Mieke Eoyang
Deputy Assistant Secretary of Defense for Cyber Policy

Cyber Media Forum
Project for Media and National Security
George Washington School of Media and Public Affairs

20 October 2021

Moderator: Good morning, everyone. If I could call this meeting to order. I'm Thom Shanker. I'm the new Director of the Project for Media and National Security and I'm honored to welcome you to this very special Cyber Media Form that is co-hosted through the generosity of the Howard Baker Forum. We appreciate your support. This is our first in-person breakfast in a year and a half, so if we want to have reasons for optimism that our country and the world is pulling out of the pandemic I look around this room and feel very, very good about that.

I can't imagine a more exciting or substantial person to have as our first speaker than Mieke Eoyang. She is the Deputy Assistant Secretary of Defense for Cyber, which means she is the senior cyber policy official over the entire Defense Department and the military. That's a heck of a job.

We're experimenting with a new format, so I will ask our guest to give some opening comments, sort of set the cyberspace for us and then we'll move to questions.

This format is on the record, but not for broadcast - either audio or video. Our pitch to the Pentagon, State, NSC, the IC, is that we're the anti-press room. We're Geneva, Switzerland. We all sit, we speak calmly, so we don't allow anything other than word stories, either print or on your web sites. I'm sure everybody will agree with those rules.

With that, the floor is yours.

DASD Eoyang: Thank you, Thom, for hosting me. It feels a little weird to be the cyber person and doing it in person because I think we should be doing this in cyberspace. But I really appreciate the invitation to come, and especially because I think that how reporters cover cyberspace and what the department does in cyberspace is so influential to how many policymakers think about this. So it's a real opportunity for me and I appreciate coming here to be able to talk with all of you because one of the things that I'm seeing since I started in the Pentagon is that we are actually at an inflection point in the department in our understanding of how we use cyber and how we operate in the domain.

When I first started in this business years ago when I was on the Hill, people often thought about cybersecurity as just defending the system. We talked about firewalls, we talked about virus protection, we were thinking about our own systems and how we protected them from malicious activity. And it was a very technical conversation which I think made it difficult for a lot of policymakers to understand what was going on here. We talked a lot about regulation, and in the Bush administration we had the CNCI that was focused on how do we defend the system - the Comprehensive National Cybersecurity Initiative. And for a long time cyber was thought of in those terms. In defense and systems.

In 2018 the department took a really big step forward in cyber strategy and we talked about defending forward, and we talked about going out and being on the offense. And in that we were talking about going on the offense against the adversary system. While I'm not going to discuss the specifics, we were very clear about that and we were not just operating on our own networks but where invited by allies and partners we were doing [hunt] forward missions and other things.

But there's another aspect to this. It's not just about the system. It's really about the human beings behind the system. How do we think about using cyber in ways that affect the adversary's calculus? What is the effect on the cognitive domain? And what is it that we as humans need to think about for a defensive mindset?

So our understanding of cyber is starting to evolve. And as we have more operational experience in this space what I've seen is there are a lot of assumptions and mental maps that we have exported and often get written about from traditional types of warfare which are actually not helpful for understanding the complexity of operating in the cyber domain. So I'm grateful to have the opportunity here to talk through some of those things with you guys and hopefully help share how we are thinking about cyber as we go forward and hopefully think through some of the assumptions that underlie some of the ways in which we write about and think about cyber to help get to better clarity on what we're actually doing and how to actually think about it in a more accurate way.

So I would just say, for example, one of the challenges that we often think about in cyber and when we think about, people talk about cyber warfare, even that terminology puts you in a mental state of thinking about warfare And when we think about warfare in all the other domains in which the department operates - air, maritime, land and even space - there is a geography and a location to that that allows you to target and think about boundaries, locations, spaces, which is not the same as in cyberspace.

In cyberspace it is a very ephemeral domain in many ways as people update their systems, as they patch vulnerabilities, transit within the domain is not necessarily linear. And so some of that mental model of the physical domain in which the department operates for most of its warfare is not the same as in cyber. So thinking about how we understand the ephemerality of that, the constant changing nature of that, poses challenges I think to all of us who are steeped in the ways of thinking about warfare. It makes the operations in the domain different than operating in the maritime domain where you know that your adversary's mobilization port is always in the same place. New IP addresses come on, go offline, people change out the system, people change the programming language, people catch things. So you have to constantly be in contact to be able to understand what the environment is like. That poses one of the challenges I think for those of us who work at the Pentagon and work around warfare, to sort of think about what that means.

It also means because of the ways in which the domain is ephemeral and transit isn't linear, that when people talk about how do we prevent adversary activity we sort of all have those mental models, you know, wargames or any other - as if you can see the attacks coming in. As if they sort of move linearly through the domain. And what we know from cyber is that they don't.

So by thinking about cyber in the ways that we might think about conventional strike, we assume that there are certain things that are possible in the domain that are actually quite difficult. Understanding where the attacks are coming from, what time lag is from decision to go to execution. All of those things are very different in cyber than they are in traditional warfare.

So we are thinking about all of that and we're thinking about what it takes to have a mature cyber force and what it means to incorporate cyber into our strategy going forward, and you have heard the Secretary of Defense talking about integrated deterrence. One of the things is like what is the role of cyber to influence across other domains? Not just within the cyber domain but across other kinetic domains including in the cognitive space.

So you guys will see as we move forward both in the National Defense Strategy and also as we develop the cyber posture reviews and cyber strategies, how our thinking has evolved in these areas.

But I'm pleased to be able to have the opportunity to share some of those thoughts with you now over breakfast.

Moderator: Thank you so much.

Just because we're back in person for the first time if you could identify yourself and your news outlet to me and those who don't know you. The first request came from Julian Barnes.

DWG: Julian Barnes, New York Times.

I'd like to ask a little bit about the state of Russian ransomware attacks. We've had some varying assessments by government officials. I'm interested in your view of the current state of threat of attacks. Has Russia succeeded in checking some of the criminal threat to critical infrastructure?

And then if we were to move or if we are, what would a more aggressive defense forward against ransomware attacks look like?

DASD Eoyang: Let me start with the second part of it. I think one of the challenges that we see in the ransomware space is that we are looking at a criminal activity of a variety of actors, some of whom are located in Russia, many of whom are located in Russia, but who are located globally largely outside the United States. I think there are serious questions about the relationship between those criminals and the Russian state. As you've probably seen in some of the indictments that some of them do have those relationships. And I think it's our sense that Russia has created a hospitable environment for these folks.

So I think what you have seen from the administration is an attempt to raise these issues and emphasize this priority directly with President Putin, as President Biden has done. And an ongoing dialogue with the experts group right out of the White House, and you can talk to them about what the state of that is. But also not making any assumptions about how the Russian state can or could change the behavior of these people.

An aggressive whole of government effort aimed at trying to hold the individuals accountable, deny them access to their proceeds, working with the private sector to shore up their defenses, and much more aggressive behavior on law enforcement. The department supports those whole of government activities. And as you've heard General Nakasone say, we view ransomware as a national security threat. The kind of targeting that has occurred, the interference with some of the companies that play a key role in critical infrastructure, certainly Colonial Pipeline, has emphasized to all of us that this is beyond just criminal, that it has a very strong national security impact. So you see this whole of government effort - Treasury sanctions, FBI activity, aggressive use of law enforcement arrests across the government to take action against the criminals even as we try to deal directly with the Russian [state].

DWG: Have they been better? Has Putin put them in a box a little bit? Or is this just as bad as it was when Colonial Pipeline caused us all to run out of gas?

DASD Eoyang: I think part of the challenge is the assumption behind that question is the degree of control and direction that the Russian state has over these actors and I think that is an open question, as to whether or not he really can, how much that is true.

I think it's certainly a problem where when these actors are going out there and with the tools that they have available through ransomware to [inaudible], they have the capability at any given time to sort of trip over, either intentionally or accidentally, something that is a significant impact to the United States.

So whether or not we can say definitively there will be no more Colonial Pipelines, I think that that's a little bit of a challenge and so it's all the more important that the private sector thinks about resilience and plans for the possibility that there may be an attack even as we in the government ramp up our effort to take it directly to the President.

DWG: Jenna McLaughlin with NPR News.

My question is actually a nice follow-up to that. Against the backdrop of the International Ransomware Summit, I think it was Australia, the UK and the Netherlands all put out pretty strong statements about further intentions about pursuing particularly criminal actors in cyberspace, those that threaten critical infrastructure, that they were capable and willing to take offensive actions in cyberspace against those actors and they were pretty specific and detailed about it.

I'm curious if you can talk a little bit about how those sort of statements, their general ethos lines up with [inaudible].

DASD Eoyang: I think that we would share that view, that we need to be much more aggressive about, that we are being aggressive against the ransomware actors. That is a priority mission for the Pentagon now.

Stepping back a little bit for some context. We have three main missions in cyberspace in the Pentagon. One is to prepare to fight and win the nation's wars; two is defense the DoDIN, defending our own system; and three would be to defend the nation. And in the defend the nation category, those are shared whole of government missions and you've seen the department work to defend elections and countering ransomware would fall into that third bucket of defend the nation mission where we are working with our allies, our partners, in the interagency and internationally to really go after the ransomware actor.

So I think we have strong working relationships with a lot of those countries and I think we are of a mind about the need to be able to impose consequences on the ransomware actors.

DWG: And do you think any of that is going to be sort of [inaudible] in public, and [inaudible]?

DASD Eoyang: I do hope it's been visible already. I mean we have seen some ransomware actors say publicly we're not going to go after critical infrastructure and I think that is very clearly a reaction to the United States saying going after critical infrastructure is not okay. But this is not just a U.S. problem. We have seen ransomware attacks with terrible consequences on countries around the world. So this is a global problem that we are working on with partners and allies.

DWG: Dmitry Kirsanov, TASS.

Sort of following up on Julian's question but also looking at it from another angle. What is the Biden administration's thinking on arms control, so to say, in cyber sphere? Is it necessary at this point of time? Would you like to do something like that with Russia, China, or even a multilateral agreement of sorts on that?

DASD Eoyang: Let me just say I think that we have strategic stability dialogues ongoing with the Russians and cyber is certainly a part of that. I think as the domain develops it's important that we understand, reach mutual understandings of escalation risk and the destabilizing nature of certain types of cybersecurity activity. So I think those conversations are ongoing and we would encourage them to continue.

I would just say the challenge of the arms control model, I know people tend to gravitate to that because it's been so successful in the international sphere, but one of the challenges of the nuclear deterrence and arms control model in the cyber domain is that it's not quite the same. In the nuclear arena you can do verification. We have physical weapons that you can count, you can locate. You have physical targets that you can talk about. In the cyber domain it is much more difficult to have that kind of a verification regime because if you had two sides with cyber, the cyber capabilities aimed at each other, and you said let's sit down and compare target lists, what everyone would do was compare their target, take the other side's target list and go home and patch. That isn't quite the same as in the nuclear domain.

So arms control is a somewhat challenging model in which to talk about establishing strategic stability in cyberspace. That said, we should certainly try to reach greater understanding with other countries about what activity in this domain means and what are acceptable and unacceptable activities in the space.

DWG: And how in general would you say those talks with the Russians are going on cyber in general? Anne Neuberger was saying that Russia did in fact take some initial steps and that the United States is looking for a follow-on. And there was a piece from David Ignatius last night. There is [inaudible], there is at least some semblance of cooperation. Are you seeing something different from the Pentagon?

DASD Eoyang: I would refer you to Ms. Neuberger to get her sense of what the talks have been. The relationship is not just about ransomware. There are a wide variety of other things that go into strategic stability. It’s not just about the non-state actor.

DWG: Thanks.

DWG: Justin Doubleday, Federal News.

I’m going to switch gears a little bit to ask about work force. I understand the department has been doing a zero base review of its cyber forces or cyber and IT forces. Maybe it’s done. If you can tell me now, it would be great. But what have you learned about, do you have the right amount of cyber personnel, the right skilled cyber personnel to get after some of these challenges you’re talking about today?

DASD Eoyang: I think one of the challenges with cyber work force is that we need to be very clear about the expectations for the Department of Defense in what the nation expects of us for defend the nation. Right now I think we are appropriately sized for the missions that we have, but if the nation were to expect us to do more, and occasionally we hear policymakers talking about DoD defending the nation alone, and I think that’s probably too aggressive. There are questions about like how far the policymakers would like us to go. So if there is additional mission then we’re certainly not sized for that.

I also think there is a question about how we sustain a robust cyber work force. Especially against an industry that is also in desperate need of skilled cyber individuals. And the industry is able to make financial offers to our people that we could never match. We like to think that we have missions that are never matched in the private sector and so that’s really important. But I think as we look to the next cyber strategy, thinking about how we mature that work force and put it on a sustainable footing, it’s really important.

DWG: Any new ideas on how you can get after those issues? Especially the retention issue.

DASD Eoyang: I think this is an ongoing conversation. I don't want to get ahead of it. But I do think that understanding where our retention chokepoints are and where it's a challenge for us is really important so that we're able to apply the right tools and the right model for that. I've had some experience earlier in my career dealing with this and I think of it sort of like the challenges that we had with airline pilots in the '90s. The department plays a really important role in training cybersecurity personnel which can feed a national shortfall. So we need to think carefully about how that pipeline works, both for the benefit of the department, but also the benefit of the nation.

DWG: Mark Pomerleau with C4ISRNet.

Going back to your initial comments about the cognitive domain. I know that one of the top priorities of your predecessor was more tightly linking information operations and cyberspace operations. And I'm curious if you've picked up that baton and how closely you're working across the OSD policy shop with folks like the Principal Information Operations Advisor to kind of more strongly link cyberspace and information operations in that cognitive domain.

DASD Eoyang: I think one of the challenges for us is we think about the cognitive domain is making sure that we are understanding the strategic orientation goals and objectives of adversaries. So from that perspective we want to make sure that cyber operations fit into a broader strategic frame for, that makes sense in the regional context. And the IO operations do the same. So there are places where we do have specific operations of very tight linkage, but really we need to make sure that it all serves the broader objectives and goals for the government with regard to particular regions and areas.

DWG: What lessons have you learned, either from a strategic defend the nation concept of deterring actors? Or even from a regional military perspective of [inaudible] and how to culture that going forward.

DASD Eoyang: One of the challenges that you see, especially if you think about the cognitive domain is it requires a lot of intelligence collection because you have to really understand the other side, what they're thinking, what their goals are And sometimes cyber and intelligence collection can be intention, and we obviously just need more of everything. So that is one of those areas where as we think about how to go forward, as we switch from 20 years of counterterrorism focus to the great power competition and China as the pacing threat, we need to understand better and more deeply the intelligence context.

DWG: Oren Liebermann from CNN.

I wonder what will be different about the next response to a cyber attack on critical infrastructure? Or is it just more of the same? The ransomware attacks are still out there even if they're not as clearly targeting critical infrastructure at the moment. But is it difficult to get someone else to reign them in? Is it just a matter of time then?

DASD Eoyang: I think this is an ongoing conversation and we have to take these things case by case because it will really depend who was actually behind the attack, how much direction or control is there, how big is the attack. So I don't want to get into specifics about how we might respond in a particular incident, and we'll have to just take that as it comes. But what is very clear is that it is a national security priority. You have seen a much more robust response from the U.S. government across ransomware attacks including the FBI seizure of the Colonial Pipeline proceeds. There are ways in which the government is being much more aggressive against the ransomware actors.

And I think that part of the challenge here is that in an ideal world we are disrupting and not reacting to the ransomware actor.

DWG: At what point does a cyber attack justify a non-cyber response? Especially since critical infrastructure is a national security issue.

DASD Eoyang: Again, I think this is on a case by case basis and it really depends on how we understand the attribution, how we understand the impact of this. I don't want to get ahead of what the decision process might be in a particular attack. But we have made very clear to countries around the world that we would respond to what we would deem the equivalent of an armed attack in cyberspace and we have very specific legal definitions. I don't want to get into like the wordsmithing of that because the lawyers will - they have very specific definitions and I don’t want to misstate them. But it is very clear that if something rose to that level that we would respond.

DWG: Lauren Williams with FCW.

I was curious how your office is working with the Cyber Advisors, particularly with the services and what kind of comes out of [inaudible]?

DASD Eoyang: The Principal Cyber Advisor for the department is collocated with my office. So we work very closely together, all the time. And one of the areas where we’re working very closely together is on the Cyber Posture Review and on the development of the Cyber Strategy. The division of labor as we’ve described it to folks internally is that my office is up and out and they’re down and in. They think about what happens inside the department. They work closely with the service PCAs on this. And as we think about the work force challenges, because the work force model means that cyber forces are recruited and trained by the services and then handed to Cyber Command, the service PCAs play an important role in understanding and helping us mature the cyber work force.

There are a lot of other places where they’re engaged with the DoD PCA, but I’ll let them speak to the specifics of the relationship.

DWG: Building on that, are there any sort of policies that [inaudible] in the cyber realm that you’ve noticed that you think should be addressed either specifically by your office or by the Cyber Advisors?

DASD Eoyang: We cover so much it’s hard to think of like particular gaps.

I think we have the authority to address the full range of things. I think one of the challenges in cyber is that it touches so many things that our ability to cover all of the places with the number of people that we have, we’re just really busy all the time. And so I think that is a challenge.

But there are cyber responsibilities federated across the department because it is involved in everything, so it just requires a lot of coordination.

Moderator: That's the end of the list of reporters who signed in in advance. I'm happy to open the floor.

DWG: Pat Tucker from Defense One.

I want to go back to something that you said in response to Julian's question where you described it as an open question the degree to which Vladimir Putin could control outside ransomware attackers. Because I get the impression talking to people that there's a lot of different opinions about how open that question is, and certainly the [quality] response where you're trying to recruit allies and have a kind of uniform pressure on the Russian government to crack down suggests that there's maybe more control than not.

So I wonder if you can clarify, how are you attacking that open question of the degree to which Vladimir Putin can control these attackers? And isn't that sort of important before putting in place a policy to pressure them, the Russian government to [inaudible] them?

DASD Eoyang: I would say one of the ways that you determine the level of control and influence that the Russian government has over the actors is by encouraging them to take action against them. And this is what the administration has been doing, again going back to the Experts Dialogue, and the President's conversations with President Putin. I would refer you to the Experts Dialogue to sort of again talk about what kinds of activities or actions they feel like have come from that.

But I think that the reason it's an open question is that we still see ransomware attacks emanating from Russian territory. No one has been able to successfully deter crime to zero in the history of humanity, so I think that there are some limits about how far that can go. But certain kinds of attacks, I think there are questions about what the Russian state's commitment is to engaging in these kinds of activities, or to people who engage in these kinds of activities from their territory.

I would also say that one of the challenges we in the department see, and you see this in the indictments against some of these actors, is that some of them have connections to the Russian state. They use their skills that they've developed in service of the state for their own personal enrichment. And that is something the United States would never do. Anyone at Cyber Command or NSA who thinks that they're going to go home and like conduct a ransomware attack against a city in Russia, the FBI would like to have words with them because that is just not something that we would view acceptable in the United States and we would take law enforcement action against those individuals.

We believe that responsible states should take responsibility for the actions of their forces. That their forces should only do the things the state asks them to do and not be engaged in this kind of personal enrichment, and we would never allow that in the United States. I think the allies that Jenna was talking about would also not allow that kind of activity from their forces. But we see in some of the criminal indictments that have come forward that that's not the case in other countries. I think that as a norm of responsible state behavior, as the United States military, we believe in discipline of your forces and we would never tolerate that.

DWG: I wonder if you could talk a little bit about the department's policy in using artificial intelligence in [inaudible] cyber operations. There's a principle for AI that guides kinetic operations necessary [inaudible], but when you get into the use of AI in targeted offensive cyber operations, the principles don't touch on them as much. It's sort of outside the domain.

So can you talk a little bit about your thinking there?

DASD Eoyang: I know that the head of the [JAIC] had talked a lot about the ethical use of AI and in cyber operations we continue to abide by all of the norms that are set for us in the kinetic space. So just because it's cyber does not mean that we don't adhere to [LOAC] and the ethical principles would continue to apply to the department across all domains.

DWG: Nick Shifrin, PBS News Hour.

Can I ask a specific one about something that you don't want to answer, and then a question about norms that goes to Dmitry's question [inaudible].

The U.S. government shared specific names with the Russian government that it wanted law enforcement action to be taken against, and we did see the disappearance, the darkening of some ransomware actors. As far as the U.S. knows, is that because the government of Russia took action?

DASD Eoyang: I don't want to attribute particular motivations to the reasons why [people] go dark or don't. We have seen a number of these ransomware actors go dark and rebrand and come back again later, irrespective of any activity of the Russian government.

As to what the specifics might be in that, I think this is a question of how we see the activity continuing.

DWG: And then [inaudible] to use [inaudible] and to cite a specific example. The U.S. government sanctioned Russia over SolarWinds. It did not sanction - sorry, I should preface this by saying I want to talk about [inaudible] rather than criminal activity.

The U.S. sanctions Russia over SolarWinds. It did not sanction Beijing for the Microsoft Exchange hack. In the discussion within the administration about creating norms, was that decision made because SolarWinds represents a unique, different attack on the supply chain whereas the Microsoft Exchange was deemed traditional espionage? And obviously my question, are you trying to create this norm, and have you guys created that [inaudible]?

DASD Eoyang: Stepping back from the norms question, I think one of the things when we think about responses to malicious activity, it's important to think about what the effect is going to be on the malicious actor. This goes to the cognitive domain piece of this. Russia and China are not similarly situated in terms of how they think about malicious activity. Remember SolarWinds was part of a long history of Russian maligned activity, state sponsored and otherwise. And so looking at SolarWinds in isolation and not as part of that broader pattern would lead you to a very different set of conclusions and responses than if you look at the entire pattern of activity. It also, part of the response is about how the state is likely to react. And with the Hafnium attribution, what you saw was not just the U.S. attributing that activity but countries around the world attributing that activity. And the two countries are just differently situated.

So what might be necessary to encourage people to a certain kind of behavior will differ as we look at the particular countries.

So this is not just there is a particular hammer and we're going around hitting everyone with the same hammer, but we're thinking about how do we calibrate those responses in light of the other countries.

DWG: So the countries around the world attributing that activity, are there fewer countries around the world willing to attribute activity to China because of China's economic clout?

DASD Eoyang: I don't want to speak to the motivations of other countries, to attribute or not.

But I do think the two countries are very differently situated when it comes to malicious activity. You've seen China, for example, ban crypto exchanges on its territory which creates a very different environment with relationship to criminals than what we have seen in Russia. You've seen Russia taking much more aggressive activity against cyber action against states on its periphery. Disruptive activity.

So I think the two countries, we have to think about them differently in terms of what they're doing, and you'll notice in the Hafnium attribution, one of the things that we really called out was this creation of an ecosystem, an ungoverned ecosystem. And that is actually really important. Again, going back to this idea of like discipline of forces, we want to encourage states to instill that discipline on their forces to not create tools and vulnerabilities out there that are used willy-nilly, and to be more targeted in their activity.

Now that's not the only thing we're trying to accomplish in cyberspace, but that is one of the things we're trying to accomplish in cyberspace.

DWG: Why can't we answer that norm question? Like shouldn't it be a norm that we don't try to do espionage that affects 15,000 systems around the world?

DASD Eoyang: Espionage is the second oldest profession in humanity so I think there are changes that like you're going to stop espionage, that seems kind of futile to me. The United States has national security imperatives in intelligence collection, other countries do too. I think the question is how. And how people go about it, how they do that without creating collateral consequences, how they do that without undermining the trust in the ecosystem. It's a difficult thing to set norms about. It's not something that anyone likes to talk about openly. But we do our best.

DWG: Travis Tritten, Miltiary.com.

You said cyber touches on so many different things and I wanted to ask you about freedom of expression and privacy of U.S. service members, particularly on social media. DoD [inaudible] program is looking at the ways that it can monitor social media and pull information that it can use. And also with accessions, there's been discussions about looking to root out extremism when people are recruited after January 6th, and how you can look at social media to identify that type of extremist behavior.

Can you talk at all about DoD's powers and responsibilities where it's power to hoover up this information and use it, and where it's U.S. servicemembers' rights as citizens begin.

DASD Eoyang: That's not one of those things that's in my office's area of responsibility, the sort of how we think about the internal counterintelligence concerns of our forces and I'll have Beth get a better answer and get back to you on that one. I don't want to --

DWG: Who would make that overarching policy? Is that something that's left up to the services? If it's not cyber policy from your office, who would set those guard rails?

DASD Eoyang: I think this is a question for the lawyers. For OGC to think about what the appropriate boundaries are of that, so I don't want to get into the specifics of a complicated legal question on where we have two values that we care about very much in tension with each other. That's a hard line to draw and I'll leave that to the experts.

DWG: Can you talk at all about guard rails, about DoD's ability to collect information domestically on social media and such?

DASD Eoyang: The department's authorities are pointed outside the United States and most of our intelligence collection is external to the United States. We do have some limited counterintelligence authorities to make sure that we're protecting our own information and we're looking after threats to our own things and people. But as to the specifics of that, again, I'll leave that to the people who focus more closely on that day to day.

DWG: Matt Beinart from Defense Daily.

I wanted to follow up on the AI question. Is your office supporting any kind of specific efforts or projects at the Joint Artificial Intelligence Center focused in the cyber or threat deception [face]. I know [inaudible] working with detecting anomalous activities. Any sort of specific projects?

DASD Eoyang: Let me take that one for the record just because I think there are a large number of R&D efforts that are ongoing about how we think about cyber or how we think about maturing the space. Let me get back to you on that one.

DWG: Maybe in a broader sense, how do you view maybe the state or the maturity of AI at this point right now to maybe help bolster threat detection or cyberspace [activity]?

DASD Eoyang: I think the real challenge because of the variety of malicious activity that we see and the ways in which our adversaries are constantly evolving their tactics, you need a certain body of information to be able to do that kind of predictive analysis. I think we obviously would be really interested in getting to a more mature understanding of that, but it's a real challenge.

DWG: Katrina Manson of the Financial Times.

I was wondering how you had responded personally to the resignation of Nicolas Chaillan, and what lessons, if any, you took from - I guess there were things that he made clear had upset him and some were bureaucratic, some were personal, and some were about just the state of the cyber [component].

DASD Eoyang: I think many people in the department have different views on things, and it's a large bureaucracy and there are certainly challenges, working within a bureaucracy. I don't know him.

But I think that we do view, to some of the points that were raised, China as the pacing threat and I think that the technology areas - cyber, AI, things like that - are very important for development and they've been made a priority in this administration.

I think this is a long term challenge and that this is the challenge of the remainder of my career and probably many others, that we did not solve this problem in three years is unsurprising to me, but some of us choose to take these things on because they're hard and we'll continue to work at them. They're complicated. And it's important that we do them, but I personally am not throwing in the towel.

DWG: What did it tell you about the difficulties of retaining talent that you manage to recruit from the private sector? You mentioned competition earlier. Is there anything DoD needs to be thinking about doing to try and retain talent such as --

DASD Eoyang: We have created over time a number of areas where we can leverage that talent and we still do that. There are a lot of areas where innovation and bringing in that talent continues and provides tremendous benefit for the department. We've done things like creating the Cyber Excepted Service. There are rotational programs. I think we are always still looking for additional ways to bring that talent into the department and create a healthy pipeline and relationship with the best.

But one of the things it says to me is that the strength of American technology and the strength of our national security is not only to be found in the Department of Defense and that many people contribute from the private sector and that is essential to us as a nation. So as individuals leave the department and return to the private sector I hope they will continue to work on some of these challenges from the outside. There are certainly ways in which the private sector may be more nimble in solving some of those challenges and the department will continue to work with them wherever they are.

DWG: Mark [Inaudible]. Good morning.

DASD Eoyang: Turning back to ransomware, everyone's [inaudible]. I'm trying to zoom out a little bit. You used the word aggressive a lot in your first couple of answers, and you used ramping up effort to take on the criminals. So it seems like DoD has already done a shift from [inaudible] criminal activity and supporting interagency to [inaudible] national security threat.

Is it just stuck on now a plane of like DoD's stake in the interagency in the space is only going to grow, or might it shrink one day in your opinion?

And then sort of building on Jim's question about public facing efforts on this, DOJ heads a Ransomware Task Force. [Inaudible] task force or something like that out of DoD?

DASD Eoyang: I don't want to speak to specific activities the department is engaging in to support all of those activities, but I think the questions about whether or not our activities grow or shrink will be threat dependent. We have recognized it as a national security threat and we have put resources against the problem. And there are many parts of the department that continue to work on ransomware both overtly and not so overtly. The Defense Cyber Crime Center has been very involved in understanding the ransomware actors and understanding where we may have incidents against the defense industrial base itself. And then we have tremendous capability to provide insights and targeting information to our law enforcement colleagues to take additional action against criminal actors.

DWG: One effort that has been talked about publicly by General Nakasone is this idea of a surge across Cyber Command NSA. Rob Joyce has said [inaudible] State, Treasury, other departments in order to get smarter on the threat of ransomware. Can you shed any light on what this surge would actually entail? The number of people? Are there MOUs being written between the various agencies in terms of what information we share?

DASD Eoyang: I would say that we have been working really closely together on all of these things and the interagency focus on ransomware and the areas for collaboration have increased. I don't know that I want to put specific task force names to things. I know the department loves to name task forces. We can also just have plain old emergency cooperation without naming everything.

But I do think there are a lot of ways in which we are working closely with Treasury, DOJ, FBI, to ensure that we can take more aggressive action against ransomware.

I spent a lot of time, as some of you know, working on cyber crime prior to this job and there were a lot of ways in which law enforcement has made tremendous strides from where they were to where they are even today in focusing on these things. And I think that's of tremendous benefit to deal with this problem.

DWG: Aaron Schaffer, Washington Post.

I was wondering if you could speak a little bit about how DoD weighs the equities of victims when weighing disruptive activity against ransomware groups.

DASD Eoyang: I would say this is really a question for law enforcement as we think about those things. We are obviously very concerned about what happens with, what's been happening to victims which is in part why we have raised this internally, raised its priority as a national security priority. But as to individual cases, I think I can't speak to how - those decisions are complicated and I don't want to get into them.

DWG: In general, like even taking actions against broader groups or sort of on the nation state level. Is there sort of an equities process that you all are sort of weighing all those perspectives?

DASD Eoyang: I would just say that under our current policy guidance for the department's offensive activities there's a robust interagency coordination process and a lot of equities get weighed in that process.

DWG: I think it's safe to say the reason we're talking about ransomware is it's sort of the [inaudible] right now from the classic attack to double extortion and [inaudible] distortion. Three or five years ago we would have been talking about something else.

I wonder what is the type or style of attack we'll be talking about next? Is there an emerging trend DoD's or cyber's keeping an eye on?

DASD Eoyang: Look, I don't want to predict the future. I think you can talk to the DNI's Futures Group about what that is. If I knew what the next generation of attack was - I think it's hard to predict what the next range of things would look like. As you look back, the department has been traditionally worried about intellectual property and loss of defense information, and now we're seeing these disruptive attacks in ransomware. I think it's a constant evolution of how we respond to the attacks, how we make it more difficult for the adversary, and then the evolution of where they go from here. I think there's a relationship between those things that we'll just have to see how it unfolds.

DWG: A quick question on authorities. [Inaudible] when officials testify in front of Congress and if they have the correct authorities they need they usually say yes. But I'm curious, as you're working the policy piece of that are there maybe for lack of a better word friction points or areas for improvement within the authorities we already have that you're still kind of working through as DoD's [inaudible] inflection point you talk about with cyber operations?

DASD Eoyang: One of the big things in 2018 was in the Defense Forward we were given a bunch of authorities, both statutory and internal to the government. And I Think the question is not one of authority. It's a question of execution of authority and how we posture ourselves to sustain and continue to operate and to make full use of those authorities. So there's a reason why we keep saying we have all the authority we need. There are many things that go into effective operations. Authorities is just one piece of it. There's also manning, resourcing, doctrine, all of these other things, and all of that as we get more experience in the operational space, we continue to evolve.

Moderator: Before I invite Ms. Eoyang to give some final comments, I wanted to once again thank everybody for coming today. The goal of the Project for Media and National Security is to elevate debate on this important topic and being a retired journalist after 40 years I get to express opinions for the first time, and that was a marvelous, marvelous presentation. I learned a lot.

Thanks as always to the Howard Baker Forum. Without their generosity we couldn't be here today.

The floor is yours, ma'am.

DASD Eoyang: Thank you very much for all coming. I really appreciate this engagement. I think the reporting that we see is really important to us. It helps shape the ways in which the American public, policymakers and academics think about cybersecurity. So I appreciate all the work that you do to not only explain what we're doing but also hold us accountable for the things that we have said and the things that we continue to do, so I really appreciate that.

I would just urge you as you guys think about and write about cyber to really think about the assumptions that underlie the ways in which you write about it. And Thom and I have talked about this since he edited David Sanger's book, but talking about some of these things as weapons and arsenal and sort of analogies that we use from traditional warfare may or may not be accurate when it comes to cyber. And in many cases they're actually not accurate and they're not helpful for people understanding the debate.

DWG: They're not the perfect weapon? [Laughter].

DASD Eoyang: One of the things about cyber weapons is that it's not the same as a nuclear weapon. A nuclear weapon will make a space unlivable and deny access to it for generations. Cyber weapons may be decisive in the sense that they change things at a particular time that make a difference to an adversary's calculus, but as we saw with Colonial Pipeline, eventually people who are determined to reconstitute and continue their operations will do so. So it is a time-limited effect. People come back online. Just because Colonial Pipeline was hit with a ransomware attack doesn't mean that they are permanently offline.

So we have to think about the impact of these things not as the kind of kinetic weapons that leave things a smoking crater for a long period of time, but about was the will to reconstitute, you would not want the United States to just lie down in a ditch after a cyber attack. We work very hard to continue to be up and running as quickly as possible after any type of incident for us.

So I think some of these analogies on weapons and arsenals, on arms control leave people to certain mental models of thinking about cyber which are not exactly accurate to the way the domain operates.

I'm always happy to talk to you guys. Ross [Inaudible] down here at the end of the table is happy to arrange further conversations if that's something you guys are interested in. But I thank you guys all for coming out for breakfast and meeting me on DoD time schedules.

DWG: Thank you very much.

# # # #