and that we've found when we looked at cyber conflict as history.

Most importantly, you can learn from the history. There actually is a history that you can take from. Many of our colleagues that speak on this topic you'll hear say, the only constant is change and it's moving so quickly. That's true at the technology level, but so what? If you look at it as a national security conflict, the kinds of dynamics have been relatively the same since 1986. Just like you could take a fighter pilot from 1916 and a fighter pilot today, and even though the technologies come so much more lethal and the battles are taking place at faster speeds over wider rangers, they're still going to be zooming in and shooting each others' fighters down and talking about some guy on a six, because the fundamental dynamics of fighting in the air haven't changed that much and the same thing is true here.

Also, we find that the more strategically significant the cyber conflict, the more similar it is to conflict in the air, land and see. So, I'll say that again. The more strategically significant the cyber conflict, the more

similar it is, and that also is like conflict -- if you hear many of the American generals today that are involved in cyber, they'll tell you about how it's speed of light and how two kids in their basement can have capabilities and deterrence is tough, and all of those things are true at the tactical level, but since when do we want our Four-Star Generals talking about fighting from -- the truths of fighting in foxholes? The generals should be looking to abstract up what's true at the tactical level to what's up at the strategic level.

For example, speed of light, you hear General Alexander talk about how cyber is speed of light all the time. It is true, but I came from the Air Force, I see many others here. In the Air Force, the dogfight could be over before you even know you're in a dogfight, but air campaigns take place over weeks, months, and years, and that's what we see in cyber.

A single cyber attack has almost never had -- a speed of light cyber attack has almost never had strategic consequences. It's almost always a back and forth between adversaries that unfolds over days, months, years. Likewise, warning tends to be very simple for cyber attacks. That's not what you hear from the Ft. Meade crowd. You hear that it's very difficult because it's speed of light, but the largest attacks take place in a geopolitical context, that you don't get attacked out of the blue, you get attacked when one nation is -- one national rival is angry at

another national rival, which makes warning a lot easier. It also generally takes attribution off the table because in almost all of the cyber conflicts that we've looked at over the past 25 years -- disruptive cyber conflicts -- it's been pretty obvious who's been doing the attacking, which I think has great implications for deterrence and what kinds of conflicts we might see next.

Thank you.

MR. WALLACE: Thank you. I'm very pleased to be here. I love this book. I also love Jason's book. They're different, complementary, but one of the reasons why I think they're both important, and particularly Thomas' book, is it does a fantastic job of setting out the true utility of cyber capabilities, and I think at a time when we're hopefully going to get into a national debate -- an international debate, even -- about weighing those capabilities against not using those capabilities and setting that into context, it is important to understand what we're actually dealing with, what we can use, what is really in the realms of science fiction.

There's an example in the book that Thomas gives of a -- that's actually been used by many -- I've heard used by senior members of the NSA about a dam in Russia that was victim of a significant accident (inaudible) a fault in software that controlled it. It caused many fatalities, but as you dig into the truth of what actually happened, as Thomas does,

you begin to realize that that had as much to do with the disrepair of the pumps as it did actually the potential for cyber attack.

And I think truly understanding the utility of cyber is going to be really important as we get into that debate.

I also think it's a great book because it focuses back on language, and I think for many people the semantics of what's war, what's not war, tends to get pushed off to the academics, and at one level that is exactly where it should belong, but there are some really important policy results that come out of how we talk about war. Wars generally get carried out by professionals and externalized by the population. If populations feel that cyber are not there -- cyber security is not their responsibility, that creates problems for the private sector, for people on their home computers.

Wars generally have an expectation that they will end. This issue of security with information systems is going to be with us forever and we need to find some way of dealing with it. And, this I think is relevant to where we are at the moment, wars tend to justify expedience and if we are more willing to cut corners in order to win a war, that potentially gets us to a place where we're willing to do things that bring, for example, the military into areas of security that we probably don't want.

And finally, wars -- or if we have the Secretary of Defense

focusing on protecting our home computers, there is at least an argument to say that he's probably not as focused as he might be about how capabilities really need to be used in actual wars that happen, and one of the questions that I think I'd like to hear more from Thomas about is if war isn't going to -- cyber war isn't going to happen in isolation, how we get from use of cyber capabilities into war and that escalation/de-escalation ladder.

I don't agree with everything in the book. I think there's an interesting question -- maybe it's too academic to get into too much detail about -- whether cyber is a domain, but as I sit here next to someone who's written a book called *A Fierce Domain* and someone who's written a book saying (inaudible) domain, I think there is certainly an issue about how we organize, and that has a bearing on that, how our military structures itself to do this, which is a literally billion dollar issue, or billions of dollars.

And finally, I think there's an interesting question as to whether, because cyber war hasn't happened in the past, and as Thomas says, there's little empirical evidence to justify that, whether with developing technology it means it's not necessarily going to happen in the future, particularly as we get more automation and the internet of things becomes not just embedded in our lives, but is the basis of which we live

our lives, and I think that's, you know, going to be an important issue going forward.

There's a good case that the bureaucracy required to run a cyber war is much greater, as Thomas says, than we actually recognize. There's also a good argument to say that the disadvantages of engaging in a cyber war are greater than realized, but as the U.S. and other countries find themselves engaged with countries that may be in a position where their existence is threatened -- and if you look around the world at certain countries that the war is possible, that's certainly an option, you wonder whether the lack of security within the U.S. does actually still raise some concerns about how cyber is used in war in the future.

MR. SINGER: So, we have a couple of questions that Ian's put there on the table that I'd love to hear from you, but then also Jason weigh in, when we have this. Let's go in on the issue of domain. Is this a new domain or not? And if not, are we building castles on the clouds out of all these new structures that have been created for it? And this is not, again, a semantics question. The issue of whether it's a new domain was one of the key areas of dispute between the Pentagon and the White House and the State Department as they were starting to put together strategy in this area.

So, should we look at it as a domain? And what are the

implications of that or not?

MR. RID: The domain question is, indeed, as you earlier said, it's slightly wonkish, but also a bit -- it's interesting to think about for a moment. Is cyberspace a new domain of war fighting? The history of this is that -- I mean, cyberspace as an idea, of course, emerged in the 1980s then got more popular in the 1990s, and in the early 2000s it had arrived inside the Defense establishment, and in 2006, I think, or early 2007, the Air Force -- the U.S. Air Force then changed its mission statement saying that it now flies, fights, and wins -- I think I need to speak into the microphone properly -- flies, fights, and wins in air, space, and cyberspace.

So, the Air Force is in charge of three domains, the Army and the Navy, each one other domain, land and sea.

Well, more complicated than that, we know that, and I'm simplifying, but the problem here is that by looking at this history we see where it comes from. I mean, it's a powerful argument for money, right? We are in charge of cyberspace, either the Air Force or Cyber Command or somebody else, give us responsibility, give us resources, give us the staff, give us the money in order to succeed.

Now, what's the problem with this? Well, cyberspace -- I mean, how often have you -- every single one of you, how often have you

used the word cyberspace outside your work context? Outside of professional environment? The word cyberspace itself has a very much 1990s ring to it today. We don't really use it that much. Why is that important? Because we understand in our private lives that there is no separate domain. It's effects -- what is online can affect us immediately, it can affect whether we have water in the tap in the morning when we open the water tap. There's a link between -- it's about control, it's about processes directly. So, I'm concerned, when we talk about a separate domain, that we are essentially creating a wall between the expertise that you need in order to effect complex systems that are very much in this domain -- real, not somewhere separate in --

MR. SINGER: I'm going to push you on this. I'm going to be the moderator -- since they're agreeing with you too much -- the implications of moving massive amounts of information online, coordination, communications, into what is arguably a domain, which is not controlled by -- here's an example of a difference -- a traditional weapon has to follow the laws of physics versus a cyber weapon can be in multiple places all at the same time, or another aspect of a change for this organizational, yes, there is an organizational grab for power going on, but there are some fundamental disruptions in terms of, for example, the identity of that fighter pilot circa 1916, he would be recognizable to the

fighter pilot in 2013, but the attributes that someone working in cyber, they could be physically located anywhere in the world, they also don't have to have great eyesight, their skill set and training may be different, the units that they should be organized in, it doesn't make sense to plop down squadrons -- I mean, there are some fundamental disruptions of moving massive -- you know, to doing more and more online, and then as what Ian put out there, yes, that involves a very 1990s view of our relationship with cyberspace, cyber -- however we want to say it -- how we conduct communication and commerce, but what happens when we move into the internet of things where it's not me just iPhoning to someone, but it's my car automatically communicating with my house, which means that someone attacking it can cause kinetic change.

MR. RID: Yes. Now it gets interesting. So, I think we have to make a fundamental distinction, and you used the word cyber weapon already. I think that's an important expression to make that distinction.

The microphone I'm speaking in here now, hopefully, is not a weapon. Would anybody be ready to call this microphone a weapon? I think very few people in this room would go that far.

If we are talking about intelligence operation, exfiltrating information from companies, which is really, at the end of the day, the major problem we're talking about. It's more in the intelligence arena than

in the arena of kinetic effects.

But then we're not talking about cyber weapons. Microphones are not weapons and video cameras are also not weapons. You have to weaponize a target system with computer code in order to create a kinetic effect, an airplane that falls down, a power plant that explodes, something -- the target has to be automated, and relatively complex, in order to be weaponized. I think that's a very important distinction to make.

So, cyber weapons, if you look at them properly, I think, we've seen very few. Was Flame a very sophisticated espionage tool, if you like? Was that a cyber weapon? I don't think so because it didn't cause any damage other than financial, possibly, damage, which is important. I'm not saying it's not important, it is very important actually, but it's not a kinetic effect.

MR. SINGER: We've got about an hour left.

MR. HEALEY: One part is that, especially in this town, we get so caught up in capabilities that we're largely losing the bigger picture. I was in an extremely senior meeting at the Pentagon. There are 21 stars in the room split up only between about eight different generals, and they kept saying, what's our service going to be in this area, what's our service going to be in this area, and they kept coming back to capabilities.

And it's a bad service that only argues that our role in something is just going to be restricted to doing certain capabilities rather than looking at what your heritage is, looking at how future wars or future conflicts might get fought and what you want to be about and how you want to represent.

For the area of domain, I've got one or two quotes I'd like to read. "Information has its own characteristics of mass, motion, and topography. Before the Wright Brothers, the air obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age, but the Information Age changed the information realm's characteristics so that widespread military operations became practical."

If you're wondering about this arcane thing of is it a domain or not, I think that's a wonderful quote, to say why we -- the people that say it is a domain, hey, great, it's gotten so complex now that you can imagine widespread military operations taking place in it. That quote is from 1995, so if you're wondering why -- and, I mean, many of us don't get impressed, but we've made so little progress since 1995 in talking about whether this is a domain or not. And it still gathers a lot of brain cells in this town for a conversation that's been going on for nearly 20 years.

Where this town gets this most wrong is we say, not just is it

a domain, but we say, is it a war-fighting domain, and that's largely where I think -- you know, where we are right now in talking about it. Is it a war-fighting domain? And we're completely missing the point that personally I think it is a war-fighting domain, but it is also not just a war-fighting domain, it is the coolest technology that mankind has developed since Gutenberg, and maybe even since, and by putting so much focus on this being a war-fighting domain, we've really militarized it over the last ten years, we've really allowed all of our cyberspace policy to get taken over on the ground in the network by Ft. Meade.

American cyberspace policy is not made anymore by the Department of Homeland Security or by the White House. Our international posture is not decided by the State Department, it's being decided by the facts on the ground from Ft. Meade because we've decided this is a -- this is a war-fighting domain. Domain is not the main word that we should be worried about here. It's that we've made it predominantly a place where our national security interests are driven by short-term-ism, of worried about the immediate national security questions rather than thinking about what our real national security concerns are going to be for what we need cyberspace and the internet to be 10 years, 20 years, 30 years out.

The internet is not going to be as cool for your kids and

grandkids as it was for us. I'm worried about this, that it's not going to be as cool for our kids and grandkids because of these national security decisions for this war-fighting domain that are being made right now.

MR. SINGER: Ian, do you want to weigh in on this?

MR. WALLACE: Yeah, I'd like to make two very short points. Firstly to say that I think when we consider this issue of domain/not domain, Jason's point about you can have a domain without that being the exclusive activity that happens in that area, just like lots of things happen on the sea without it being war-fighting, but I think the practical reason why this is an important -- is, you know, when the joint commander sits down at his table and looks for options in order to decide how he takes out the air defense systems against a country about to attack, he really needs somebody who understands the air domain, the land domain, potentially because he's the guy who's going to have to pick up the pieces, but also the cyber domain, not just because he can say what he can achieve, but he can also say what he can't achieve, and that's where the utility of these capabilities is important, as Thomas picks up.

But I would also pick up another of Jason's points and say, sitting above this defense discussion about domain is a separate discussion about what are the consequences of using these capabilities,

which is also really helped by understanding what those capabilities are, but what you lose in wider international terms by employing capabilities that may have defense, even intelligence, benefits, and in some ways it's not the military commander's job to do that balance, although they have an important role to play in that, it's people sitting above them in government who have to weigh that cost benefit, and too often those things get blurred in a way that that distinction doesn't properly get considered.

MR. SINGER: Thomas, one, you have a couple things here to respond to, but also the challenge for any author writing in this Gutenberg-style domain of books is that things happen in the news between when you're writing and they come out, and one has been all the various revelations linked to the NSA and Snowden, and this links back to Jason's argument. He's saying that essentially we've let Ft. Meade run amok. What's your response to these, but also perhaps you could weave in, how do the recent Snowden revelations affect change, not affect what you're thinking on this topic?

MR. RID: I think the Snowden revelations have received, obviously, a lot of attention in the public, but I think for many students of intelligence history, of security, the surprise effect was probably not as significant as in the wider public. I mean, we are paying spy agencies to

do that kind of thing -- intelligence agencies. Now we're finding out they're actually doing it, surprise. I mean, I'm being slightly facetious here, but we have to be careful.

I think the Snowden revelations are not fundamentally changing the analysis, certainly that's in the book, I think, that may be confirming some of the analysis.

So, let me give you an example. A key question that's underlying the debate here is the balance between offense and defense in that environment.

If we look at conventional weapons, think anything from an assault rifle to a missile, are not target-specific. I mean, they're target-specific to a degree, some missiles are specialized, some rifles are specialized, but you can't practically shoot with many weapon systems against any number of targets, even if they're specialized. It's different targets.

If you look at cyber capabilities, not just cyber weapons with potential kinetic effect, but any cyber computer attack tool, even knowledge that you have -- you don't even have to build software sometimes, and look at the number of targets that you can hit with this. Sometimes they're vast. Think of a denial of service attack. You basically just need a tiny bit of public intelligence, a URL, and you can bring down a

website. So, no target-specific -- not target-specific.

But on the other end of the spectrum would be the Stuxnet example, which was extremely target specific. The payload for Stuxnet was so finely tuned to its target that it didn't do anything on any other system that it infected collaterally.

So, between building a weapon tailored practically to one target and having a weapon that is entirely generic -- between specific and generic is an entire spectrum in the cyber capabilities realm, and the argument that I'm also making in the book is that maximizing the kinetic effect of a cyber weapon will push you towards more specific targets. Why? Because if you want to weaponize a target system, you most likely have to attack some sort of control system. Today, at least, that may change in the future, control system installations are rather unique. Though in the case of Stuxnet you had to know the spinning frequency of the rotor at precisely which the rotor would collide or touch the hull of the -- it gets very technical very quickly, you have to know something about currency converters and which companies provides the currency converters installed in (inaudible), et cetera. It's very technical, almost boring, I don't want to give you more details here, but the point is, some of these capabilities, essentially, if you develop them, would be one-shot weapons. You can only use them against one specific target.

That means their political and operational utility is drastically limited, so that is one example how investments in the offense are, you know, building a cyber Tomahawk missile is very hard, so investments in the offense are not necessarily making us any safer on the defense. That's one of the fundamental issues that I found unfortunately reconfirmed when the black budget -- the Intelligence budget was released.

I'm a little concerned that the U.S. is spending too much money on the offense and perhaps is not organized well enough on the defense.

MR. SINGER: You're nodding your head.

MR. HEALEY: Oh, yeah. Here, here on the last point. It was -- when I first got involved in the business in 1998, there were two things that were very obvious from the leadership that I picked up in the Pentagon. First was from the Deputy Secretary of Defense on down, it was "defense is most important". We're probably not going to win the next war with information warfare, what we called it back then, but we could certainly lose it if we're not doing our defense well enough, therefore defense is most important.

One of my colleagues, Gregory Attray, when the topic comes out about cyber deterrence, he always brings up, when we talk about

cyber deterrence, why do we always assume we're going to be the ones doing the deterring? It's far more likely given the terrible state of our defenses that we're going to be the ones that are getting coerced through cyber means rather than the other way around.

Last point, so when I got involved in this in 1998, the Air Force was just bringing our programs out of the black, we were just starting to say that, yes, we have information warfare programs, we've got cyber weapons, we won't talk about them. That was '98. So, again, we're a long ways into this debate with very, very little progress.

So, here I am working in the Pentagon, many of you here have worked in the Pentagon, I'm sure, so you had the Navy guy saying, oh, you know, the next war is going to be won in the seas and you need more ships, and the Army guy saying, no, no, it's going to be boots on the ground, and the Air Force guys, no, it's going to be the Air Force, we're going to win the next war. Even then the (inaudible) guy saying, it's going to be the fast movers, bombers saying, no, it's going to be the guys that can drop a lot of bombs.

The only thing everybody agreed on, oh, it's those information warfare guys, the cyber guys. They're probably the ones that are going to win the next war. This was '98.

Until I got behind that black door among these cyber warriors

and they would all say, we're not going to win the next war. We're lucky if our capabilities even get used, and you know what, that fact that we're -- that cyber is not going to win the next war, we're lucky if we're going to get used, is still true. It's still true that we're not going to win the next war, but we might lose it because we do cyber bad, but we have lost all of that humility. We've lost all of that focus on defense because it's not sexy.

So, all of the money -- if you've got cool skills, you don't want to go defense, you want to go on the offense side because that's what's attracting all the money. When we're talking about all of the stuff about cyber and warfare and capabilities, we're not talking about defensive capabilities, we're talking about offence capabilities.

We've got so many ways to blow stuff up that we don't really need another capability to do that. We are so vulnerable -- and this is why I'm so against things like Stuxnet, why I'm so against a lot of -- how aggressive the NSA has been, because we have glass infrastructure and we shouldn't really be throwing stones.

MR. SINGER: Okay, with that, let's open it up to the audience here. So, please wait for the mic to come to you and stand and introduce yourself. So, right here in the front.

SPEAKER: Hi, my name is (inaudible), I work for the Johns Hopkins Applied Physics Laboratory. As a technical person who's given

all of these issues a lot of deep thought, I love to debate certain little pieces with you, but what I really want to say is the level of sophistication of the thinking that I've been hearing here is such a huge relief to me because I don't hear it in my day-to-day work, and I just want to say, if any of you guys want to go to work like as a general, you know, as U.S. Cyber Com, you know, you get my vote.

MR. SINGER: Let me turn that kind word into a question, which is, how do we raise the level of discussion on cyber issues? My joke about this is that this is a topic that has primarily been left to the "IT crowd" and therefore we have a set number of people who are viewed as experts and then there's a deference to them, and yet this is a topic that connects across whether you do regional politics or you do ground operations, whatever it is, we're seeing movement on it.

So, how do we raise the level of discourse and discussion on cyber security issues besides write books about it? Ian?

MR. WALLACE: I offer one thought. I'm not sure I know how to raise the level of debate, per se, and if I did, I'd probably be writing about it right now, but I think one thing that can be said is if Edward Snowden, who has done anything good, it may have actually contributed to the raising of the debate. I should say for the record that I think he's done an awful lot of bad and I think he's a terrible man, but I also think that

he will focus a debate around the cost benefit of using cyber capabilities, both in terms of espionage and potentially cyber offense, and weigh that against the dominating paradigm for the last 10, 15 years, which has been counterterrorism, and cause more of a debate, I think, within -- both nationally and internationally about the cost benefits on either side.

Now, that debate needs to be informed by a better understanding of what those capabilities can do, but I think more people in senior positions will start to ask those questions, both inside and outside of government, as a result of this.

MR. SINGER: Thomas or Jay?

MR. RID: Yeah, I think an important lesson that I learned is we have to be distrustful of any analogies and metaphors, especially if we talk about technology. Let's make an example, firewall, packet, fundamental terms that we use in a technical context are ultimately metaphors. A firewall, in an IT context, is not like a firewall in a building. It needs to be configured. Building walls don't need to be configured really.

So, metaphors break down, every metaphor breaks down, and we need to be able to spot the point where it breaks down and say, okay, here maybe we shouldn't call it cyber weapon because it doesn't make sense.

To spot that point of breakdown I think we need expertise

and getting expertise means really talking to a lot of people, and that's the second lesson that I learned, which is heartening, I find. I very quickly discovered when I wrote this book that there's nobody who understands it all. You have experts in the technology field, in IT, who have highly specialized knowledge and specific control systems from a specific vender used in refineries, for instance, but they may have no further knowledge about, say, network analysis, or whatever, or penetration testing or how to build a data diode.

There are many different sub-disciplines and no mind can combine it all, so don't be afraid to ask stupid questions, because here, I think, I mean, there are a few stupid questions, of course, but by and large, a lot of people who think they know -- who give the impression that they understand the full picture of cyber security, don't, and that includes myself. I often have to ask people for help.

MR. SINGER: Jay, you wanted to weigh in?

MR. HEALEY: Yeah, thanks. And I heard a lot that I like here, and especially Peter, when you brought it in and say that it's not writing books that's going to make a difference, and I really want to emphasize that it's buying books that is going to make the difference, so, please, everybody, you can buy his, it's $9.99 for the Kindle version --

MR. SINGER: Let's move on. I will just add on top of that --

MR. HEALEY: No, I do have some serious points. One, because you did ask a very serious question, one is to realize that cyber conflict at the national security level is far more similar than the IT people have been telling us. Personally, I think we're being told that specifically so that they can continue to do what they want because they are the master magicians that are read in and they're being -- we're being told, for example, speed of light so that some commanders can have looser rules of engagement than they would otherwise have if everybody understood it.

Second, we're completely ignoring the history. If you're in the Air Force and you don't know big week, you don't know big week, you don't know Midway, you can't say who Rickenbacker was. If you're in any Navy in the world -- Nelson, Trafalgar, what was that? If you're a United States Marine, you're going to get a blanket party if you don't know who Chesty Puller was.

But in this field, we are actively trying to ignore what happened before. We have no heritage, we don't try and remember the lessons of what's come earlier. When I try and go through the things in this book -- an espionage case, 1986, Germans that were selling the stuff to the Soviet KGB. Talk about that at cyber command, talk about that at Pentagon, nobody -- one in three people has never even heard of this case. That's forgetting Trafalgar.

Last is we are being steered into this position partly by accident, partly deliberately because of over classification. Some people don't want us to know what's going on, and they're completely over classifying this, and that leads to forgetfulness. Classification leads to compartmentalization, compartmentalization means we can't keep learning what's been happening. So, history is vicarious experience, so we've got to start learning the stuff that's gone before.

We've had eight separate wakeup calls and each one is a wakeup call because the leadership comes in, says, wow, that's important, we should do something, and they go on to their new job. The next set of leaders has to go through this. We've done it eight separate times.

MR. SINGER: I think on top of it we need to turn the bad metaphors that are used as ways of ending the argument into things of mockery, so to put it more directly, when anytime someone says "cyber Pearl Harbor", it should not be seen as a justification, it should be seen as something to tune someone out and it should be mocked. And that would help raise the level here -- or "cyber 9/11". That's not the end of the argument, that's you showing you don't have a good grasp on your own argument.

I want to give more chances for questions. So, right there, I really want (inaudible) be able to participate. We're going to let him.

MR. FLYNN: Hi, I enjoyed it very much. My name is Matthew Flynn. I'm a professor of history, Department of War Studies, Marine Corps University, Quantico, Virginia. So, right down the road. Glad you're hosting this event.

A ray of sunshine for you all, we do this endlessly with senior level officers at Marine Corps University talking about what cyber is. So, as you ask, how do we get it beyond writing books? It's being done.

My question -- one of the things we do is we ask what kind of war -- you've got to understand the war you're in to win that war. So, I would ask you, you did raise what kind of war is it. I would ask you more specific -- any of you -- how about ways of war? Is cyber representative of an American way of war? An Eastern way of war? A Western way of war? Some kind of new way of war? I've got five other questions that I will not ask right now.

MR. SINGER: So, styles, cultures of war. Where does this fit into?

MR. HEALEY: I think you are seeing different national types of how they're using this. So, I think you are -- you can definitely see Russians and Americans tend to be a bit more similar, Chinese tend to be a bit more different in it. I haven't seen that much overall scholarship into that as an area yet, so I think it will be curious. I liked Peter's point on

metaphors. As we start thinking about future warfares and future ways of war, I like the metaphors because we've been talking about digital Pearl Harbor, that's one thing. I like, for example, talk about cyber St. Mihiel. That was the first time that you saw Air Forces fully integrated in a ground battle. Cyber St. Mihiel is where you would be taking cyber forces and integrating them into a military campaign.

You can imagine a cyber Vietnam. My colleague Greg (inaudible) talks about, this years long back and forth slog between a non-state force that is backed potentially by a state. And the metaphors can actually help you quite a bit to think about these future wars we might be facing as long as you don't take them too far.

MR. WALLACE: Thomas recently debated this in *The Economist*, so I'd be interested to hear his thoughts on it. I would just reference -- make a very short point to reference this question to the last one to say that one of the things that we need to do is find metaphors that don't have a military take on them to raise the level, and we have to have this conversation about military cyber in its own context, which is very important, but separate that from a wider question about how we protect ourselves and by throwing war in, we blur those in a way that's not always that helpful.

MR. RID: So, just as a brief response, I briefly -- I debated

this question on cyber war with Richard Baklig from (inaudible) who's sitting just here in front of me, and he made a very important point in one of his contributions in *The Economist*, and that is that from the Chinese, if I may use that obstruction here, the distinction between commercial espionage and political espionage or intelligence operations is not made in the same way. Oftentimes we see a blurring. It's very hard to say what is used for economic -- for commercial gain and what is used for political advantage in terms of the exfiltrating of data.

Now, let me use this opportunity to make a statement to say something about the Snowden revelations and China's reaction to the Snowden revelations, and not just China's, but also of other countries.

I think the international dimension, the way of war -- it's not a war, it's an intelligence competition here -- the international dimension is extremely important because we have to remember -- and this seems to get lost in the media coverage, I have to say, I'm quite worried, really -- we're still in an open democracy here, also in the UK, and in Europe. China is not an open democracy, and I dare say that Russia is also not an open democracy.

So, it's fundamentally different whether the NSA is eavesdropping, to use that phrase, in a major way the way it does, or whether the FSB or the PLA are doing that, because the FSB -- China and

Russia don't make that distinction, as Richard pointed out. The NSA does make that distinction. NSA is not spying for commercial advantage. The NSA is also not spying to suppress political opinions in the United States or elsewhere, for that matter, which is also a sharp contrast to what's happening in China and Russia and other countries.

So, I find it somewhat hypocritical to overly pounce on the NSA in that context by people who are also usually -- should be quick to criticize authoritarian countries and their security establishments in a fierce way.

Ultimately, I think, to put it really bluntly, we have a -- there's a moral case to be made for the most powerful and (inaudible) intelligence agency to be in an open democracy. We don't want the NSA to be in Beijing.

MR. SINGER: One last point on this question of -- I see it not as a national type of war, but the descriptions are often Eastern versus Western style of war and what are the attributes, and if we're looking historically at the attributes of Western warfare, and particularly post-gun powder, it tends to be highly linear, hierarchal, and focused on speed, the famous quote that "speed kills", and by contrast if you're going to characterize Eastern style of warfare, it's usually non-linear, it's network versus hierarchal, and more deliberative. It's willing to let things settle as

opposed to trying to have everything act on first day.

Or if we're looking at metaphors, there was the famous argument of Americans do American football and everyone else does international football, so it's the notion of, you know, can you -- this was a discourse a decade ago, can you win a counterinsurgency playing football style versus soccer? And so this question here is, is cyberspace or is computer network operations, whatever terminology you want to -- is it something where organizations that are hierarchal or is it something where linear thinking or is it something where speed orientation dominates or is it the alternative.

MR. FLYNN: I mean, is it an avenue for non -- for fighting without fighting, it would be the foremost --

MR. SINGER: That's nonlinear. Okay, so let's -- but it's an interesting debate. Let's move back here.

MS. CHARLES: Hi. I'm Debbie Charles with Reuters News Agency. I wondered if each of you could answer this: what do you see -- if the U.S. decides to strike out at Syria, what do you see the role of cyber having in this?

MR. SINGER: Let's just go down the line.

MR. RID: I -- this is a tough question because obviously there's -- I have no privy information on that one, but I would assume that

if -- let's assume the U.S. Air Force -- the Pentagon has the capability to blind the Syrian air defense systems efficiently. Would they really want to use that in Syria? Is that really important enough to give away that capability? I don't know how that question will be answered inside.

MR. SINGER: Ian or Jay?

MR. WALLACE: I would agree with that thought. I mean, the classic use case for discussing the utility of cyber capabilities is taking out air defense. The points that Thomas alluded to, however, is once you've used it, then you've exposed it and the question is whether this is, A, so difficult to do with conventional capabilities that you would want to depend on cyber, and secondly, whether you want to give away that capability if indeed you're confident that you're willing to put the lives of your pilots in harm's way on the basis of that will definitely be successful. And I think one of the further considerations if you get all the way through that is what you actually ultimately want to achieve.

If you intend to have a long-running no-fly zone, then obviously permanent destruction is more important than a short-term mission, but I think the truth is, until the commanders have absolute confidence in what they want to achieve, then they're going to be cautious.

MR. HEALEY: That's an important point, the commanders understanding what's happening, because cyber is very difficult to use on

the battlefield because you can't always know it's going to have the effect that you want, you can't always know that it won't cascade out of control, and it's difficult to know if you've actually achieved the effect because you don't have the pleasing splatter of debris that you get when you drop a bomb.

So, I think there's both outbound and inbound, when we're talking about what to expect on cyber, so first is I would expect that NSA is already inside those networks and has been collecting intelligence off it. It would not surprise me to find that NSA internet-based collection is leading to some of the facts that's leading President Obama to be so sure that Assad was behind it.

So, I would suspect a lot of that access is already in place within those networks, within the email.

Also for outbound, I made the case last week that -- in Defense One, that we should, regardless of the military utility -- well, not regardless, but as a separate consideration for the military utility, consider doing strikes because right now there's been a big debate going on about cyber, can it fit in within international humanitarian law. Some countries are saying, how could you even do cyber within Geneva Convention? It doesn't even make any sense. It wouldn't be done like that.

I've felt, for a long time, that we should use it within a

battlefield sense and we should go and make known the fact that we used it, in this case, to shut down these air defenses, to shut down this power plant, to disrupt this command and control communication or disrupt these chemical troops, which are all rather difficult targets, to say, look, we could have killed these people, their lives were forfeited, this was during a war in a humanitarian mission, and cyber can be done in this humanitarian way fully in line with international humanitarian law.

All of the norms -- many of the norms the United States has set and the way that they are used, our intelligence and cyber capability, have reinforced all of the wrong norms, that it's okay to stab the buddy in the back, you know, the skullduggery, cloak and dagger kinds of stuff. Let's actually use it in a humanitarian way and in a humanitarian mission.

Second, for inbound, a piece that came in, I think, yesterday in *U.S. News and World Report* -- or Saturday -- I would anticipate that we're going to see a big uptick in Syrian Electronic Army. None of it's going to make any difference. It's going to generate headlines, but it's not going to crush the United States, it's not going to disrupt U.S. military power. It might give one or two organizations a bad day, but it's not going to do anything military useful. That's the easiest prediction to make because cyber attacks have never achieved anything militarily useful or almost never achieved anything militarily useful.

China's not going to get involved even though they sometimes will let their patriotic hackers get involved. Putin might. If this really goes far, he might decide to let his youth groups like Nashi or Russian organized crime. If he is so angry at Obama, he might just say, yeah, you guys can go ahead, and why don't you let them know that we're angry, so we could see Russian patriotic hackers.

We expect Iran and their proxies maybe to get involved a little bit because they're already involved today, but unless Obama strikes switch into regime change, which I don't think they will, that's certainly not the (inaudible) expecting, then it would surprise me if we saw Iran get any farther in and really decide this was where they were going to dive in fully.

MR. SAMROV: Mike Samrov, U.S. Marine Corps, and I know a good deal more about Chesty Puller and blanket parties than I do about cyber. So, I apologize. Dr. Rid, in your initial discussion you talked about sort of properties of war that cyber doesn't share. You spoke about violence just as a divider and then rational subordination.

Well, getting back to war, the interesting part about violence is that as that aspect of war which makes war tend towards an absolute extreme and rational subordination can either bound it or push it towards that extreme.

The third aspect that a fellow that I was tortured about at

Marine Corps University wrote, was chance, chaos, disorder. Does cyber share any of these characteristics? In other words, is there a characteristic, let's say not violence, that pushes it towards absolute extremes? Is there some level of rational subordination that can do either/or? And then is there that aspect of disorder in your studies? Thanks so much.

MR. RID: So, good to see a fellow Clausewitzian in the audience. Certainly the friction, chance, uncertainty come in a very powerful way, possibly, in a conflict that can be escalated into that arena, but again, we have to be -- I resist -- and I mean, that's also why I answered only with a very short sentence to the previous question. I made it a principle, even in Q&A, is not to be drawn into the speculating game because there's enough of speculation out there already.

I don't see myself in the business of speculation. The fact is, we've never seen a single blackout -- electricity blackout caused by a cyber attack. We've seen people try. Certainly it's theoretically possible, but we've never seen it in practice. Or, for instance, we've never seen a single person killed or injured as a result of a cyber attack.

In fact, the single only external cyber attack that has ever caused physical damage to a machine was Stuxnet. All other control system incidents that had a kinetic effect were insider attacks, which is a

different story.

So, what does that mean? That means we have to be able to answer the question, why? We can't just ignore the question, why has nothing happened yet, and I think we see a strange combination of two main actors. One, those with the intention to do harm, haven't got the motivation to do so, because I assume that some people would be able to use that as a tool, and those with the motivation to do harm, don't have the capability to do so.

That may change at some point in the future, but -- and once that happens, then of course there's going to be more chance of uncertainty and friction, but I would be hesitant to speculate more than that.

MR. SINGER: What would chance, friction, the fog of war, look like in this space?

MR. HEALEY: It's very deep. I mean, the uncertainty in this field is far more than I would say in warfare in the other domains, starting, not least, that you've -- and two of the biggest differences of conflict in this domain isn't speed, isn't that the borders are kind of funny, isn't difficulty of attribution, all the other things that get quoted, it's that it's owned, run, and operated by the private sector for their own purposes. In all the conflict in the other domains, civilians would try and get out of the battlefield if they

can. Here they've built everything within it, almost everything within it, for their own purposes.

There's uncertainty in the effects of your weapons, there's uncertainty in the targeting of your weapons, there's uncertainty in you can develop this whole capability and if they've got backup tapes, then your whole plan is ruined.

So, there's far more uncertainty in this conflict in cyberspace than in other places. I liked -- I agree with the bits that Thomas has just said. I'd go a touch further in that -- because I want to say how this is similar to the other domains. I mean, we've come up with some things that make it different like the role of the private sector, but if you're in the military, the Air Force, you knew you can't just bomb a factory or bomb a runway because they're going to come back and they're going to fix it. This is why AWPD was so wrong and so much of our World War II planning was wrong, because after you bomb something, they fix it.

And when we look at cyber conflict, we know it's easy to take something down, it's extremely easy in cyberspace to take a target down. It's very difficult to keep it down over time. Even Stuxnet, I mean, that was a back and forth over months, years, of back and forth to keep down the centrifuges. Shamoon. General Alexander loves to talk about how the Iranians took down 30,000 computers, essentially turned them into

paperweights, at Saudi Aramco. But you know what? They took down 30 computers, but the computers got replaced and supposedly the Iranians were trying to do this to disrupt oil production, and they didn't. So, General Alexander says this as, oh, my gosh, this is a terrible story. I see it as a defeat because if they were doing it to disrupt oil production and they failed, then we shouldn't be talking that they destroyed 30,000 computers, we should be talking about they failed in their strategic objective.

MR. SINGER: So, Jay, doesn't this in some ways, though, counter your previous call to use this in Syria? Because we heard from these two that the reasons not to use it in Syria was, to use another bad metaphor, essentially if you're a coach of a football team, you don't use the trick play on Middle Eastern State University, you save it for the big game out East. And then you said, but I want to use it to actually show that there's a new norm, that we can carry out these operations, sort of open up a new space of what's viable. But you're just -- the counter to this would be, couldn't, one, the Syrian regime could say, goodness, you've started -- opened up a new realm of war in our operation, but the second is, aha, we defeated you. You turned off your computers for a day and now we've got them back on. Would we be handing them an easy win?

MR. HEALEY: There's two answers to the question, it's a

great question. One is to use cyber, remember, it's very difficult to keep things down. I don't think we're going to be able to keep the air defenses down, power down, command and control down, for more than a couple of hours, maybe a day or two at most, so it's to open up a window so that we can do conventional military strikes rather than a substitute for. I don't think our capabilities are there to really keep it down for a long period. That takes a lot of effort. I see it much more as just opening a window so that we can do our regular kinetic things.

MR. SINGER: Basically just do Operation Orchard, which the Israelis did.

MR. HEALEY: Correct. Second is, we've already put the war fighting norms out there and then we got caught doing it. We tried to say that some of the -- that what China was doing for espionage was completely beyond the pale, but somehow what we were doing with Stuxnet was okay. That was always a tough argument to make, that Chinese espionage was just far too much, but our actually destroying stuff, that's cool. And now that we've also got caught with espionage, we're already seen to be the war makers. We're already seen to be the worst even though I would -- there's -- I'm not saying we are.

So, all I'm saying with Syria is, let's at least maybe show that this can be done in a humanitarian way, not just --

MR. SINGER: Okay. Ian, you wanted --

MR. WALLACE: Yeah, I just want to say I think the reasons why we haven't seen any massive cyber physical attack, particularly against the United States and her allies is because the United States is the biggest military power in the world and, you know, there is a deterrence effect that comes from that. What instead I think you see is people who are, to date at least, calculating how they can poke Uncle Sam in a way that doesn't provoke enough of a reaction to get a, either military or in some senses any other kind of response, back at them.

The question, therefore, is, you know, what is the stability of that? And do we settle into a regime whereby at a certain level those attacks or those incidents keep happening and adversaries can manage to avoid?

MR. SINGER: So, we'll have to identify a red line?

MR. WALLACE: Well, the red line has -- the red line is very fuzzy and it's a question of whether someone is going to send that into a more solid red line.

MR. RID: Yes, I'd like to steer the conversation to something that -- like in the book, in the last chapter, the attribution problem. We haven't mentioned the attribution problem in this discussion yet, but I think it's a very important question. Attribution problem is to find

out in very simple terms, who did it? Who attacked you? Who is the perpetrator? Who is offending you?

Now, let's take Syria as an interesting example here. In Syria, early on when the administration started to make the case for the strikes, we saw that number in the media or cited, I think, 1,437, or something like that, fatalities as a result of the attack. Right? Do you remember that number? A question to the audience: was that a SIGINT source, or a human source? Any thoughts? SIGINT or human?

MR. HEALEY: Does it matter?

MR. RID: So, probably it wasn't a SIGINT source because -- it was a human source because if it would have been a SIGINT source, a signal intelligent source, nobody would have used that precise number because then the person sending the number inside the Syrian government would have known, oh, god, they intercepted me, and you give away your sources, possibly, by using such a precise number.

Now, that is exactly, I think, what we also observe in the context of cyber operations and the attribution problem there. So, the point I'm trying to make with this example is that we have to assume that the level of attribution is very heterogeneous. Some people may know a lot about who did it but can't say it publicly, for the reason that I mentioned. Some people may know -- and even if you say it publicly, it's

very hard to convince those who just don't want to be convinced.

So, the attribution problem here is a very, very complex picture, and again, I'm looking here at -- I see Richard here and the Mandiant Report implicating Unit 61398, which is also mentioned in the book, is a great example here. It's very difficult to do attribution, but of course it's possible to do attribution. It's a nuanced, hard process and some of it is public and some of it is not public and will never become public.

This, I think, is something that we need to understand in the context of cyber operations. It's a very tough question.

MR. SINGER: Right here in the front.

MR. FREEDBERG: Sydney Freedberg, BreakingDefense.com. Warfare, you know, purely in one domain is neat, like fighter pilots in the clear blue, but where it gets interesting is when domains intersect, whether or not you call them domains.

I'm curious, you know, what is the potential for cyber to actually, you know, impact operations that do physically kill people? You know, if the U.S. is trying to mobilize to respond to a crisis, and somebody does something bad to our global logistics network, or for that matter, on a tactical level, if some -- because I know the Navy is very worried about this -- if someone uses, you know, old-fashioned electronic warfare to force

open an aperture we have for something else and insert bad things into the computers on a ship or even into a whole tactical network, because those are wireless, you know, the tanks and the planes and the ships are not running fiber optic cables to each other, that's a potential vulnerability.

MR. HEALEY: Yeah, it's a great point, Sydney. Thank you. I just mentioned it's easy for a cyber attack to take something down, it's very difficult to keep it down over time. That's always been true because things in cyber space are made of -- you're destructing either silicon or you're disrupting bits and bytes. And both silicon and bits and bytes are very easy to replace.

You know, when you were writing your term paper, you were writing something, if you've got a deadline and your computer eats the article, it sucks, you have to rewrite it, but you don't lose that much time, it's not that disruptive.

The more that we start doing the internet of things that Peter brought up, like smart grid, connecting the electrical grid, now you're connecting things that are made of concrete and steel to the Internet, and when concrete and steel fail, it's not just a short-term disruption, rewrite your term paper, it's real failure, real destruction, real death.

So, Thomas and I agree on this point that we can't find anyone that's actually died from a cyber attack. We're going to remember

these days not as the days of cyber war, like some people are trying to scare you into believing, but into the halcyon days when all you had to worry about was credit card theft or someone putting a picture of their butt on your webpage, because once we start connecting things of concrete and steel to the Internet -- and we're already starting this, and we're already doing it the same way we do all the things Internet, we roll out some cool products and then we say, oh, we should worry about securing them. And that's exactly what we're doing right now for the internet of everything and the smart grid.

In another couple years, we're going to look back and we're going to think about the days when no one had died from this stuff as the sweet, sweet days.

MR. SINGER: Thomas, you want to weigh in?

MR. RID: No, not on this one.

MR. SINGER: Ian, do you want --

MR. WALLACE: Only to say that I think there's a -- that that is the key question, there's an added dimension to it, the extent to which those attacks are against military targets and those attacks against non-military targets, and I think, you know, one of our colleagues, Ralph Langer would point to the relative ease of which you can go after non-military targets.

I think the point that Thomas makes in his book, which is important, is there are good reasons not to do that if you're an attacker as well, and I think the challenge for both us and the policy community and people in government themselves is actually getting a good sense of where that dial -- or where that pointer is at any one time so that you can calibrate your strategy around that.

MR. SINGER: I would toss in, if it is within the realm of an actual, you know, state on state conflict or actors with true capability and the stakes are high, there's three trends that are taking place by which an adversary might take advantage of this. Now, whether they meet the definition of violence or its an indirect action that has the same impact, that's a terminological -- it's a question of terming, but to me it's three things. One, as we rely more and more on unmanned, remotely operated systems, blocking or co-opting those connections of communication actually do have impact. So, yes, I'm just dealing with communications, but if it's a communication between me and my drone, then I can either take away a core capability or maybe even co-opt it.

So, we've already seen examples of insurgents, for example, hacking into Predator video feed so that they're getting the same kind of information that our guys are getting on the ground to have the did they or did they not incident with RQ1-70 drone over Iran, where we certainly did

not want it to land in Iran.

What you're getting at is not battles of destruction, but battles of persuasion, where I'm trying to persuade the enemy's assets to do what I want. We've never been able to tell a bullet in mid flight to stop or go in a different direction.

The second would be -- and similarly within that, I was in one war game and basically we called it the Carnival Cruise Line Scenario, which was almost every Navy ship engine room operates under a SCADA system, which we've seen things go after, and so do you have to physically violently blow up the ship, or is the effect the same if you turn it into the Carnival Cruise Line and it's just floating there without its engines working?

Second is our reliance on the civilian economy on the military side. So, do I actually have to destroy the system or do I just have to hack into, for example, the private military contractor that's supplying it and change the shipment of gasoline that was supposed to arrive that day and do a ship -- the barcode but swap it, and instead they get toilet paper. That will have the same impact on that unit, and the civilian networks are not protected as much.

And then the third is just network-centric warfare. Again, we are able to operate because we're so linked together. I would pose it this

way: if you had an important memo to take your boss, what's the number, what's the percentage at which you would email it versus hand carry it if you knew it wouldn't get there? So, 99 times out of 100, it'll get there, but 1 percent of the time it won't? Would you hand carry it or email? How about 10 percent of the time?

In war, if I cause an important communication not to go -- not to get to a boss, I believe the numbers are different, and so I only have to cause that communication to go down once before people stop relying on it, and then you can't operate in the same way that we've been able to do for the last 20 years.

We've got time for one last question here. Right over there, on the Navy side.

MR. HAGEROTT: Mark Hagerott, now the Deputy Director at the Naval Academy Cyber Center. Peter, you just talked about the potential of cyber warfare against unmanned systems. We just had a ship run aground; I think the first time in history, They released the report, because of overreliance on GPS. They had to cut the ship up, the Guardian.

When I was in Afghanistan -- I'm a recently retired Navy captain, my army officers that worked for me talked about the younger officers being less and less able to do land navigation visually. The old-

timers could look at a slope and almost calculate in their mind the terrain contours. The younger guys are more and more reliant on electronic decision aids. Companies trying to deploy language translator machines. Is there also something where we're de-skilling our work force, in this case the military work force, that makes cyber vulnerability -- hacking the language machines, the GPS machines, and people just don't have the skills anymore to manually safely navigate either terrain or even to fight without these machines?

MR. SINGER: So, in essence, the question is, will or will not cyber war take place, but by focusing on it so much, do we lose capabilities within traditional war?

MR. RID: I suppose some of that certainly is happening. We all know it from our own personal experiences. I mean, I haven't used a paper map in a very long time, I suppose. But what I think may be in your question, there may be the underlying assumption that all those systems could fail at the same time.

Well, that's a tricky assumption to make because let me just say that what we're seeing is an increasing diversity of systems, of operating systems, of other software, and the more diverse the environment of systems that we have, the more difficult it is to take them all down at the same time. I mean, that doesn't even consider the

problem that some systems are not connected to the Internet in the first place. It's actually really easy to error gap the system by putting in a uni-directional gateway of one way or the other, of a really critical system, also on a ship, I'm sure that's already done.

So, there are ways to deal with this problem, but, yes, of course, I mean, one of the situations that a lot of people seem to be concerned about is that as we are making grids -- electricity grids smarter, it may be the situation that you have in an electricity outage and a telecommunication outage at the same time, where each needs the other to get back online, thus creating a rather vicious situation, that is a real concern.

So, obviously there are risks that we should consider, but the risk of generic attack against all those systems at the same time, a hacking attempt, I don't think that's a very significant one.

MR. HEALEY: And I'm quite keen to see -- I've been very happy, I think it's been one of the few things that's really made a difference in DoD doctrine, vision in the last couple years is to say, look, you know, we trained surface warfare officers, we trained pilots to fight through jamming to get used to always, you know, encrypting the radios and never flying if you can't encrypt, of just being able to operate through the difficult electromagnetic environment, and I've been very happy to see

the Pentagon recently say, we've got to do the same thing, we've got to assume that the intruder is going to be in our system, we have to assume we have to fight through the disruptions, fight through the intruders in our system.

I think there's always going to be a trade-off of teaching people the old school stuff and making sure their brain has enough time for the new stuff. That's going to be a tough tradeoff whether that's elementary school or whether that's basic training and intel school or surface warfare school.

I'd love to see this to be what NATO builds itself around as NATO's getting ready for the next summit, because you could easily have the kind of situation that Peter talked about and you talked about where you've got a NATO member, like Norway was deeply involved in the Libya strikes, or say UAE as a partner was also involved in Libya strikes, imagine we're getting ready for the next Libya and one of those has a disruption or intrusion.

It could be a very small issue technically, but that would become an issue for the NAC of saying maybe we've got to keep them out of the ATO and the air operation because they have this intrusion. Very small technical thing, now it becomes a very high level political issue of whether to leave them in or not.

I think it would be great for getting into the next summit for NATO to think about that. See, got a good NATO thing in there.

MR. WALLACE: And I think that is -- I mean, you essentially answered your own question, but the reason why it's such an important question is because while we have Defense Secretaries and organizations like NATO focusing on defending the homeland, they're arguably not focusing on how they fight in alliance in an expeditionary operation, and I think one of the important things that comes out of Thomas' book is focusing the fact that there are serious questions about how cyber applies to warfare, which really aren't being addressed, or at least if they're being addressed, they're not getting the due attention. And part of that is because big, bureaucratic Defense Departments are arguably focusing more on the domestic issues that are properly the concern of others than making sure that when vast Defense resources are deployed abroad, they can actually be used in the way that they were intended.

MR. SINGER: Well, I think we've achieved our goal of opening up an issue, debating, bringing in discussions that need to be brought out to the fore. So, first I want to thank you all for joining us and then ask you to join me in a round of applause for our speakers here and particularly to wish you good luck on the book.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016