DEFENSE FORUM FOUNDATION
Congressional Defense and Foreign Policy Forum

“Cyberwarfare and New Threats to American Security”

SPEAKER:
Bill Gertz
Best Selling Author
Award Winning Defense and National Security Journalist

Introduction and Moderator:
Suzanne Scholte
President, Defense Forum Foundation

Location:  B-339 Rayburn House Office Building, Capitol Hill
Washington, D.C.
Time:  12:00 p.m. EDT
Date:  Friday, March 4, 2016
Suzanne Scholte: Good afternoon, I would like to welcome you all to our congressional defense and foreign policy forum, on behalf of our Chairman Ambassador Middendorf who is on an Amtrak right now, and he hasn’t arrived yet. I’m going to get things started and hope that he’ll be coming in soon. I appreciate you coming out, I know the weather was a little bit iffy, but fortunately we didn’t get hit that hard, especially after that last snowstorm.

It’s my honor to welcome you! Our forums were established in the 1980s for the specific purpose of giving congressional staff the opportunity to hear from expert speakers on critical national security and foreign policy issues. We have a long tradition of bipartisanship because we strongly believe that when it comes to America’s security, this is no a partisan issue at all. Certainly, the topic that we are going to discuss today fits that description. There is this great concern about the devastating impact of cyber warfare and the effect that a cyber attack could have on America. We could not have a better speaker to address this topic than the speaker who is with us today. Cyber warfare and new threats to American Security.

For this topic, it’s an honor to have Bill Gertz. He’s an award-winning journalist and bestselling author. Four of his six books were national bestsellers. He has a reputation for breaking stories and I just want to give you some examples that run the course of many issues. He was the first to report on the Chinese submarine secretly sailing undetected within five miles of the US aircraft carrier Kitty Hawk, the first to report on how the Pentagon activated its missile defense system in preparation of a possible shoot down of a North Korean missile launch, the first to report on the Chinese deployment of a new class of attack submarines, the first to report on Russia’s covert involvement in removing weapons from Saddam Hussein’s Iraq, the first to report on the North Korean government’s involvement in counterfeiting U.S. currency, how the French and U.S. companies violated U.S. export rules by selling oil-related equipment to Iran, the first to disclose how China is building up short range missiles opposite Taiwan, how China had exported ballistic technology to Pakistan, which is the disclosure that led to the imposition of U.S. economic sanctions against China and Pakistan. For this work, and these are just some examples of stories he’s broken, Bill was awarded the Western Journalism Center award for Investigative Journalism, and the United States Business and Industrial Counsel awarded him the Defender of the National Interest Award. He currently serves as editor of the Washington Free Beacon and as the National Security Columnist for the Washington Times. Personally, he’s one of my favorite speakers. He’s always somebody that inspires many people on these issues, and it’s a great honor to have him back in our forum to discuss cyber warfare and new American security threats.

Gertz: Thank you. I’ve got a little PowerPoint here, so hopefully this will work out. This is a threat briefing, which is really looking at the threats of cyber warfare as well as cyber attacks. It’s not going to be a technical briefing, it’s really looking at the threats and making them understandable. I’m going to go through these slides rather quickly. If you see something that I didn’t cover completely, we can get to it in the question period.
I like to use PowerPoint. You know what they say about PowerPoints: Power corrupts, but PowerPoints corrupt absolutely.

My thesis is that Conflict and Competition in the 21st century will be dominated by information warfare. There are two aspects of information warfare: one is the kind of content side, which is the kind of propaganda influence, and the other is technical, which is the cyber side of it. It involves cyber, media, legal, financial, cultural, ideological, and other electronic and non-kinetic warfare.

A lot of nations have figured out that the US is still the most powerful military in the world, so information warfare is now becoming a surrogate for how to indirectly wage information war against the United States.

Electronic systems are ubiquitous. When I started in the news business in the eighties, we had gigantic desktop computers, and eventually came a real small Tandy RadioShack TRS-80 computer, which was a real breakthrough. Now, of course, everything is moving to this [holds up a cellphone]: the computing power of supercomputers back in the eighties is now put into these handheld devices. They’re very critical. If you go any place in our society, you’ll see people’s faces buried in them.

So what is cyber warfare? Cyber threats and cyber warfare include pre-conflict reconnaissance, intelligence activity, and then what I call “Low Intensity Conflict in the Electronic Domain,” known as cyberspace. This is kind of a new domain. The military is just beginning to adopt strategies, policies, and doctrines for dealing with conflict in cyberspace. Cyber attacks range from network penetration to stealing information, to large scale attacks capable of crippling information systems and causing catastrophic destruction. That’s kind of where we are headed.

So this is kind of the range of cyber threats. It can go from low-level web to space nets. It’s become a kind of traditional thing of hackers and others, but it’s escalating. The trend is going to the higher end of threats and dangers. Obviously, espionage, cyber espionage, has become really focused on the cyber realm. It’s a place, because so much information, is stored electronically and moves electronically across multiple platforms, it’s become a major espionage. Reconnaissance is kind of a military term; it really means preparation of the battle space. And, of course, this is, how do you distinguish between when the Chinese break-in that steals information and when they’re actually mapping the network for when they’re planning for a future cyber attack. There’s a very thin line between those two activities. Any effort to try and define them clearly is a big mistake because they’re very closely blended together. It’s a big vulnerability for the US because we have a very strict intelligence system and then we also have a military operational system.

Then there’s theft of intellectual property, denial of service attacks, and the use of destructive malware – that’s becoming the big problem. A new trend is the manipulation of data. This is getting into what they call in the intelligence world “the wilderness of mirrors” where, if you can get inside somebody’s decision making system, and manipulate data, you can actually force them to make incorrect and catastrophically wrong leadership decisions. Now, obviously, this is a key for the military, but that’s one of the trends.
Who are the cyber threat actors? Foreign nation states (most prominently), criminal groups, terrorists, hackers and hacktivists who are kind of techies and people who have an agenda, fishers and scammers, spyware and malware, botnet (botnet is a computer network that has been taken over by hackers and used to conduct attacks such as flooding the entrance of a certain website and causing it to shut down), business competitors, international spies.

I think it’s good to have a little definition here. This is defense secretary Ash Carter, he talks about cyber warfare as being “malicious, as activities that can result in death, injury, or significant destructions, or any such activities that would be regarded with utmost concern and could well be considered acts of war.” So, he’s leaving it a little bit vague on what exactly is cyber warfare. This was given when he was nominated to be the Defense Secretary in 2015, so it’s a pretty fresh definition. It’s also being modified as they try and work some of these things out.

This is a quote from the Director of National Intelligence James Clapper. This was in congressional testimony just last week: “Moscow and Beijing, among others, view offensive cyber capabilities as an important geostrategic tool and will almost certainly continue to develop them while simultaneously discussing normative frameworks to restrict their use.” That harks back to the Cold War, where the Soviet Union used to build up its weaponry, but at the same time they engaged in arms control talks to try and constrain U.S. forces.

A quote from Admiral Mike Rogers, who is really on the front line of cyber warfare today- he wears dual hats as the director of the NSA as well as the Commander of the U.S. Cyber Command, which is a sub-command of the U.S. Strategic command, the command that is in charge of our nuclear weapons and missile defenses as well as a number of other things: “Since the nation that’s being challenged has never before had to defend its interests in values in cyberspace, adversaries increasingly seek ways to magnify their impact and extend their reach through cyber exploitation, disruption, and destruction.”

Now he talks about the trends in cyber attacks, and I mentioned it. First, it’s really espionage getting information, and then reconnaissance. The destructive element was demonstrated in 2009 when the DHS conducted a test, which was called The Aurora Test. This is a picture of an electrical generator that the DHS was able to destroy using cyber attacks, by inputting into its industrial controllers, certain commands that had it basically spin out of control and explode. An even better example was something called the Sayano Shushenkaya Dam – in Russia. This was used a lot by the intelligence community to identify the unclassified way that destructive tactics worked. What this involved was the dam in Russia that had ten turbine generators. They were conducting some servicing on one of the 10 generators. Someone remotely turned the generator on, while they were servicing it. This ten-ton generator exploded and took out eight of the nine remaining generators. This experiment is often used to tell how the trend in cyber warfare will enter into the destructive realm.

So I mentioned that, again, cyber tech trans is basically infrastructure reconnaissance, and that’s really a big issue. I broke a story this week that the defense intelligence agency sent out a notice this week that warned that a Russian commercial security software from a company you may have heard of Kaspersky Labs, was basically developing a security software for industrial control
networks. The DIA believes that if American utilities, the electrical power, water, financial, and others, were to use this security software that it would allow Russian hackers to break into our critical infrastructure and shut it down in a crisis or conflict.

And then of course, I mentioned the hand-helds, things that are going on here include radio for frequency projected malware, the U.S. is working on that as well in network attack and electronic operations.

Data manipulation is used for deception and perception management, and it’s a real concern because we are so reliant on our information systems, that if someone gets inside and can change it in ways that will make you make wrong decisions, it becomes a real strategic threat.

Cyber attacks are being viewed by our adversaries, namely the Russians, Chinese, North Koreans, and the Iranians as a surrogate for kinetic conflict.

So what are the characteristics? It’s electronic, networked, stealthy, strategic, asymmetric, and speedy- as in the speed of light.

This is an anatomy of a cyber attack: You have pre-attack planning, identification of targets, studio reconnaissance, then you send out, in a lot of cases, fishing emails where you do identity theft to gain people’s credentials, then you get inside. Once you’re inside the system, you can steal data or you can shut it down. We’ll show how that was done in the case of the Sony attack.

So these are some of the nation states, North Korea, China. We have North Korea; the Sony attack is the most visible. It was really the first time the U.S. Government came out of its secrecy shell on the issue of cyber attacks and identified a nation state as conducting an attack. The Chinese, of course, they are robbing us blind in terms of cyber attacks and cyber information. They’re doing what is known as big data mining on massive data bases of Americans, 80 million healthcare records, 22 million federal workers and more. Of course Russia, is using cyber attacks- most recently against Ukraine. They tried to shut down an electrical grid, as part of their covert destabilization efforts. Iran has been doing quite a bit of hacking, not quite in the same class as these other attacks.

And of course there’s ISIS, just this week, the Pentagon, for the first time, revealed that it was engaged in cyber warfare. This didn’t get a lot of press attention, but it was a landmark disclosure by the defense secretary and the chairman of the joint chiefs of staff at the pentagon. They didn’t reveal a lot of details, but as part of the anti-ISIL campaign, they are now using cyber warfare techniques to disrupt the command and control networks of the Islamic State.

North Korea- Under Kim Jong Un, Cyber has been given a prominence for strategic military activities of that state. They do quite a bit without the same technical capabilities as their counterparts. North Korea has stated several times that it wants to build the capability to land nuclear weapons on the United states- not just south Korea and Japan. IT’s considered a very serious cyber security threat, but not the most sophisticated. They’ve gone after banks, media outlets, and of course Sony Pictures. For Pyeongyang, cyber attacks represent war by other means. Cyber operations are run by the intelligence service there, which is known as the
They were able to do long-term reconnaissance and very sophisticated intelligence work to identify key people in Sony and then get their credentials, break into their system, and then get what they call “Brute Access,” the ability to really have total control over a network. They used a malware called Destroyer and whip all, customized for the Sony attack- not something your average hacker could do. They were traced to seven different proxy servers in Thailand, Poland, Italy, Cyprus, Bolivia, Singapore, and the US.

The Interview – Why did they do this? They were after the US and Sony because of the production of this movie because of the central focus on North Korea’s leader in the movie. It was a pretty funny movie – I saw it. It wasn’t really great, but one of the reasons the US responded so hard was because we felt that this was an impingement on our freedom of expression. The US response was not really that good, it was basically dominated by excessive secrecy in dealing with it. In the beginning of it, the FBI’s first reaction was to state that there was no attribution to NK for the attack, when in fact, the national security agency knew very early on that the attack was sponsored by North Korea, even though they used the name “the Guardians of Peace,” to try to mask the attack. A lot of US theaters decided that they were going to cancel the showing of the movie, which really prompted the US’s response.

President Obama called it an act of cyber vandalism, not cyber war, and again, that initial definition, nobody died, there was no strategic implications- so they didn’t classify it as an act of war. The president said that we were responding proportionally, and in the time and place of our manner. Basically, there hasn’t been a response that we have noticed. There was a power outage in Pyeongyang, but using cyber counter attacks against North Korea, it would not be proportional. The country is very less wired, and less electrified than most of the other countries in the world. So the response, we may still see something coming in the future, but that situation is very serious.

China: This building here is headquarters of Unit 61398. In China, there military and intelligence units are all categorized with code numbers and names. This particular unit is dedicated to military cyber warfare and cyber intelligence gathering. This is General Clapper just last week, “China continues to have success in cyber espionage against the US and our allies, US Companies. Beijing is also using cyber attacks against targets that Beijing believes threaten Chinese domestic stability or regime legitimacy.” China is among the most significant of cyber threats. It used to be the number one threat, but based on some recent intelligence, the US Intelligence committee has categorized Russia as the most significant nation state cyber threat. China has been on a massive 20-year campaign of cyber espionage and cyber reconnaissance. Sometimes the government tries to dismiss the cyber intelligence part of it as “Well that’s something that we do too.” But from what I’ve learned in my research is that when they go in and get into these systems, whether it’s the Anthem healthcare system, or the office of personnel management, they don’t just steal information. They also plant what’s known as sleeper agent software. Something that’s very difficult to detect. This software only communicates with its home base in Beijing infrequently, perhaps only once or twice a year. We know that they’re in there, we’ve captured some of it, but they don’t have a really good handle on how much of this
sleeper agent software is inside of the networks that China has penetrated- and this is significant because this software could be used to shut down the networks.

Imagine if there were a crisis or conflict and the power grid or computer networks that provide services just shut down- this is the kind of thing that is expected to happen in future conflict.

This is a chart that shows some of the Chinese activities. This is an NSA chart, thanks to Edward Snowden, that shows the main units: there’s the military intelligence that’s known as 2PLA, then there’s the technical department of the general staff department, known as 3PLA. On the list of Chinese military cyber outfits, they’re the number one. On the more civilian side, is the ministry of state security, which is there intelligence service. They’ve been assessed as having a very strong cyber intelligence and attack capability. They also had some unattributed activities.

There’s also some interaction with non-government hacker groups, although in China, most of the non-government hacker groups usually either were with the government and security services or are still affiliated with them.

In China, the Cyber operations is among their most secret programs. This is the reason why whatever/whenever China is accused of cyber espionage or cyber attacks, their blanket response is that this is a groundless accusation. The reason for that is very clear, it’s a strategic move. If something is groundless it doesn’t even warrant a response. The reason this is, is because within the Chinese system this is among their most secret programs. They have some that are semi-secret, some that they’ve acknowledged, but their cyber warfare and cyber intelligence are the most secret. In other words, not only do they not discuss it publicly or even in military writings, but they will categorically deny that they do any of it. That creates a problem, especially when you are trying to, from the Obama Administration, develop negotiations or what they call “norms of behavior” in cyberspace, and that’s been the key policy for the Obama administration.

Of course, industry has been urging a much stronger response. Industry is getting killed on the intellectual property front. Again, complements of the Snowden documents, it is an astounding amount of information that the Chinese have stolen, something like the level of 30 libraries of congress worth of information. And, the targets have been some of our most secret programs, including all of our frontline fighters: The F-35, the B-2, the F-22. They’ve been able to not only steal this data, but actually incorporate it into their own jet fighters. They’re building a J-20 fighter that looks exactly like the F-35, with some of the same design characteristics. They believe that this was also stolen by the Chinese.

Last September, at the Summit meeting, there was an agreement between Chinese president Xi Jinping and President Obama. The Obama administration was about to place sanctions on China for its aggressive cyber attacks and right up until the meeting with the two presidents, it wasn’t clear that they were going to impose sanctions or not. When Xi Jinping made an informal agreement that China would not conduct commercial cyber espionage against the United States, the administration backed off and decided that it would not impose sanctions. Now, here’s the thing: it’s a very narrow category of commercial cyber espionage. In China, basically the companies are either state-run or state-affiliated. They have what they call the “Red Telephone,” all of these companies that have any consequence in China can be controlled by the communist
party. All it takes is a phone call for them. Again, it was kind of a hollow measure, but the private industry of America was saying “you’ve gotta do more,” and some of the options are doing offensive cyber attacks.

Well, guess what? Under current law, under the Justice Department rules, U.S. companies are prohibited from conducting offensive counter cyber attacks against foreign states or others that may have attacked them. But there is definitely a trend- the Congressional U.S.-China Economic Security Review Commission in its most recent report said “That’s gotta change. They need to change the law so that companies can go in and steal back the information that was taken from them or at least go in and destroy the information that was taken from them.” So that’s the ongoing debate.

These are the five hackers from China, military hackers, who were indicted in May of 2014. These guys performed very successful hacks. They went after all of these companies: Westinghouse Electric, US Steel, Alcoa, Allegheny Technologies, US Steel Workers Union and Alcoa. And that’s only the civilian ones that were in there. This did not include the government attacks that were performed. They were able to take a lot of this valuable information and pass it to Chinese companies, reduce US competitiveness.

This is Anthem, the healthcare provider- they suffered a major attack: 80 million healthcare records, including the records of large numbers of US Senior officials. They used a software that was chased to the Chinese group that has been dubbed “a deep panda” by security researches. Again, this is part of their effort to steal large amounts of information and then use that information to conduct additional cyber attacks and also to identify people who can support their other cyber attack missions. OPM, you’re probably familiar with that as well, again, it was the same software and group that was traced to the hack. In this case it was 22.1 million federal workers, including some extremely sensitive data on security clearance holders and background information. For a sophisticated intelligence service that is knee-deep in cyber warfare and cyber attacks, this is the kind of information that can be used to provide leads and other information to conduct further attacks.

I mentioned Russia, this is the GRU headquarters. It’s a very interesting point that they have kind of a Batman symbol. A lot of people talk about the intellectual property theft, you might assume that the batman series and franchise originated from the GRU.

Russia is the most significant cyber threat, I don’t know why, but again, this is the intelligence assessment that was changed recently, and there was some new information that gave our intelligence agencies confidence that the Russians are a very serious cyber threat. They’ve done a number of attacks: the Republic of Georgia in 2008, the Ukraine electrical grid was last year, 2015. They also attacked the Joint Chief of Staff’s email. For a while last year, the Joint Chiefs could not use their emails. It’s un-unclassified system, but the entire system had to be taken down because of a Russian cyber attack.

The biggest threat from Russia, identified by the DNI in public testimony, are Russian efforts to penetrate our critical infrastructure. We have 16 critical infrastructures, including the electrical grid, the financial grid, communications, telecommunications, water, waste management. but of
course, out of all of the critical infrastructures, what’s the most critical of all? It’s the electrical grid. If you take down the electrical grid and shut out the lights, nothing else is going to work. We are an electricity dependent society, and becoming more so.

Russia has advanced cyber warfare capabilities - I mentioned about the industrial control systems. They call them ICS. Basically, the way that our infrastructure is operating is that they have industrial control software and networks that are remotely controlled. They’re remotely controlled so that somebody at a keyboard can tell a dam to open or close, to switch electrical grids when there’s a power outage someplace. These are very vulnerable systems. They’re extremely vulnerable, we are a vulnerable society. From our industrial controllers. Of course, both the Chinese and Russians have been detected, deep inside, mapping our industrial control networks. The problem with our industrial control systems is that once you get inside of them, you can control all of the controllers. It’s just the way the architecture is designed. Now, they’re trying to find solutions to this, but it’s going to take a while before they ultimately close that strategic vulnerability.

Iran, again, not the most sophisticated, but also is using cyber as an asymmetric attack. Two significant ones: one in Saudi Arabia, ARAMCO, that’s the state Saudi oil company. They were attacked with a malware that was able to destroy thirty thousand of their computers. It was traced to Iran. The other attack was on the Las Vegas Sands Casino; this was also an Iranian origin attack. They were going after Sheldon Attison, the owner of the casino.

Clapper said, “Iran views cyber warfare as one of many tools to be used in carrying out asymmetric but proportional retaliation against its foes, as well as sophisticated means of collecting intelligence.”

The NSA likes to say in speeches that there are two kinds of networks: those that have been hacked, and those that have been hacked but the administrators don’t know about it. That’s how extensive this problem is today.

I didn’t go into the criminal side of the hacking, I’m going to pass on that, but I’ll mention the deep and dark web, which are also used by intelligence services, but these are the dark parts of the internet which are used by criminal activity. It’s kind of a problem, because in one sense you can spy on the dark web and get a lot of information about the “bad guys” and what they’re doing, but on the other hand, you allow them to facilitate criminal activities, by allowing these activities to go on.

The problems for cyber warfare and Cyber Command that the legal authorities are currently facing are very muddled. For example, the US Government lead agency for the “dot com” domain security and attacks, is the Department of Homeland Security, which lacks the expertise. The military domain, the “dot mil” domain, is in charge of cyber command. The problem with cyber command is that it’s co-located with the National Security Agency. The NSA is the most effective intelligence and cyber intelligence organization. They’ve been doing it since the eighties and they’re kind of in a difficult strait now. They’ve come under fire since the Snowden revelations about the alleged massive surveillance of Americans. My experience is that they’re an incredibly effective intelligence organization. They’re not out to spy on Americans, they’re...
out to spy on the “bad guys” that want to do damage to America. They’ve been kind of put down as a result of the controversy that accompanied the Snowden revelations, but some of the materials that have come out from NSA have shown that is an amazing organization. For example, the NSA has the ability, is so good at spying electronically, that they can break into foreign spy networks and steal the information that those foreign networks are getting from their spies. They call it Third Party Collection. They have a code name for it too, “I drink your milkshake,” which comes from the movie “There Will Be Blood,” which talked about oilmen who were able to drill holes into neighboring wells and steal the oil from them. It gives you a sense that the NSA has this incredible capability.

To the rescue, US Cyber Command was set up in 2009 and is still in the development stage. They’re having problems with definitions, legal authorities. how do you set this up, how do you allow commanders to be able to conduct attacks, who has the authority, when does the president have to weigh in, when does the defense secretary? They’re still working out all of these things. But, that said, their plan is to develop 133 cyber mission teams. Just last week in congressional testimony, the Pacific Commander and the US Forces Commander talked about the fact that they now have cyber components that are a part of their operations. In other words, at Pacific Command, when they’re doing contingency planning, if an attack happens in Asia where the US has to respond militarily, these cyber warriors are there and a part of the planning. They would be used in the early phases of a cyber attack to getting enemy command and control networks shut down, or spoof them as they would try to do to us. They’re making progress, but they are a long way from reaching the goal of 133 teams, which will be deployed to various military groups around the world.

I’m going to wrap up here. This is basically what a cyber war would look like and I’ll just go to this: this was my story last week, which talked about the first cyber warfare against ISIS.

Surprisingly, it wasn’t against Russia or China, but against the first military target that we have. ISIS is kind of a semi-national state group. This was very significant. First, the pentagon acknowledged that they were doing cyber warfare. Again, they didn’t provide any details. One sign that we know we were having an effect was the Islamic State came out just last week and threatened directly the head of Facebook and Twitter, because they were taking steps. My own view is that was a response to some of the cyber warfare operations because the Islamic State has been using Facebook and Twitter and other social media, not just for recruitment, but for their military operations and to send commands and groups.

If you’re interested in finding out about news about this, I’ve created a website called Flash Critic, which is a combination of two code words: a flash message is one that has to be disseminated quickly, a critic message is one that has to get to the president within 30 minutes. Its called flashcritic.com. But, I’m trying to focus on providing news and information about cyber threats because right now, the problem with talking about threats is that once you talk about them and identify them, the bad guys change their operating methods, so there’s a reluctance within the government to actually talk about these things. On the other hand, if you don’t educate these people and don’t let them know what the nature of the threat is, they don’t think there’s any problems. I’m trying to fill the gap there with this website. I’ll stop there and move into questions.
QUESTION AND ANSWER

Q1: Does the shift to cloud base storage help against cyber attacks?

GERTZ: I think the shift to cloud-based storage does create some vulnerabilities. I look at the cloud as a back up system. I know that there’s probably other means for it, but I would say that everything is vulnerable. You’re only as good as your passwords and your ability to keep the bad guys out. With the methods that they use today to get into systems, its getting more and more amazing. For example, we have massive video surveillance wherever we go. If you’ve ever used your laptop and had to key into a computer code to get into your system, there’s ways to survey that and get that information. There are lots of means to break into things that are supposed to be secure cloud based systems.

Q2: What do you think about action on the international stage to push for international norms on cyber deterrence?

GERTZ: That’s part of the debate. There’s definitely a debate. Admiral Rogers, the NSA Director, who’s been kind of in the forefront of this concept of cyber deterrence. He believes, and he just said this weekend in San Francisco at the RSA conference, “People ask me what keeps me up at night. What keeps me up at night is not if but when we are going to see an attack on critical infrastructure.” So that’s his big concern. He thinks that the price of entry to do cyber attacks or cyber reconnaissance is way too low, so he wants to increase the cost for adversaries to do reconnaissance which is a basically an indication that they’re planning for a future cyber attack, by showing some demonstration of national cyber power, going in and knocking out Unit 61398 and all of their computers would be an example of this. Something that we could do would be to say “Look, we have this capability, if you continue in this course, these massive operations and penetrations, we’re going to retaliate.” The other side of this debate is “no, we can’t do that because the risk of triggering a cyber war where we start knocking back and forth and then the next thing you know is the lights are out,” is the white house’s position. They have sought to use negotiations to develop norms and agreements. To be honest, it’s not working. In fact, the U.S. intelligence community, according to people I talk to, did a national intelligence assessment, which is the product of 16 agencies and they said that unless there is greater pressure on these people and adversaries that are performing these attacks, they’re going to continue. In other words, it was the intelligence community’s way of saying that the idea of seeking norms of behavior and agreements is not working. There needs to be something, perhaps in between those two sides.

Q3: For addressing Cyberwarfare you have all these institutional groups involved in this issue. Is there a chain of command? How much do you have to go back and forth to get approval to take action?

GERTZ: Right now, it’s highly restricted, and that’s one of the problems. Basically, we cannot conduct offensive operations. Now, defensive, again, I’m not exactly clear on how much defense can you do proactively. But, for offense, the president has to authorize it, and then it comes through the chain of command through that. We’ll have to see how the authorities are shaped and
how they can do the rules of engagement and all of these other things that come with the operation.

That’s actually intelligence gathering, which would be neither. It would not be a cyber warfare operation. It could be military recon, or intel gathering. They try to distinguish between the two, but the lines get blurred very quickly if you’re preparing to do an attack. The NSA since the 80s has been doing an incredible job of this, so if the president were to authorize a cyber attack on Unit 61398, first thing that would happen would be all of the intelligence about that, all of the openings and potential vulnerabilities, could you get a human spy in there with a flash drive, can you radio frequency some software – all of these things would go into the planning of it. That’s a big piece of it.

Q4: For some entity getting access to a database, is that considered an offensive action, offensive attack?

GERTZ: That would fall under the intelligence function, military versus intelligence. It would be a kind of covert action; in other words, you’re taking a cyber action that would bring about some kind of influence or political outcome. I’m not sure how much we’re doing of it. That’s kind of among the more secret stuff of the U.S., and I don’t have a good handle on how good we are at that. Traditionally, the U.S. has not been good at using strategic disinformation. That’s clearly been the specialty of the Russians and the Chinese as well.

Q5: Can you comment on China’s capabilities beyond cyberwarfare?

GERTZ: The Chinese are developing a large array of high-tech weapons. The pentagon calls them Anti-access material deny weapons. It’s part of a high tech military buildup, cyber being part of this, submarines and space warfare as well. Cyber and space are being put together in the Pentagon’s pantheon of threats that they’re dealing with. The Chinese have a very capable, several types of anti-satellite missiles. They’ve tested them recently, they blew up a satellite in 2007, which has left 10,000 pieces of debris floating around which threatens spacecraft today. They also have electronic jammers and lasers which can blind or disable satellites, which are key strategic missions for us. They also have demonstrated small maneuvering satellites, one of which has a robotic arm that can reach out and grab and crush or damage a satellite. Of course, they understand that they can’t meet the U.S. head on militarily, so they’re using these to try and cripple through asymmetric means, the U.S. strategic advantage. Our communication satellites, our GPS are both critical for our precision guided weapons and they’re very vulnerable. The air force is spending lots of money trying to deal with this threat, short of putting weapons in space. One idea is to have a lot of low cost, small replacement satellites that can be lost into space if they start shooting down our satellites.

Q6: With the theft of intellectual property the Chinese are able to replicate programs that we may have spent trillions of dollars to develop. How are we protecting against that kind of theft?

GERTZ: I would make the point that the Pentagon has announced what it calls the third offset as a way to maintain the U.S. dominance in the military sphere. First two offsets are one, precision guidance and weapons, and two, stealth, low profile radar, and perhaps drones. The third offset
will seek to leverage technology, especially drones, autonomous systems, artificial intelligence, high technology to keep that edge. The problem is, if you rely on high technology, and you can’t protect your systems from being hacked and having the information stolen, it makes you wonder if that’s truly a good strategy. There hasn’t been a lot of public discussion by pentagon officials about this third offset, but they have mentioned that they are protecting this technology and information by hardening computer networks and information systems is part of it. With the success that the Chinese and Russians have had, breaking into systems, it raises questions whether or not this is going to be effective.

Follow up Q: If you project ahead ten years, can China match or exceed the United States’ capabilities?

GERTZ: Absolutely, in fact, in all of the key areas that China is seeking to develop these anti access area capabilities, that’s cyber, missiles, space, underwater- they are either on par or moving ahead in some cases, compared to the U.S. They’re not trying to do a massive tank-for-tank or warship-for-warship. They’re looking at key areas that are going to give them a strategic advantage, and they’re making a lot of progress on it. Another area is hypersonic missiles. This is an area that I’ve been reporting on. They’ve conducted six tests of something that is called a hypersonic glide vehicle. It’s an ultra high speed 7,000 mph maneuvering missile that doesn’t quite go in space or stay in the air. It skims along the atmosphere. The idea is that by being able to maneuver at such high speeds, it will be able to defeat U.S. missile defenses. They think it is for a nuclear delivery system, again, to get through missile defenses, even though the U.S. says that it doesn’t have missile defenses against China, or Russia. The other thing it could also be used for is long range, what they call “Prompt Global strike,” which the U.S. is developing as a conventional means to be able to hit any place on earth within thirty minutes. If they find a terrorist hideout or an underground biological weapons lab or a nuclear program.

Q6: Even if you have a closed system, what stops someone from just talking out a flash drive with the information?

GERTZ: That’s a good question, I don’t think I know the full answer. I can tell you this, though. Snowden was not the first major compromise, the first major compromise was Bradley Manning in WikiLeaks, who was able to exfiltrate and that was a result of this relaxed sharing environment, where the need to share information was allowed to advance over the need to protect information from leaking out. He was able to do that. Nothing happened after Wiki Leaks, and then came Snowden. The interesting thing is that the NSA out of all the other intelligence agencies, was always warning everyone else that you’ve got to watch out for the so-called insider threat. Well, he was the ultimate insider. It was clear, that though we don’t know all of the details of how he did it, that he had the intention from very early on that he was going to find ways, as a systems administrator, you have to service these systems. There have to be input points and retrieval points, even the classified ones. He was able to do that and get that information out. So, what’s been done? I’m not sure that they’ve fixed the problem. My view is that we have the technology to produce very strict auto systems so that every bit of information that is monitored, classified or otherwise, you can find out who is doing it at what time. I don’t think we have that; I think that’s currently part of the problem with the Hillary Clinton email system. They’re trying
to look at who looked at certain classified information and what, and was that information then retyped into the unclassified system. I think we’re going to find out in a few months what went on there.

SCHOLTE: Thank you all for coming to the program today, I have two quick announcements I want to make. First of all, a housekeeping thing, if you RSVP’d to invite you to the next program, but if you came in and we don’t have your email, we would like to get your email in order to invite you to future programs. Two quick things that we are working on in addition to the forums that we do on defense and foreign issues here on the hill, we’re also engaged in promoting freedom and democracy abroad, and we have two things I want to mention really quickly. We just sent messages from six members of congress that were broadcasted into North Korea during the month of February on Free North Korea Radio. The responses were just amazing. From actual people in North Korea, that responded back about how effective, and how much it meant to them to hear that American leaders cared about them. These were basically new year’s greetings for the new year. I mention this because we had six members of congress that participated both republicans and democrats, and if that’s something that the members that you work for may be interested in, I’d love to share with you what we’re doing and how we’re trying to get information into North Korea. Second thing, we’re also very much involved in North Africa. We have a trip coming up in May. The Saharawi people, the people of Western Sahara. We had people of congress that participated in a past trip and absolutely loved it. This is an incredible problem that doesn’t get a lot of attention, but it’s an opportunity to establish a pro-west Muslim democracy in North west Africa. I’m very involved in that issue as well. If anyone is interested in that next trip, it’s going to come up in May, during that congressional recess, just shoot me an email and I’ll make sure you’ll get invited. Again, thank you all so much for being here, and I want to recognize our Chairman Bill Middendorf for being here.

##