America's Cyber Future: Security and Prosperity in the Information Age

A ROUNDTABLE DISCUSSION FEATURING:

Moderator: Ellen Nakashima
National Security Reporter, The Washington Post

Featured Speakers:
Rand Beers
Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security

Robert J. Butler
Deputy Assistant Secretary of Defense for Cyber Policy, Department of Defense

Max Kelly
Former Chief Security Officer, Facebook

Dr. Kristin Lord
Vice President and Director of Studies, CNAS

June 2, 2011
3:15 p.m. – 4:30 p.m.

Transcript provided by:
DC Transcription – www.dctmr.com

MS. ELLEN NAKASHIMA: My name is Ellen Nakashima. I'm a reporter with the Washington Post. And I'd first like to thank CNAS for inviting me to take part in this fifth annual conference which is a very timely one.

And the topic we're here to discuss here today, cyber threats and national security, is, as we can see from the headlines, one that is only growing in relevance. But it's also one that is often difficult to grasp, speaking as a lay person, because things cyber happen in the unseen and policies are shaped quietly, often obscured by layers of classification or jargon. And so the debate is very often abstract.

But we have a distinguished panel of experts today here to help us pierce through that fog. And I thought we will begin by introducing the panelists. We'll do 40 minutes of panel discussion and then open it up for questions. And as we do the panel, I'd like people to feel comfortable with just jumping in.

So I'll start with my left, the Honorable Rand Beers, under secretary for the National Protection and Programs Directorate, Department of Homeland Security. He oversees the policy and operational functions for the NPPD. He's a former Marine, served in Vietnam, former diplomat and State Department official who has also served on the National Security Council under four presidents. And he served as co-leader of a DHS transition team for the Obama administration.

To my right I have Robert Butler, the deputy assistant secretary of defense for Cyber and Space Policy at DOD, a retired Air Force officer and information operations warrior who has also worked in industry, has an MBA from the University of Maryland and a minor in Spanish, I see. He is responsible for providing cyber policy advice and support to the secretary of defense and other senior DOD leaders.

And on my far left is Dr. Kristin Lord, vice president and director of studies at CNAS and a former fellow in the Foreign Policy Studies program at Brookings. She's also former associate dean at George Washington University's Elliot School of International Affairs. And is co-author with Travis Sharp, of CNAS, of the new report, "America's Cyber Future: Security and Prosperity in the Information Age" which everyone should get their hands on. It's a collection of 14 outstanding papers on the topic with noted experts such as Jim Lewis, Mike McConnell, former DNI, Gary McGraw, and Joe Nye.

And to my far right we have Max Kelly, former chief security officer of Facebook. He built and managed the Facebook security team. He's a former FBI senior computer forensics examiner and a regular speaker at security conferences. He has keynoted both Black Hat Europe and DEF CON.

So clearly it's a panel with a breadth of experience in all quarters. And now I'd like to open with a basic question that I see in cyber which is, the difficulty in fashioning effective ways to deal with the cyber threat because we, the public, do not know the scope of the problem and there's a disconnect between what we hear and what we experience. We hear your dire proclamations, we're at cyber war and we're losing; the DOD's networks have been probed, scanned millions of times a day; we've lost $1 trillion worth of intellectual property, yet life goes on.

So what is the most significant damage that can plausibly happen to us and that would alter our way of life? And in what context would it happen? Is it sabotage of a nuclear plant? Breakdown of a financial system?

How about we start with you, Bob?

MR. ROBERT BUTLER: Okay. Thanks, Ellen. And thank you to CNAS for the opportunity to join the panel today. From the Department of Defense perspective, let me talk a little bit about the context of how we look at cyberspace and cyberspace policy.

As I think many of you know, the department has a fairly big enterprise – 15,000 networks, seven million computers, over 4,000 installations. And as we continue to work around the world, whether it be in Afghanistan or humanitarian relief operations, the dependence upon information technology continues to grow. So at one end of the spectrum is this increasing dependence upon information communications and technology.

At the same time we see a growing array of actors that are involved with cyberspace activity, not always aligned with U.S. interests, which creates challenges for us as we move forward in time. As we work through that, that context, we have come to the conclusion that, yes, there are vulnerabilities that we need to deal with, that we need to deal with them now and we need to continue to move forward in a posture that allows us to continuously innovate and take advantage of technology but at the same time mitigate those risks.

From that vantage point then we set the context for an environment where we see continuous breach of networks and an opportunity then to work from where we are with threats that manifest themselves with exploitation activity today to what we would consider some very challenging, some significant challenges down the road with regards to disruptive activity. And that's I think primarily where our focus is in DOD as we move forward is ensuring that we can operate effectively in cyberspace, especially in the areas of command and control and the key functions that allow us to meet the needs of the nation.

MS. NAKASHIMA: Do you see anything that would pose an existential threat in cyber?

MR. BUTLER: Well, in terms of what we see today, we see a lot of different actors and you're constantly assessing both intent and capability of those actors. It's not – we do not specify or directing our efforts on just an actor or a particular event. And I think we in DOD have a culture of planning for a variety of scenarios.

MS. NAKASHIMA: What is the most dire of those scenarios? (Laughter.)

MR. BUTLER: Ellen, I'd be happy to kind of get into scenarios at other times but it depends upon exactly the context of where you're going with regards to this scenario. In one case, if you're thinking about supporting homeland and security, I mean, certainly we're going to follow the lead of DHS as we look at domestic response. If we're talking about looking at environments elsewhere, you know, how do we operate effectively in Afghanistan, it's a very different set of ideas.

MS. NAKASHIMA: Okay. Rand, what do you see as the most damaging scenario that could disrupt our way of life?

MR. RAND BEERS: Recognizing that DHS is focused primarily on critical infrastructure and key resources within the United States. And I want to accept the national security, the military community in answering this because they do their own protection and planning.

We are obviously worried about something that would cause a piece of critical infrastructure to be unable to operate and to be unable to operate for a prolonged period of time in the sense that it therefore affected the economy overall. There have been a lot of scenarios that people in the private sector have written about which have a degree or not of actual credibility but I think that those kinds of scenarios that have been painted are representative.

Have we seen any of those scenarios? No. Have we seen potentialities of some of those scenarios? Possibly, but I don't even want to – I don't want to give the sense that we've actually seen them because we don't know what the intent of the individuals that prosecuted those, what do you want to call them, reconnaissance efforts. We don't know what their intent actually was. So they may or they may not have been one of those things. But I don't think we've seen those yet.

What we want to do obviously is figure out how best to prevent those kinds of events occurring to our critical infrastructure. That's what we've been doing on a private voluntary basis with the private sector. That's what the cyber legislation that the administration has proposed is about trying to build a stronger way in which we might be able to protect that. And we've spent a lot of time working with our partners at defense in terms of both doing that with respect to the federal

government and thinking hard about doing that in the private sector. This is something that DHS may have the lead for in the private sector but it's clearly working with their partners at defense.

MS. NAKASHIMA: Okay. Let me just ask you one thing. Do you think the scenario of a meltdown of the financial system, cascading failures across Wall Street and beyond is plausible given that maybe the only actors with the capabilities or sophistication should take that on probably don't have a motive to do so?

MR. BEERS: I think you answered your own question there. I think that it is hard to come with a scenario in which the interdependence of the globe economically doesn't act as an inhibitor to destroying the financial system except in the possibility in which we were moving in the direction of nation state war. And that would represent a different scenario, but even there, even there in the old sense of conventional warfare that we used to talk about it's not to the advantage. When we talked about nuclear war scenarios, it was more talked about because we were operating under the idea of mutually assured destruction. That would have left a pretty devastated globe as a result of that. We thought about it. We planned for it. It never happened.

MS. NAKASHIMA: Good. I want to come back to that point later, but I'd like Max maybe to weigh in on this if you have any thoughts.

MR. MAX KELLY: Sure. I think – I definitely agree that there's been a lot of private individuals talking about different scenarios and planning. And to me, when I read them, it reminds me a lot of Y2K issues in 1997 in that people are building a hype around this Armageddon that's probably not going to happen, that they're using it to help sell some of their consulting services and it's not really focused on the real issues that we have.

When I look at what real cyber warfare scenarios are going to be, I think they're going to be very much like cyber criminal scenarios in that they're largely covert, they're – if they're actual actions, they're very targeted actions, they're not necessarily whole sale actions, and there are specific motives for doing those things.

And I think from a scenario planning standpoint you can look back and say there's a technological issue that needs to be addressed, obviously, because that's the medium under which this is occurring. But the same types of motivators that have always occurred behind warfare are there for this type of worker as well. And your scenario should encompass going after those issues as much if not more than the technical issues.

MS. NAKASHIMA: Well, that would also seem to raise questions of who should be going after what types of activities when we see, for instance – and we see penetration of a financial system. Do

we treat that as a criminal event for the FBI, an intelligence event or something that even DOD needs to respond to?

MR. KELLY: I think it's multidimensional. It's all of those things. There's an element where the FBI needs to determine if there's a criminal aspect to it, that that needs to happen. There's the FBI and CIA's intelligence work around probably that same event. And there has to be a DHS response and a DOD response to determine if there's a larger environment that this action occurred in.

MR. BEERS: Certainly what we've seen to date requires all three. There's nothing to suggest that any one of the partners would be – not have a reason to be there to – (inaudible) – to dealing with it.

MS. NAKASHIMA: Okay. Kristin, what about evolving threats and those from non-state actors? Your report talks about the increasing degree to which it's possible to gain access to sophisticated technologies on the black market, about the increased use of artificial intelligence and weapon systems? How and where do you see this threat evolving?

MS. KRISTIN LORD: Absolutely. And I wonder if I might be able to put this in context a bit first. We haven't talked yet about the range of threats that exist and if I might I'll just spend a minute talking about this.

And first, let me say that we have people in the room who are bona fide cyber security experts, Gary McGraw, Roger Horowitz, and others, but for the last year or more, along with our co-chairs, Mike McConnell, Joe Nye, Peter Schwartz and Bob Khan, Travis Sharp and I have been talking to a wide group of people from the government, like these kind of folks here, from the private sector, from NGOs. And we've been sort of scouts for the rest of us who don't understand cyber security and try to go out into this forest and meet with the natives and learn their customs and some of their language. And we'd like to come back and explain to you what we think we have learned. And having done more than 200 interviews over the last year, let me explain to you how we see it. First of all – and this is from a national security perspective.

First of all, there's cyber crime. And this is a tremendous problem for granny getting her credit card number is not a national security problem. What is a national security problem is if that level of crime happens to such an extent that it starts to undermine confidence in the Internet. What that would do to our economy, what that would do to our society. That starts to become a national security threat.

There is the incredible loss of intellectual property that's going on. The loss of intellectual property by any individual company is not a national security threat. It is to the extent that it's a defense contractor or if you are Lockheed Martin and this is code having to do with the Joint Strike Fighter,

that's a special case, but in particular – no particular company tends to have enough intellectual property to present a strategic threat to the United States.

However, if that sap into intellectual property becomes so severe that it starts to undermine the very basis of American economic power, which is our innovation, that in the medium term and the long term it really becomes perhaps one of the most serious national security challenges posed by cyber threats.

And then, when we get into the more traditional sphere of national security, it is almost impossible to image any future conflict not involving a cyber dimension, whether it involves trying to attack command and control, whether cyber attacks are launched more along the lines of the Stuxnet attack – it's hard to image this not being a component in the future on the offensive side, on the defensive side. It's unimaginable.

And at the very high end, we know that tens if not hundreds – into the hundreds of states are developing cyber capabilities so that we hope there won't be another major war between nation states but it's impossible to imagine that the next major war between nation states won't include a cyber component and so it's incumbent on all of us to think through on both the offensive and the defense side what that would look like, what the implications are. And we know that major nation states – these gentleman won't name them but I will – Russia and China in particular are developing some very sophisticated capabilities and we don't know the intent. Certainly we are not at war or any kind of imminent conflict with either of these countries but if we look over the longer span of history, and some of us in the room are recovering political scientists, we need to factor in these capabilities looking forward.

Now, to get to Ellen's question about evolving threats, one of the very interesting things that Travis and I found in our research is that folks in the government were quite focused on state actors, especially powerful state actors that are developing asymmetric capabilities. People more in the technology community were pointing out to us however just the incredible diffusion of capabilities to non-state actors in how even relatively small actors but not very powerful actors, even individuals could really create quite a lot of damage and wreak quite a lot of havoc.

And what I think we're particularly worried about going forward is the most sophisticated capabilities marrying with the most malicious actors and then increasingly these two can find each other more and more easily. And on the Internet they're even black markets where you don't even need a lot of knowledge to buy these capabilities. You can kind of fill out something that looks like an order form and check off what you need. And this is I think over the long term is quite a challenge.

And Greg Rattray and Jay Healey have a great piece in our volume about the rise of non-state actors. And they talk about the rise of unholy alliances and how what we might see in the future increasingly are states marrying with criminal organizations, marrying with just individual hacktivists out to make a buck or I think what we've seen increasingly, ideological groups like the anonymous group that was going after some targets on the Marine base in Quantico, for instance, that are trying to achieve a political or an ideological objective and they have very powerful tools at their disposal so massively better positioned to think about some of the technological trends with cloud computing, the spread of mobile devices and whatnot, but those are some of the things that we found in our research.

MS. NAKASHIMA: Okay. Great. Perfect. I wanted to move for a minute here to the issue of defending the homeland and what the government's role should be in defending what is primarily, as we all know, a private network of computer systems. We all know by now that DHS has the lead in protecting or helping to protect the private sector and that DOD stands ready to assist. Last fall we signed a memorandum agreement to collaborate. But there's ambiguity in that assist role.

Bob and Rand, in what areas would DOD, particularly NSA and Cyber Command, be called on to help DHS in assisting the private sector? Is it only after a breach is detected or can the government help of detection of incoming malware that might target a particular plant? What about neutralizing that malware? And is there framework for when intelligence or military authorities would be used?

MR. BUTLER: So I'll start and then Rand can chime in. Since we signed the memorandum of agreement, we've really been focused on looking at ways that we can take the competencies that we have in the department, best use them inside of this broader question. So that takes the range from operational kinds of planning that we're doing today with DHS into the area of capability development.

A great example is working through technical assistance to DHS as we develop and continue to refine the national cyber incident response plan. DHS lead, the National Security Agency, as well as the Defense Cyber Crime Center which has a tremendous capability in its own right providing support to DHS efforts that take you into the realm of forensics and analysis as well as supporting in the planning activities in general.

Cyber Command, as it continues to grow, again, available and postured to provide help and risk mitigation support. And as we've done this, we've set up this agreement. I think it starts with the sharing of personnel. It also includes the idea of collocating some folks together through a joint coordination only that allows us to begin to synchronize and see each other's competencies in different ways.

As you move forward in time, it's really driving towards more a vision of how we can help not only in the planning side but also sharing our talents with regards to capability development, so how do we move forward to help on the sensing side, how do we move forward to help link a much more proactive way of supporting the United State government and specifically the homeland mission.

MS. NAKASHIMA: At this point you would need new authorities if you wanted to move forward on the actual act of sensing side or –

MR. BUTLER: Right. Yes. We have the dot mil domain and we have everything covered under our DOD authorities there. But as we work with DHS, we are really taking cues from the Department of Homeland Security and enabling and supporting them within the resource constraints that they have, we have, and looking at what they can execute within their own authorities.

MS. NAKASHIMA: Thank you. Rand?

MR. BEERS: I think that's a good overview. What I would say is there's no question that DHS is a more recent arrival in the field of cyber security and there's a lot – a wealth of information technology in personnel in the defense department that are extraordinary, extraordinary help to us in getting started. Some of the problems that we deal with are different but that doesn't mean that the expertise that DOD could bring to the table isn't helpful in thinking about new problems as well as taking on old problems and taking some ideas and solutions that the Pentagon has had.

One of the things that we've discovered though – and this is very interesting – well, we're obviously getting a lot of help. It's ended up in some ways in being very much a two-way street that some of the things that we had gotten into before the defense department, if you will, had begun to work more closely with us, actually gave us some awareness to some of the problems in the private sector that the defense department haven't encountered or thought its way through. And so this is really a two-way street.

I think one of the examples we have here is a collaboration that we have been working on in the Defense Industrial Base. Now, that's a sector that the defense department is responsible for under the 18 sector plan that DHS have overall responsibility but defense is the sector specific agency. Going out into the private sector is a different model for the defense department than working with the defense department but we'd already been out in the private sector. So, to some degree, we have some things to add to the things that they have.

But, as a number of us have said overall, we are not in DHS trying to recreate the defense department capabilities within DHS but we are certainly willing to learn from and have profited

from the technical assistance, the information sharing and the personnel that the defense department has got.

One of the things in the legislation that is important to DHS, for example, is to have a hiring authority that parallels the defense department hiring authority because theirs is a much freer and more open ability to hire than we currently have because when we were created nobody thought about us needing that and that's something that would be very beneficial, not that we're – or we are going to compete with the defense department for hiring those very same people. But, more importantly, that we as a whole of government effort can do a better job populating the kinds of expertise that are necessary to deal with this threat. Bottom line, we can't do it without the defense department but it's a team effort.

MR. BUTLER: Yes. Just building on a couple of points, it really is about understanding and partnering and not so much in the competitive side. I mean, I'm looking for instance where we're going with next gen workforce. We actually need much greater expansion in that area. And my sense is DHS with potentially new hiring authorities is actually going to help us big time down the road. We need to build a much larger base of capability and not only within the public sector. We've got to create cross flow programs. I mean, personally speaking, coming out of the industry and then back into government service has been great because I've been able to see some things very differently than I had when I was just doing government work. So I think it's really important to continue – we talk about the word partnership but putting action behind partnership is absolutely critical.

MS. NAKASHIMA: Yes. I wanted to get the private sector perspective in here a little bit. So, Max, you've said that the military and commercial defense against cyber attacks should be unified. What did you mean by that? And does the private sector want or need government's help?

MR. KELLY: On the second question I think not. It depends on what the help – what form the help comes in. But I'll get to that. On the first question, I – as Facebook grew, we grew very quickly and we became a target for worldwide actors coming against us. And as I started to see the types of attacks that we were fighting against and the types of motivations that our attackers were having against us, I began to think about a worldview in which cyber security and cyber warfare are actually the same thing. Unfortunately, there is a long history of cyber security in the private sector that doesn't view what they're doing as fighting a war and cyber warfare doesn't yet have I think an evolved enough doctrine that encompasses working with the private sector.

And interesting – a semi-technical but not too complex example is if you have a technology company where you have a bunch of servers sitting out there and you have a lot of bandwidth that goes to those servers, there's no direct indication that that's a cyber warfare asset, except for the fact

that if a state actor or a non-state actor who's aligned with some state gets access to those computers and that bandwidth, they can suddenly use that to attack anywhere they want to in the world and it's going to look like it came from you.

And there's thinking in cyber security about how you should keep people from doing that but there's not a large enough awareness – and this was my talk I gave last year – about a big motive for people wanting to do that is to just gain access to your systems and sit there because eventually they're going to use them to go after someone else. And that's not something that most cyber security private sector people would think about or worry about as much as they should.

Now, to the role of government in helping the private sector deal with that – when I came to Facebook in 2005, coming from the FBI, there were already things going on there, even though it was much, much smaller than it is now but people were attacking – there was awareness on my part and many people with companies that as we grew we'd become a larger target very quickly. And I went back to people I knew in FBI, people I knew in government and said, can you help us out with information, just what's going on, what do you see, if you ever hear about anyone coming after us, can you let me know so we can figure it out?

And for years the answer was no. Can't give you anything, can't help with anything. Given that was five years ago, there's a lot more awareness now of what cyber is and I guess there's a lot more awareness of what Facebook is. (Laughter.) But, you know, if I was starting a small company, I would still want that type of information.

By and large, I was referred back to InfraGard, which is an FBI public-private program to share information with industry. When I was in the FBI, I would speak at industry conferences and I would recommend that people in industry join InfraGard and submit to it. Then I joined InfraGard and saw the type of information I was getting and felt very embarrassed. (Laughter.)

And, in fact the last – I was thinking about this this morning – the last InfraGard notice that I received – and not the last one they've sent but the last one that I decided I didn't need to pay attention to them anymore – was a notice saying that Chinese hackers were becoming very active and may start attacking American assets. (Laughter.) And this is in 2006. And I thought, I can probably get better information elsewhere.

When I ended up speaking with people who ran InfraGard and in particular the head of cyber at the FBI at the time – (inaudible) – and asked, why aren't you actually putting real information or actionable information there or at least putting in a system where InfraGard can pre-screen people and then you can determine whether or not you can give them more accurate and targeted information. They came back to everything that's important is either under investigation or

classified. And even if we could declassify it, they felt that they would have issues about giving one company a competitive advantage over another company to which I suggested just give everyone the same information and then you don't have to worry about that.

But I think that these stories indicate how government typically has decided to put roadblocks in the way of helping the private sector with information. And information is really the thing that the private sector needs more than anything to help mitigate many of the scenarios that we're talking about here.

What the private sector doesn't need is – unfortunately, there's a strong awareness, I could think of this in government right now, is a cookie cutter kind of standardization approach, certification approach to cyber security. The problem's so dynamic and so fluid that you really just can't put an ice cube tray of solutions on top of it and hope that you can solve the problem. That being said, there are still people who want to do that because it's a comfortable dynamic for how the government's treated security for the last 50 years, still thinking about computers and networks as if they're buildings and bombs when in fact they're more like soldiers.

MS. NAKASHIMA: Bob, you've been nodding your head a lot. Could you respond to the point about government not sharing the classified information that industry wants and needs to better protect themselves? I keep hearing the same thing today that it is still an obstacle and especially even within the DIB, the DIB project which has been very slow I guess to get started. Maybe that's one of the obstacles.

MR. BUTLER: I agree with Max. My sense is a good role for government is in the realm of building situational awareness across private and public sector. We learned a lot from the private sector as we've collaborated and it starts with information sharing.

MS. NAKASHIMA: What are you doing to –

MR. BUTLER: So in the Defense Industrial Base – I mean, we started this back in 2007, we've grown out to about three dozen companies here where we are now sharing information which helps us with – helps them with understanding a bigger picture, tactics, techniques and procedures and some signatures.

That program has I think been quite successful over the time that it's been in existence. And we're trying now to work to expand that working with the Department of Homeland Security now looking at the expansion of that program into other sectors. And, again, it can take different venues. It can be worked through arrangements, individually with companies but then there's a challenge of some get the information, some don't get the information.

There's a recommendation in the CNAS report with regards to a kind of a government clearing house fusion approach. We are looking at other approaches with DHS and using the ISACs. So there's many ways of working it but the general principle of updating our policy and legal basis to allow greater information sharing is one that I think we do have agreement on.

MR. BEERS: So, if I could just add one point there? We have also come to the same realization that the information that we were putting out wasn't particularly helpful and I'm sorry to say that Max's example wasn't all too frequent kind of example of the sorts of information. What we have tried to do recently, broadly but in the cyber area in particular is to ensure that when we put out some indication of malware, we put out something with it that acts as at least some effort, first order, second order, third order mitigation strategy for dealing with that. The same is true for the industrial control systems that we are working with as well. It isn't always the best that we can get to but it is something that we're embarked upon.

And Bob mentioned the financial sector pilot program we have now. The good news is we're embarking on this. The challenge is that it requires a clearance on the other end in order to exchange classified information. That's something we're piloting with the private sector. We're trying to do it more broadly and we'll see what the results are. But we're hoping that as we work through the legislation and if we get to the legislative point that the ability to share information will be much better and it will be a two-way street, not just industry sharing with the federal government but the federal government sharing it with industry.

MS. LORD: Ellen, I'd be happy to comment on this as well. One of the things we found is that this problem of information sharing is one of the big knots that has to get cracked if we're going to solve this problem. And it's a big challenge for a couple of reasons: one is it's simply bandwidth in government. Even if government has information, just getting it out to companies and sharing it and – I mean, it's just is an incredible problem. I mean, who do you share it with? Who do you not share it with? What are the thresholds you have to cross? So that's one very realistic problem.

Another, of course, is the whole issue of sources and methods and not exposing sources and methods. People like Mike McConnell, if he were here today, would say we need to be much more aggressive in terms of clearing people to get information out. But, frankly, the challenge is also on the corporate side and for some very legitimate reasons. Corporations for quite understandable reasons don't really want the whole world to know their customers, their competitors, when they have a major security breach it's something they don't really want you writing about, Ellen. I'm sure you've encountered that. And so they don't really want to talk about it. They certainly don't want to sit in rooms with their competitors and share that information.

And then, to be really provocative, some people we interviewed said, well, you know, we'd be happy to share some information with the government but we understand their networks aren't so secure. Well, how many times a day do your networks get probed? And then there are a whole set of questions about the legal issues, about liability, about potential violations of anti-trust, about if they give information, will that information become available via for you request. So there's a big thicket that needs to be navigated in order to do this more effectively. But it's a big challenge.

MS. NAKASHIMA: And we need to move on to – but I wanted to get in one line of questions around Stuxnet which I think in the realm of cyber operations was a game changer. I mean, here for the first time was a worm that could target a specific type of equipment in a specific country's nuclear facility.

Bob, if a worm like that were to infect a nuclear plant in the U.S. disrupting and damaging the facility, maybe if we had centrifuges, causing them to spin out of control but not causing deaths, would you consider that a use of force? And assuming you had attribution and it was a nation state, what response would you favor? (Laughter.)

MR. BUTLER: Simple questions? I think we went a long ways in the president's promulgation of the international cyberspace strategy to talk about some of the things that we would do related to deterrence and response, as you saw in that document, really a whole of government that took you from the areas of openness and innovation to security and resilience.

And so, as you read through that document, we talk about a response, a response that's governed by international law, that is not restricted to any specific means but that is couched in the context of not only our national interest but norms that we would develop and would be governed through existing laws that we have on conflict, U.N. charter, and what have you.

So, again, a lot of this is contextual. I mean, Max has brought it up, Rand has brought it up. We would have to work with the rest of the national security community. And, again, the direction would come from the president.

MS. NAKASHIMA: What if it were created by a terrorist group or maybe a corporation, other non-state actors? How would you respond to it then?

MR. BUTLER: So one of the challenges, of course, we talked about it briefly in threat the variety of actors. So within the area of non-state actors, one of the areas that we spend a lot of time discussing and trying to move forward on is how do you create deterrence within – for those actors that you really don't have organizations buying into law. And what we come to are means where we on one end of the equation we're providing additional protection in our defensive posture.

Another end of it is really looking at how we can go ahead and have others adopt with us tougher rules on law enforcement for cyber criminal activity and working with other nations to help enforce mechanisms that would be able to pursue non-state actors, criminals as well as looking at groups of folks that are, as Kristin was mentioning, involved in collusion of activities. We have partners in trying to sort through ways that you can prevent and deter at the same time if activity happens from these types of actors to prosecute.

MS. NAKASHIMA: I'd like to throw this one open to maybe Max, Kristin, Rand. Some say that Stuxnet in a way was a very smart tool. It bore the marks of lawyers steeped in international law. There was no death, no collateral damage, no civilian deaths, no regional conflagration yet it appeared to have delayed Iran's nuclear program by a year or two. So do you think the creation of these increasing sophisticated cyber weapons, such as Stuxnet, is a valuable tool, a politically palatable method of warfare or is it ultimately destabilizing?

MR. KELLY: I guess I'll take that a little bit. I think that the spread of cyber tool development is so wide and has so many motivations that it's kind of an automatic arms race in that all viruses over the last 30 years have gotten progressively more and more advanced. The technological basis upon how they are created and shared and used and what they're used for is more and more advanced. I think that that type of development will continue as long as there are motivating factors for it to do so. And crime is a big motivating factor for that.

For the specific payload that I think that you're talking about, I won't comment on whether I think it's a valuable or a valid form of work or not because I don't have that under my belt. Maybe you want to. Or Kristin can. But I think that it is – it's going to happen and that a defensive posture against those types of attacks would need to be built and maintained.

MS. NAKASHIMA: Did you want to –

MR. BUTLER: I think there's been a lot said about Stuxnet. I don't think that we –

MR. BEERS: And I would concur with Max's last thought. We need to make sure that we can defend against those kinds of activities. That's why we've taken it apart, put it back together again and are developing ways to mitigate it.

MR. BUTLER: That's actually very important, Rand, because that is another part of the partnership. I mean, DHS has been leading the charge on helping us collectively on Stuxnet in terms of the forensics analysis and that truly has been a great partnership trying to figure that out.

MS. NAKASHIMA: Have you finished your forensic analysis?

MR. BEERS: I think we have.

MS. NAKASHIMA: And –

MR. BEERS: No. I say I think we have because these things are such that you're never safe and say your 100 percent sure.

MS. NAKASHIMA: Yes because that it one of the points that your report raises, Kristin, is that when weapons or capabilities such as Stuxnet are released into the wild, probably unintentionally in this case, they can – the risk is they've been reverse engineered and maybe even used against us so you want to make sure you're doing something to prevent it. Did you want to –

MS. LORD: Sure. I mean, I'll just answer your question: are these tools valuable and are they destabilizing? The answer to both questions to me is quite plainly yes. They're extremely valuable tools and in many ways they are highly precise so they can be highly precise. Stuxnet was highly precise even if Stuxnet two, three, 5.0, 100.0 is not because it may be used by other actors in other ways that we can't predict. So they are incredibly valuable and they also do last damage.

Someone pointed out to me in one of the conversations for the report that in a preparation for an actual kinetic conflict it is not uncommon for us to begin by taking out a power grid. Well, imagine if we could do that and then, when the conflict was over, say in Baghdad we could have just flicked a switch and suddenly it was working again. That would have been really handy. (Laughter.) So these are very, very useful weapons.

But they're also very powerful weapons or increasingly will become powerful weapons because I think one of the problems in thinking about cyber threats is that we need to think forward and it's been a lot of hype and a lot of misunderstanding. Gary and Nate's chapter – I don't know where Gary is – is really great on this in terms of separating what are good examples and what aren't. Stuxnet was useful in a way because it helped people to grasp this in a tangible way for perhaps the very first time. And it is a real threat. But in terms of – so the question was, were they valuable? Yes.

The question, are they destabilizing, yes, extremely. And I worry about it quite a lot. They very much favor the offense. They very much favor those that are weak, defense is extremely difficult. I mean, there's a statistic that cyber geeks like to quote all the time which is 20 years ago – it took about few thousand lines of code to defend against a cyber attack. And now it's tens of thousands.

But it used to take about 120 lines for code for malware and it's still about 120 line of code. So the benefits to the defense or the cost of the defense are going up but it's easier to attack than to defend.

But the other point I wanted to make is that there's no transparency. I mean, even in an incredibly difficult nuclear balance, even in the height of the Cold War, we had ways of counting tanks, counting missiles. We knew pretty much how much damage each tank, each missile could inflict. We could count how many there were. And we might not get the numbers quite right but we could have a fairly rational assessment of what the other guys capabilities' were and even though we got that wrong, obviously with the whole missile gap challenge in cyber you can't know. You have no idea what you're up again. So we've been told over and over again the United States is currently in a very active cyber arms race.

But one of the reasons is you just never know if you're ahead or not. And so it's incredibly escalatory. It's incredibly destabilizing in that sense. I think there are a lot of things the United States and other governments can do around the world in order to tamp that down. But I think it's extremely important that we start to have those conversations now.

MS. NAKASHIMA: Thank you. Great. And on that note, I think we'll throw it open for questions. If you could state your name and affiliation, and then your concise question. This gentleman right here, second row. Is there a microphone? Okay.

Q: Hi. Charlie Dunlap, Duke University. This is for Mr. Butler and Mr. Beers. Are you all comfortable that there is a good process by which you can go back and forth if necessary between a law enforcement regime and a national security legal regime? And as a follow-up to that, does anybody on the panel see a utility for an international cyber arms agreement?

MR. BEERS: In terms of our ability to go back and forth, I would say it is getting better. It is still very much a work in progress. But I would also say that at the incident event occurrence for most of the events – well, for all of the ones that I can actually think of, it's law enforcement first. And then we come with them to do the mitigation, attribution and forensics. So the question you pose is not a question we've had actually practically to answer yet, wouldn't you say, Bob?

MR. BUTLER: I think that's right. One of the ways that we actually put life to the response there is we have a standing group, the National Cyber Investigative Joint Task Force. That's kind of a whole of government approach. DHS is involved as well as the Department of Defense, under FBI lead where we begin to work through the determination of what the activity is and what we need to do next. So I think when we look at the partnership with LE and then figuring out when an event actually is more than a criminal event or is moving in a different direction, you already have the partners at the table and you're working through that.

MR. BEERS: That's part of what the national cyber incident response plan is supposed to be the initial building block of. And we've done it. We've created it. We've practiced it. We're revising it in light of cyber storm three at this point in time and it's never going to be done. It's going to be an evolving document, quite frankly. And it should be.

MR. BUTLER: Now, on the second question, and we've just gone through a fairly lengthy discussion about threat and how you begin to understand threat and the challenges with attribution, our sense at least from DOD and then kind of as a part of a greater USG team is that we can make the greatest inroads on the international side with working to develop norms, understanding ways that we can help each other to think about a safe and secure, reliable cyber space. That's certainly cited clearly within where we're going with the international cyber space strategy. It is part of our approach as we engage the United Nations and other international bodies. It's a foundational piece for how we build bilateral, multilateral frameworks in this space. It's a key element of where we're going with our thinking with our forthcoming national or defense cyber strategy. So I think that's really the thrust of where we're headed on the international front.

MS. NAKASHIMA: Yes. Over here.

Q: Rachel Oswald, Global Security Newswire. If I could throw out to the panel to touch on the news that Lockheed Martin recently suffered a cyber attack. I know that not much can be shared but I've read that it's probably Chinese in origin. And what would that mean then if this was not a state sponsored attack but this was a group of individuals operating on their own, how would the United States prosecute this?

MR. BUTLER: So just starting with the dialogue. Lockheed has reported intrusion activities that some of us at DHS ourselves are involved with through our Defense Industrial Base arrangements understanding what has happened, analysis ongoing.

We stand ready as part of our DIB, Defense Industrial Base Information Sharing program to provide assistance in collaboration with DHS. But as we've talked about over the last hour or so, the analysis on these activities, first of all, is challenging. It's diffuse and lots of different pieces have got to be put together. And so from the vantage point of working with Lockheed on this, the question is better directed to Lockheed or the FBI. There is an element within the information sharing aspects here where you begin to move from analysis to seeing what can be done with remediation.

And I think there's two sides of the equation that you have to continually work through, whether you're working this on the public sector side, the private sector side and determining when you reach thresholds that allow you to move in much more proactive ways. So that's kind of where we

are in terms of generally speaking about our relationship from our information sharing program with Lockheed and other Defense Industrial Base partners.

MR. BEERS: And obviously Lockheed doesn't want this to happen again. So they are very much interested in whatever might help them be better protected than they were as a result of recognizing that they've been penetrated. So we stand ready to help them in that regard.

MS. NAKASHIMA: We have a Twitter question here. And then we're looking for Twitter answers – (Laughter.) Can the panel concisely comment on the difficulties of attribution in considering cyber attacks as acts of war?

MR. BUTLER: So I think Max was starting to allude to this earlier when we talked about how malware is designed and how it moves through a system. I mean, typically as you think about cyber capability that's being developed for purposes that – to harm or to create challenges for us, there's intermediate stops along the way in terms of hot points and redirection activities which make it very, very difficult. There are ways both across networks, hardware, software, to provide a great sense of anonymous activity that makes the analysis piece very, very difficult. Sometimes you can find marks, watermarks and others that help you. I mean, we have toolsets to try to assist but today as I think most of us would agree, attribution is extremely difficult.

MR. BEERS: And that's certainly one of the things that we want to think about internationally to see whether or not we can build systems in which the ability to hide behind the national border in a system or to jump can in fact be better tracked by cooperation with those in the international community.

MS. NAKASHIMA: Okay. Thank you. Yes. That gentleman there in the second row.

Q: So I'm here as a geek and a cyber security guy. And I'm also from the private sector. And I think the government is way behind. I'm worried about that. And I've been listening to you policy people all day with just it's astounding, it's really cool to hear what you talk about. (Laughter.) So I'm going to try to ask a question in what I believe is policy wonk speech and let's see if it works. Okay. So not a (long?). So by social contract the state gets obedience from citizens in return for protection, right? That's the idea. But the state's not really delivering when it comes to cyber security. I don't believe. The U.S. spends some say $50 to $100 million a year fighting cyber crime, which is way more than the rest of the world combined. That's cool. But guess what? Google spends more. Google.

MS. NAKASHIMA: And so what is your question?

Q: So the question is what gives? Why is there not more focus on cyber crime than there is on cyber war and cyber espionage if all these things in fact share the same root cause? And I'd actually like to hear what Max has to say about this.

MR. KELLY: Okay. I've sometimes wondered that same thing myself. I think the – I mean, the government is definitely a little behind but I think they're on the right track. They're vectoring in the right direction. You know, and as an instance, a couple of examples where there were very large cases that I brought to FBI that were criminal under the CAN-SPAM Act and they did not pursue them or didn't pursue them very aggressively.

And we ended up pursuing them under the civil recourse that we had under the same act and found the individuals, prosecuted them, won the cases, very, very large cases. I think the largest one we had statutory damages of $8 billion but the judge thought that that was too onerous so reduced it to a mere $800 million. And those were cases where we felt that the enforcement was a slam dunk, handed the whole case over and it just wasn't something that the bureau wanted to focus on at the time. To be fair, they had other things going on.

I think that part of how the cyber security and cyber warfare policies are going to evolve are going to be creating a much stronger awareness on both sides of what the capabilities are and what the priorities are and how sometimes the private realm, the private enforcement realm will be best for people and sometimes the public enforcement realm will be best. And a clear agreement I think will be made on how that happens.

That goes back to my point from earlier of how cyber warfare and cyber security need to become one kind of unified idea of how to deal with it and I think that enforcement action between government and civil, criminal and civil also needs to be more unified. I'd like – I mean, I wish I had a lot more legislation that allowed me to do civil activity against people who are committing cyber crimes because we would have done a lot more. And I think legislation going forward, if it has that capability, it means that Google or Facebook or Microsoft can be very aggressive in a civil action and probably deter a lot of criminal activity just from that.

MR. BEERS: I think that's a really good question and that's part of what we are trying to get at with respect to the cyber legislation. One it's to have the private sector actually share with us when in fact there has been a penetration and do it in a way that they don't feel that their bottom line is jeopardized but that they do feel that the government will be in a position to do something about it.

Secondly, we also need to ensure that we actually have enough investigators who can actually do this and that's an issue as well and that's part of the personnel side that we're talking about in the legislation. So there is actually a need there. Dollars obviously follow that but it can't all be done by

the police because you've still got to answer the question about what is the degree of the government involvement in the lives in the cyber space of private citizens in the same way that we ask that question when we talk about things with respect to conventional crime and we talk about police presence and how much is appropriate, how much is enough.

Those are all questions that we're going to answer, have to answer because we're never going to be able to be 100 percent perfect in this realm. So how do we find that right balance but we don't have the right balance now. And Max is right. We need this law or something like this law to put ourselves in a better situation and deal with this because the penalties for cyber criminals are not adequate at this point in time and we're going to have to fix that.

MR. BUTLER: If I can just build on that point. I take the critique but I'd also like to push back a little bit. We think about what we're doing not only within DOD with the United States government, but certainly a huge focus from how Howard Schmidt with regards to cyber criminal activity and working with the Department of Justice. Within DOD we continue to grow our defense cyber crime center not only in terms of forensic specialists to support investigations but also on the training side. We are training people at unprecedented scales in this area to try to assist in dealing with that threat and with a loss of certainly from the standpoint of defense intellectual property. And we are backing that up with dollars as we move forward. Do we have a ways to go? Yes. We have a ways to go. But there has been a recognition both within the department of defense and other departments about the fact that we have to do more from a public sector standpoint and we are doing more.

MS. NAKASHIMA: Thank you. How about one in the back? Yes, that gentleman there.

Q: Hi. Bill Polevik (ph), reporter at Bloomberg News. A question for Mr. Butler and Mr. Beers. So you said on the Lockheed case that you were still investigating the challenge – and it's a challenging issue and it's diffuse. I was wondering what you're investigating and also last week the Pentagon said that the impact from that intrusion was minimal. So I was wondering how you came to the conclusion that it was minimal if the analysis is ongoing?

MR. BUTLER: So DOD does not have the lead on investigating. It's an FBI lead working with Lockheed. We know based on our information sharing arrangements with Lockheed a lot about how the Defense Industrial Base aspects that they manage are affected. And that was the reasoning for why we made the assessment that we did last week.

MR. BEERS: But right now it's pretty early, pretty early in the process. So it's hard for us to be able to give you anything – certainly anything definitive but even much information. These things don't – they don't play out that quickly. Think about a normal criminal investigation. You're not usually

able to answer within days of the revelation that an event has occurred, a reasonably full description of what actually happened. That's equally true in cyber space.

MS. NAKASHIMA: That gentleman back there. Yes.

Q: Hi. Michael Hauser (ph), one of the 2011 CNAS next generation fellows. I wanted to ask getting back to the issue of organization authorities for defending the homeland. One of the key assets that seems to be left out of the debate is the National Guard. They seem to have the right mix of authorities, title 10, title 32, great congressional support, defense support to civil authorities but they don't seem to be talked about or leveraged or put out front. Instead you see Marines setting up two stars and three stars to do cyber com stuff. Could you talk about that a little bit, the National Guard?

MR. BUTLER: So we have within DOD established over the last half dozen years a variety of National Guard units, primarily in the international side where we are taking advantage of expertise in different areas, whether it be in the financial services arena or co-locating with international guard units say out in Redmond, Washington, with companies like Microsoft.

Our Deputy Secretary Bill Lynn announced in February at the RSA conference the expansion of that program. We're continuing to work to co-locate and build guard units and innovation networks around the United States. At the same time, we're working with the Department of Homeland Security with Rand's team here on looking at ways that we can leverage them both in the military capacity as well as in supporting homeland.

The next steps along the way really drive us into some pilot programs to look at ways that we can do that and thinking about not just what they had been doing, what their expertise is but how we can better leverage the expertise with, as you said, the different authorities. A good concept for where we are working through that is in the (CERTs ?) as we look at guardsmen working in state CERTs and taking advantage again of their expertise in helping with fusion activities and information dissemination.

MR. BEERS: And we in DHS have already, as a general proposition, been using the Guard to do things like vulnerability assessments and as this capability builds out in the cyber area, I know we will be wanting subject to the available of the personnel seeking to have them be part of our general outreach to the private sector.

MS. NAKASHIMA: We'll have one last question. Yes.

Q: This might be a little off subject but there's a lot of talk about what you're doing with the private sector but I was wondering about smartphone technology and its ability to be hacked, especially as

they're being used increasingly by first responders. So what's being done to protect that technology, especially if it's going to be used in responding to events such as 9/11 if someone can get into that, if they're using them for maps or whatnot and hack into that, what's being done to protect that technology?

MR. BEERS: Well, we're certainly looking for any problems of that nature that might be able to be dealt with. With respect to the actual cyber security within the technology as being built by the manufacturers of those, we're certainly trying to create a sense of awareness that they need to think about security as well as the other aspects and value of that. That ends up being a private sector, private manufacturer decision as to whether or not they want to include security within their package. I think to the extent that there is disclosure about failures of security in that regard, it places a premium more on them to do something about it. But we in DHS and the Pentagon don't have the authority to tell them that they have to have those security measures in their technology.

MS. NAKASHIMA: Okay.

MR. BUTLER: One of the areas that we build upon together is again pilot programs here and thinking through not just smart phones but mobile devices in general, how do you operate in degraded environments. And we're constantly exercising running technology pilots in there so that drives you into technology solutions that take you from the realm of encryption out to other kinds of resiliency concepts and it's truly a partnership with DHS and DISCA support as well as abroad for us on humanitarian relief operations.

MS. NAKASHIMA: Okay. If that's it, I think – thank you very much everyone for good questions, lively discussion and the panel. (Applause.) And there will be a 10-minute break between us and the next panel. Yes. Thank you.

(END)