Mieke Eoyang
Deputy Assistant Secretary of Defense
Cyber Policy

Defense Writers Group
Project for Media and National Security
George Washington School of Media and Public Affairs

15 September 2023

Moderator: Welcome to this Defense Writers Group with Mieke Eoyang, the Deputy Assistant Secretary of Defense for Cyber Policy. As I told her in the elevator on the way up, now that I'm no longer a Times reporter and am allowed opinions, I think the work that DASD Eoyang is doing is incredibly important and I've found her to be a forceful and intelligent advocate of her issues. And every time I talk to her, I get smarter so I hope that you all are here to do the same thing.

The ground rules, as always, this is on the record. Please record it for accuracy and quotes, but there is no rebroadcast of audio or video. I know you all get that.

I'll ask the first question, then we'll go around the table for others. Eight of you emailed in advance. We'll do those first. Then whatever time is left at the end we'll go to others.

My opening question is somewhat general but very important. You and I have talked before about the importance of definitions. Cyber weapon, cyber tool; cyber war, cyber what. Could you walk us through the most significant changes between the earlier Cyber Policy and the one that you released? I see major shifts in offense and defense and STRATCOM and all that, but rather than me try to be a Talmudic scholar and interpret it, I'd love to have you do that for us.

DASD Eoyang: I really appreciate the question because I think there are a lot of folks who are wondering why did we do an update 2023 strategy off of the 2018 strategy. In many ways, the 2023 strategy does represent some continuity with the 2018 strategy, but given that we have a National Security Strategy, a National Defense Strategy, and a National Cyber Strategy, there was a framework of strategic guidance into which we needed to think about how do we bring cyber to bear across all of those things.

So there’s a piece of this that is about cyber and its role in integrated deterrence from the NDS. And then there are some shifts that reflect our real world experience for the department in the time period between 2018 and 2023 to include our experiences of observing the conflict in Russia-Ukraine that have shaped and refined our understanding of the role of cyber in warfare, the ways in which we defend the homeland, and of course the importance of working on strengthening the cybersecurity of our partners and allies. And those are I think the three big things that are shifts for us in this.

To go through that, I think part of the challenge on the integrated deterrence piece is that a lot of people often thought that cyber war was a thing that occurred in its own domain and there were cyber for cyber responses. And what we have seen is that it’s not about cyber for cyber. Cyber deterrence as a concept is a misleading concept. Instead, it’s about integrated deterrence and how does cyber play a role alongside of all the other elements of national power, all the other capabilities in the Department of Defense, to enable, to provide optionality with those other things.

On the defend the homeland piece of this, there had been a sense and people were persistently asking us in the department why were we not on the networks inside the United States to defend the nation from all these cyber attacks? What we have discovered is that’s not a posture that we are going to maintain. Our authorities in the Department of Defense are pointed outside the United States. We’re not pointed at the American people. There are domestic agencies that have responsibility for cyber inside the United States. How do we work better with them to defend the networks? And those networks are often run by private sector actors who know them intimately and operate them day to day. In a crisis, the theory that says we're going to send a bunch of military personnel and say, "Hi, we've never seen your network before, but we're here to help" is I think one that does not match the technical reality of that.

So what you saw from us on the outside of the Russia-Ukraine conflict was sour participation in the Shields Up activities run by DHS which is that we worked very hard to push what we knew about what the adversary could do with our domestic agency partners to the private sector so that they were better able to arm themselves, and we remained postured to try and disrupt those threats before they come to the United States. That's a different theory about how we will defend the United States, but we think it's a better model for us in the Department of Defense and one that allows us to also maintain the focus that we need on our warfighting mission.

The third thing we talk about that's a shift between this one and the last one is our emphasis on partners and allies in cybersecurity. Some of your outlets have reported on some of the efforts that we have undertaken to improve our cybersecurity with our partners and allies and our recognition that where we have shared networks, their cybersecurity weaknesses are our cybersecurity weaknesses. We need to work together to address them. And our cybersecurity weaknesses, frankly, are their cybersecurity weaknesses. So we need to work together to do that.

Our tools in the Department of Defense to try and improve those networks, it's not something we have thought about or matured particularly and that is on our to-do list as directed out of the strategy.

Moderator: Great. I have ten more questions, but I want to be a good host to all my friends and colleagues, so the first question goes to Joshua Keating of The Messenger.

DWG: Thanks. I was wondering what you're most concerned about or what you're seeing in terms of threats to the 2024 US election and how those threats might be different this time around given the evolving technology and capabilities around [inaudible].

DASD Eoyang: Election defense remains a no-fail mission for the Department of Defense. The 2016 election and our experience there fundamentally changed our orientation towards offensive cyber and we have had an election defense mission since the 2018 elections. So we work really closely with our interagency whole of government partners on how we defend that. As you know, elections happen inside the domestic United States. The military is not actually involved in that part of it, but we are part of the whole of government theory and plans for how to do that.

I think that we are very concerned about it. There are certainly malicious actors who have every reason to try and get better foreign policy outcomes for themselves by trying to change the minds of the American people, so we are constantly on the lookout for foreign maligned influence.

I think at this point it's a little hard to say how the threat landscape will evolve, but certainly we are worried about the ways in which technology might enable different kinds of approaches to this. But I don't want to get too much into the details of how we're seeing the threat because this is still something that is coming towards us as opposed to something that's behind us.

DWG: I'm just curious, given what was reported recently about China's use of AI in the Maui fires, to spread disinformation about, is that sort AI-enabled misinformation approach, is that of particular concern when it comes to sort of political -- to elections and political security --?

DASD Eoyang: Certainly generative AI as a means to try and help people who may have not a particularly wide range of language skill affect a nation where they don't speak the same language is a concern, and their ability to get better at that is a challenge. Certainly PRC is one of the actors that we are quite concerned about when it comes to elections defense and foreign maligned influence. And I think our concern is that they will see the value in that kind of misinformation/disinformation and use those tools to get better.

Moderator: Net question is Julian Barnes of the New York Times.

DWG: I want you to talk broadly about the sort of cyber competition with China and two points, one to sort of follow up on the previous question. Do we think China will play a role in election interference in 2024, akin to Russia in 2016? And we've been dealing with a number of Chinese cyber intrusions and perhaps most worryingly is the "living off the land" exploit that has affected military bases. I'm wondering if you can give us an update a little bit on mitigations about that, and what you can say publicly about how concerned we should be about that capability.

DASD Eoyang: The first question, just to make sure I got it, was following up on PRC elections and how we see the landscape evolving?

DWG: How is China in this cycle going to be Russia in 2016? The Maui fire sort of efforts raised them adopting Russian tactics.

DASD Eoyang: I think the question for another country that is thinking about engaging in election, in maligned activity with regards to a US election is whether or not the outcome on the other side of that would have a substantive difference for them in terms of their position relative to the United States.

I would just note that the activities the Department of Defense is undertaking with regards to our ability to counter China received broad bipartisan support. I wish I could read Xi's mind on this one. It would be really helpful for a lot of things that we're doing. But I think that's a calculation they will have to make about whether or not they see that kind of fundamental difference that would make it worthwhile for them to engage in that kind of outcome.

I think with regards to Russia, there's a very clear difference of approach, and they saw that in 2016.

On the "living off the land" techniques and the Microsoft Volt Typhoon report, we see that as very troubling. We see that as very troubling in a couple of ways. One is the sophistication of the actor. The "living off the land" techniques show the importance of people moving to zero trust network management tools to be able to better monitor and log network activity to be able to identify things that look anomalous and be able to figure out if that's in fact just something weird or that's actually malicious activity on their networks. So we would really encourage people to lean forward into being able to do identity in access management, anomaly detection, those types of things.

Secondly, the "living off the land" techniques and what that suggest about where China is prepositioning suggests a theory of disrupting military mobilization but also of sowing chaos in the United States. And for the United States military, while we don't like people trying to interfere with our military mobilization, we understand why people do that. But it is the second piece of that, the sowing chaos that would cause harm to the American people that we find an anathema. That is not something that we, the United States military, would do to deliberately harm civilians with no military nexus there.

Our obligations under the laws of armed conflict would require us to have some kind of military necessity in the operations that we would conduct. So to the extent that the PRC thinks that is acceptable, we point back to all nations' obligations under the laws of armed conflict to avoid civilian harm, to follow the principles of proportionality, discrimination and necessity. So we have some real concerns about what that activity might mean.

DWG: So if you're penetrating a military base for a military effect in the context of a conflict, that is allowed under armed conflict. If you are trying to turn off the lights in a major American city or cripple a hospital in an American major city, that would be impermissible.

DASD Eoyang: I would refer you back to the ICRC on the specifics of this, but I think we have very strong rules about interference with medical care, first responders, things like that. I think those principles really do matter to us. Again, we think it is wrong for other countries to engage in this kind of -- I take that back. While we might understand, we are going to do our best to prevent countries from being able to preposition to disrupt our military. If we caught them at it and we knew who those people were, we might have something to say about attribution and holding people accountable for that. But there are rules about the conduct in the war. There are norms about peacetime conduct. I think we very much would consider imposition of harm on the American public beyond the pale.

Moderator: Next is Lauren Williams of Defense One.

DWG: Thank you for doing this.

Can you talk a little about implementation and metrics for success? You mentioned earlier that the strategy of [inaudible] situation from [inaudible], but cyber is an ongoing thing. So can you talk about how you guys are going about measuring yourselves to make sure that you're actually getting after the things laid out in the strategy?

DASD Eoyang: We got asked this question a little bit when we did the roll-out in the briefing room. I think the specifics of how we're going to measure some of those things -- because the actual strategy document is a classified document we're not going to be able to get into. But I would just say that the department, we are big believers in metrics and big believers in implementation strategies. We did have an implementation strategy from 2018 to make sure that we were making progress along those things, and also Congress has requirements for us on a periodic cyber posture review, so we do have mechanisms in the Department of Defense that we use to make sure that we are moving forward with that. But I can't give you like an A, B, C, D grade or point to things that we are going to do because I think some of those things are going to be quite sensitive.

DWG: But more broadly is there an updated or a new implementation strategy in how [inaudible]? Or is this kind of going along with what you already do now?

DASD Eoyang: This is a yes. I don't want to get ahead of where we are on that. As I said earlier, the strategy is a to-do list and not a report card. So how we move forward on these things, how we measure ourselves on that, we will have to report on that to make sure that we are making progress. This is not just a rhetorical document. But I feel like I can't get into the specific details on it.

DWG: Next is Demetri Sevastopoulo with the Financial Times.

DWG: Can you talk a little bit about what China's doing in the cyber area that might help it if it decided to move on Taiwan at some point?

DASD Eoyang: We are -- Let me just start by saying we think the PRC has very sophisticated cyber techniques, but we and they have been carefully observing the Russia-Ukraine conflict to figure out how cyber best enables or doesn't military activity. And we see signs of PRC activity to disrupt Taiwan already. We saw after the Pelosi visit a significant uptick in disruptive cyber activity in Taiwan.

I think we worry about disruption to their critical infrastructure. We worry about ability to cut Taiwan's communications. I think that we still believe that cyber can be a critical enabler in armed conflict but it is not the way that I think we anticipated before the conflict. How exactly the lessons of Russia-Ukraine are landing with the PRC I cannot say but we certainly expect that cyber will play a role in, if any conflict may occur.

DWG: Can you give maybe one or two specific examples of lessons learned?

DASD Eoyang: One of the things I think we saw -- well, there are a couple of things.

One is that we saw the importance of cloud migration during this conflict. The ability of the Ukrainians to move their data extraterritorially but still maintain access to it was really important. Data localization laws can be a bit of a national security issue if you have limited territory.

We saw the value of the Ukrainian people being able to continue to tell their story to the world. That denied Russia the information environment that they were seeking at the outset of the war and the narrative that they were trying to put out there. From this perspective, the ability of the citizens of Taiwan to be able to talk about what is happening to them, not just official channels, is really something that I think is of value to the world and I'm sure to all of you as you would report on any such conflict.

The third thing I think we saw, the Russian attempts to disrupt satellite communications as something that I think many people are still trying to understand the aggregate effect of that on the conflict, but certainly it is something that we are looking at very carefully. The telecommunications structure for Taiwan is different than that of Ukraine.

Moderator: Next is Courtney Kube of NBC.

DWG: You said at the briefing the other day that there was a sense that cyber didn't have much of a decisive effect on warfare in the Russia-Ukraine conflict. So I don't understand, do you expect it's going to have -- I know you can't predict the future, but it sounds like you expect it to have a much bigger impact in Taiwan if there's a conflict with China.

DASD Eoyang: One of the things that we saw in Russia-Ukraine was the importance of integrating cyber alongside other things and that's a matter of planning, patience, things like that. So I think we do worry about the relative strategic patience of parties there.

I think we also -- One of the things we have learned here is that the kinetic conflict is different than what we expected cyber to do on its own. So cyber has an important role to play in conflict. It's just not the role that I think we expected it to play at the outset of Russia-Ukraine, but we do expect cyber to play a significant role in a conflict but it would not be a cyber by itself role.

DWG: I have to ask you about, since you mentioned the satellite communications read over Ukraine, the reporting on Elon Musk and Starlink. Has there been, was the US military, the Pentagon, aware that Ukraine was asking for additional coverage in southern Ukraine and Starlink denied it? And have there been other cases like that where they requested or Ukraine has needed some additional communications capabilities that have been denied and may have had an impact on --

DASD Eoyang: I'm not going to comment on conversations between a particular company and another country. I'm not in a position to comment on that.

DWG: But that's a [inaudible] you're aware of, not talking about even a specific case or specific company, where there's been a request for additional communication capabilities that Ukraine has needed that's been denied by a private --

The reason, not to just put aside the whole Elon Musk show, [inaudible] whatever. But I think one of the questions going forward, especially if you're talking about a conflict in Taiwan, is would the DoD have some sort of a role in ensuring commercial satellite communication capability?

DASD Eoyang: Not to get into the specifics of particular contracts, particular conflicts, I do think one of the things the Russia-Ukraine conflict did show is that commercial providers, telecommunications and internet technology services can have an impact on the conflict, and what the role of those companies is, what their status is, how they make those decisions in an armed conflict, especially in a future one, is something that I think we need to understand better and that's a conversation that needs to happen on an industry-wide basis so that companies understand if there were to be another armed conflict what would they want to do or not do, what is their exposure or not. But certainly where those services are provided to militaries, the militaries need to have some understanding of what they can rely on.

So I think that is something, this is really the first conflict we have seen of that nature. That industrial/military relationship is one that I think is an ongoing conversation.

Moderator: I'm going to use the power of the chair to follow on that.

It does seem the point you're making is that public/private partnerships are essential. Whether it's cyber writ large, AI specifically. I mean Colonial Pipeline affected hundreds of thousands of Americans, millions, and they didn't even talk about it for a couple of days. Right? They were afraid to share what was going on. So how do you as DASD Cyber try to develop a public/private partnership of trust for the defense of the American people?

DASD Eoyang: It is very important that we -- it's part of why this shift in our homeland posture. We recognize that these private sector partners are indeed partners, and that we need to be able to share information that is valuable to them. We need to enable them to be in a better position to defend themselves. That is a very different posture. We're not in one where we think -- There are compulsory tools that government has, but that is not actually I think the most effective way for us to engage in these relationships with the private sector. We have contractual relationships, we have cooperative relationships. And the shift for us in the relationship between us to the private sector to enable resilience, to have these conversations is really important. It forces us to be, I think, a little bit more, you know, come out of our shell a little bit more and have these conversations. And you're seeing that happen.

NSA stood up their Cybersecurity Collaboration Center which is an outside-the-wire activity to provide that assistance. That's a big shift for an organization that used to be referred to as No Such Agency, to have this kind of publicly known, outside-the-wire deliberate place to engage the private sector. But that's what's necessary.

Moderator: Next is Georgina DiNardo of InsideDefense.

DWG: I actually kind of [inaudible]. So [inaudible] reading [inaudible], I asked some industry professionals about what they would look forward to this new relationship between the department and private sector regarding [inaudible]. And they [inaudible] they would like to see a couple of things. Mainly corrective education and definition of the controlled information; ease compliance [inaudible] requirements; and further assistance with the current CMMC [rule]. Does the department plan on addressing any of those concerns? And if so, how?

DASD Eoyang: Starting at the back with CMMC, that is, as I understand it currently, notice in comment rulemaking, so that is a thing that I think the department intends to provide greater clarity on. But rulemaking across the broad swath, it is a process and so we're working through that. We expect there would be more later, but I would refer you back to the CIO's office who's running that for more details.

On the audit requirements piece, I'm not going to get into -- I would put you all to sleep if I got into audit requirements.

But on the controlled information, I think this is actually a challenge I've talked to some of my colleagues in the interagency about. Different industries have different standards for controlled information and how they talk about those things. That's a conversation that we need to make sure that we understand how people handle information controls in the energy sector versus the financial sector versus the IT sector so that we understand how to share that information out. This has come up fairly recently and this is I think, because we're talking about cross-sector information, more of a whole of government challenge in which the Department of Defense plays a role rather than one that is I think unique to us.

Moderator: Next is Sean Lyngaas with CNN.

DWG: A quick clarification in your response to Demetri's, if I may. You said after Pelosi's visit there were some deployment of disruptive capabilities in Taiwan by China. Are you referring to the --

DASD Eoyang: The web site --

DWG: All right. That was just --

Going back to Volt Typhoon, first with the strategy one of the lines that stood out to me the most was, you mentioned that cyber operations on their own can't really deter, that you need other tools. So how do you approach deterrence vis-à-vis China with that in mind generally?

On Volt Typhoon, has there been any -- you said it's unacceptable, [Roth Joyce] has said it's unacceptable because of the prepositioning. Has there been any communication or other signaling from the Pentagon to Beijing other than talking in the press that it's unacceptable?

And then lastly on Volt Typhoon, if I may, you have ground truth on the number of intrusions affecting military bases. In addition to anything else, in addition to Guam, have you seen additional prepositioning activity from that actor or other Chinese actors since the disclosure of that report?

DASD Eoyang: Okay, other networks other than Volt Typhoon. Let me answer that then I'll have you come back and --

I think you asked if we have fidelity on it. I think the challenge on this has been it's really hard to prove the negative and tactics, techniques and procedures change. We are persistently concerned about PRC intrusions into networks and it is something that we see network activity across the US government fairly frequently. The reporting about jamming [inaudible] emails and other things. So I could never say with fidelity that we know exactly where they are at all times. They are very sophisticated actors. But we do in the Department of Defense have very sophisticated tools to be able to identify that activity. But I'm not going to get into specifics about networks. You can understand why that would be sensitive from a security perspective.

The other question?

DWG: Just in the context of, well specifically on Volt Typhoon, has there been any communication between the Pentagon that we haven't seen in public?

DASD Eoyang: I can't comment on non-public communications. But I would just note that the government is working across a range of levels to continue to remain open to conversations with the PRC. I recognize that we are in a challenging geopolitical environment.

DWG: But if it were you, you would welcome discussions with the PRC? It's more of a State Department thing, but also it's been [inaudible] acceptable behavior in cyberspace, to include what you consider unacceptable.

DASD Eoyang: Yeah. We are happy to talk about it any time. They are welcome to call and I'll be happy to sit down with them to go over these things. And we are engaging in a verity of not just forums like this but academic forums and others where -- and with other countries around the world, to talk about how we think about acceptable and unacceptable behavior in cyberspace.

I would note that our colleagues in the UK have put out a report about responsible cyber power. So I think we are having a conversation to try and create clarity around what is responsible use of this power. We think democracies have a responsibility to be transparent -- not obviously everything, as much as you guys would like that -- but to create more transparency about how we think about that responsibility. And you have seen some states come forward and talk about that. We think it is an important thing to do in order to prevent miscalculation and unintended escalation from the cyber domain through the others.

Then I think coming back to your question on cyber deterrence, and people always ask has cyber deterrence failed because we see all this network activity. I think the fundamental question is to deter whom from doing what?

And we have not seen nation states launch cyber attacks on the United States that would rise to the equivalent of an armed attack kind of thing, which I think we have always feared. So from that perspective there is an argument that deterrence has worked. But that deterrence is backstopped by the conventional military power of the United States. For people who don't want to engage the Department of Defense, we have some deterrent value.

But I think there are other actors out there in the cyber domain who are able to cause disruptions that are still very significant, and a lot of those are criminal actors, which is why for the Department of Defense it's really important that we are partnering with our law enforcement colleagues to address that activity.

Moderator: Is arms control possible in cyber and AI? Or is that too using an old definition on a new problem that doesn't fit?

DASD Eoyang: I think you want to separate cyber and AI about the arms control question. I will leave it to you guys to talk to my colleague Dr. Horowitz about the AI questions.

But I think in cyber there are some challenges to the arms control model. People who would say well how about we'll both talk about a series of targets that we're holding at risk and then negotiate down from that. If the other side wants to bring me their list of targets, I would welcome that because then I'm going to go home and patch.

So like the verifiability of an arms control regime in cyber is quite difficult because unlike nuclear weapons that can be counted and have physicality to them, cyber is a clandestine capability, works best as a clandestine capability. The other side knows what you are doing. They will take technical steps to stop you from doing it. So this arms control model has some real challenges when applied to the cyber domain.

This is part of the evolution of the department's thinking on cyber. We did start cyber in STRATCOM, and a lot of that thinking on nuclear deterrence you saw reflected in our language. CYBERCOM has become its own stand-alone activity and our operational experience in this space has shown us that some of those framings do not work in this domain.

Moderator: A problem of definitions. Thank you so much.

Briana Reilly of CQ Roll Call.

DWG: Thank you so much for doing this.

I wonder if [inaudible] you talked about [inaudible] of cyber strategy is sufficient to [inaudible] with allies and partners. I was curious what that looks like when thinking about not necessarily deterring but responding to PRC aggression. What has that looked like up until this point? Are there any capability gaps that our allies and partners need to shore up in directly responding to a PRC --

DASD Eoyang: Cybersecurity is a shared challenge. While we may be a little further along on this, this is something that everybody is grappling with. And we are working with our partners in the region to help them think through their cybersecurity and shore it up as we go along. Especially for those places where we have US forces based, we worry very much about the security of our networks and where we are operating in alliance with them. We worry very much about the security of those communications, recognizing that adversaries have interest in getting between us and them, or getting in the middle of us and them, us and our allies that is.

This is something that frankly is on our to-do list in terms of the tools and how we shore things up. The department's security cooperation tools have been geared mostly towards weapon systems. The tools we have for cyber, we actually need to think about how to do that differently. We know how to do delivery of weapon systems, munitions, things like that. Delivery of cybers, in air quotes, I think it's a little bit more complicated given these are capabilities that are not uniquely military capabilities. A lot of them were provided by the private sector. How we the US government think about the range of assistance that we can provide across a range of networks. Not just military to military but whole of government is something that we're still working through.

DWG: Are there potential export control issues here? What [inaudible]?

DASD Eoyang: This is something that actually, again, I don't want to put everyone to sleep with this, but we do hear and are engaging with industry to identify particular bureaucratic barriers that they may be experiencing, and then how we are able to address them to be able to provide better cybersecurity.

We have, in conversations with the defense industrial base and others recognized a few of those things but we I think would like to address them more comprehensively as well.

Moderator: That was the last of the advance questioners. We have about 15 minutes before I turn the floor over. I saw you raise your hand.

DWG: Mark [Matishak] with [inaudible].

We've talked about a lot of topics, but last November at Aspen Cyber you said that Russia underperformed on cyber when it came to the initial invasion of Ukraine. Now you have the strategy saying that cyber is an aspect of warfare, not [as central]. That would [inaudible] where we sit today, what is the state of the cyber war in Ukraine? Is the cadence still very high? Is it going to go higher in the months ahead? Is it static? Is it lessening as the counteroffensive has begun? Where do you see this aspect of the conflict today? Then I have a follow up.

DASD Eoyang: One of the things that we talk about Russian under-performance, performance in cyber is often net defense, right? And the Ukrainian defense has been tremendous and has I think set an example globally of how you continue to maintain and run your networks when under pretty high duress. If those activities would happen in peacetime we might be thinking very differently about them as we did in 2015, 2017 earlier. So there are some real lessons learned there for defenders in that.

I don't expect that that activity would go to zero, and we still continue to see certain kinds of disruptions. But in terms of the long term imposition of harm against the Ukrainian people as part of this unjust invasion, I think that Russia needs to ask itself whether or not that is a value to it. There is certainly cyber activity happening. I don't want to say that it's not there, but the strategic impact of that relative to what's happening on the physical battlefield is I think not what they expected, and I think they are finding it much harder to integrate cyber than they experienced [sic].

The other thing that it points to is the value of cyber defense in the conflict and keeping one's own systems up and running as the priority for a lot of nations in a conflict.

DWG: So do you see that activity lessening over time? You said it won't go to zero. I don't expect it to go to zero. Do you see it lessening over time as we enter another winter and things like that going?

DASD Eoyang: It's hard to predict. Because I think these things change a bit with what's happening on the physical battlefield and what is going on with that. I think certainly -- I don't want to -- I'm not going to speculate on the future because I just don't want to be in a position of sharing my concerns in ways that advances Russia's.

DWG: My real follow up, Tuesday's roll-out of the strategy you were asked about the cyber force that's in the NDAA, which it looks like they're going to conference on next week. You said it was premature to say if it's the right model or not. I know you're working on Section 1502, the generative [inaudible] forces. But does the cyber, in your opinion does the idea of a cyber force merit study?

DASD Eoyang: We're going to study the question, and we've been directed to do that. We have the 1633 study which tells us to look at our model and alternate models, so we'll certainly look at the question. We already have an effort underway to do that.

I think the question is for people who think the cyber service is the answer to our cyber, our current challenges in cyber personnel management, be careful what you wish for. Again, I think there are some cons to -- A cyber service might have some benefits in ease of administrative management, but we have a variety of services in the Department of Defense, military services in the Department of Defense who perform a variety of missions. Those missions are enabled by technologies that are particular to those mission sets. Having a cyber service that is divorced from those particular mission sets may pose some challenges in understanding the warfighting needs of the services to provide cyber to enable that fight.

So we need to understand what the pros and cons are. There are certainly challenges to managing a career field that spans multiple services. There are challenges to jointness. I earlier in my career worked for Ike Skelton who was a big proponent of Goldwater/Nichols. The department did struggle with jointness to begin with. The question is which set of problems are we willing to live with? And taking a look at all these things, to understand that better before we throw out what we have in favor of something else, or decide actually what we have needs to be fixed, or there's something else completely. I think that is a study that we are taking very seriously because it is important in the Department of Defense for us to get people right, and we are committed to doing that.

DWG: We just want to see what the DDU was --

Moderator: The Space Force set a really high, high standard for --

DASD Eoyang: I assume whatever they are they would be pixilated.

Moderator: That was fast.

DWG: Mark Pomerleau with Defense Scoop.

Pre-Russia, I'm curious if you can articulate maybe what the department's assumptions were on the role of cyber in conflict. Access is hard. You have to have it ahead of time. War happens very quickly. What as the department's assumption that the role of cyber would be in conflict if they're learning now that maybe it wasn't what they thought it would be?

DASD Eoyang: I think certainly I but I think others, assumed that the disruptions to communications via cyber would be much more severe and have a much more strategic impact on Ukraine's ability to fight than it did. Ukraine's ability to be resilient and its will to fight surpassed those disruptions. But I think we expected, based on what we understood and understand to be Russia's capability in cyber, a much more impactful and integrated series of cyber incidents, malicious cyber activities, happening on the battlefield.

Russia underperformed in cyber. They underperformed in a lot of areas. They were, as I think many of you have reported, not particularly ready for the fight and the magnitude of the fight that they were engaged in. The planning is important.

DWG: I guess conversely, the US military has set up a lot of different mechanisms to integrate cyber with kinetic operations, traditional operations, [inaudible] commanders. Are you guys looking at maybe a rethink of some of those mechanisms based on these lessons?

DASD Eoyang: For those of you who haven't read it, I really recommend this article called "The Subversive Trilemma" which is an analysis of Russian cyber operations against Ukraine prior to the conflict which talks about some of the factors that make cyber operations hard. I don't expect you to report on this, it's an academic paper. It's quite long. But just in terms of people's background.

It talks about three factors -- speed, impact and control, or intensity. This may be how they phrase it but we can say speed, impact and control and how those factors play against each other. Sort of like in Silicon Valley, good, fast, cheap -- pick two. You can't have all three things. You can't have really impactful cyber operations that are well controlled on a very fast timeline.

For us in the Department of Defense, we're going to optimize for control because we believe in precision across a wide range of things. And so that means that for us to make sure that thing are impactful, it's going to take some planning. So I think it is interesting to assess Russian activity in this conflict. And thinking about the factors of timing for them, cyber is not a tool that is a responsive to battlefield conditions if you are seeing it on the TV and ask for the cyberists to address that thing, it's unlikely there's going to be much that is impactful to deliver at that time. It takes a significant amount of planning to do that or do that well. Or you risk what Russia experienced in [Petya] which is spillover and unintended consequences that are beyond what you anticipated and can be rebound and be harmful for yourself.

DWG: Now we know what the Guardians of Cyber Force are going to be called. The cyberists.

DWG: Thank you very much, Diego Laje with Signal Magazine.

I want to follow up on Demetri's question. You are concerned with coms denial of Taiwan. You're concerned with physical cables. Right? That's your primary concern. Just to clarify.

DASD Eoyang: I'm not going to go through the priority order of things that we're concerned about because that will just give our adversaries a targeting list, but we're certainly worried about the broad problem.

DWG: But it is the cables, right?

DASD Eoyang: They are in our list of things that we are worried about. I'm not going to say where they are.

DWG: Okay. I'd like to turn around your question, and it is what are we learning from our allies, countries like Estonia are in a cyber class unto their own. Right? What are we getting from them?

DASD Eoyang: We are in regular communication with our partners about best practices. And we are learning really important lessons from the Estonians, from the Ukrainians about the values of resistance, how to engineer your networks in ways that are helpful. Tactics, techniques and procedures. Our hunt forward operations are designed to help us understand better from those partners what kinds of malicious activity they are seeing and how we can use that knowledge to better strengthen our networks collectively. And that's really important for us. Thoe are activities that are part of our commitment to strengthen partners and allies, but really in many ways are for our benefit to understand adversary activity.

I think we will continue to do those. We continue to learn really important things from partners around the world because while the United States is a very big cyber target, we are not the only one.

Moderator: A few weeks ago we had Nate Fick, the first US Ambassador writ large for Cyber. Of course you're part of the same interagency. Do you interact with him a lot? Is his mission very different from yours? What's the interagency piece there?

DASD Eoyang: State and DoD work together a lot. I'm in regular communication with the folks at State Department which is something I did yesterday. We talk all the time. And Nate Fick's team is great. And we often do road shows around the world together, engage with international partners.

Moderator: You should add Julian to the road show list.

DASD Eoyang: Julian would love to be in the road show. You're not welcome. [Laughter].

DASD Eoyang: But the State Department does have a different remit than we do and some of the things they talk about on digital freedom, digital economy, standard setting, are not part of what the Department o Defense talks about. So we have complementary missions but they're not the same.

Moderator: Thank you so much.

The last question before I give you the floor.

DWG: I am Rishi. I am with Foreign Policy Magazine.

So I have a couple of related questions on contrasting Russia-Ukraine and a potential China-Taiwan conflict.

One is the private/public partnership. In Ukraine we saw Amazon, Microsoft, Google helping Ukraine move to the cloud. And then you spoke about Starlink to keep satellite communications active. How do you see the private sector's role in a potential conflict over Taiwan? And sort of the major similarities or differences of the two arenas?

A similar question with allies in the region. So say like Poland, Finland, Estonia versus South Korea and Japan for instance?

DASD Eoyang: ON the public/private partnerships piece, we do think that the private sector has an important role to play in shoring up the cybersecurity partners and allies. Many US cybersecurity companies are global companies and there is a lot of ground to cover. We don't expect that US government personnel are going to be able to be the sole solution for securing the cybersecurity of our partners and allies. So we have been encouraging our interagency colleagues and working with them to help those cybersecurity companies understand the international marketplace and do introductions where they can. I would refer you back to the Commerce Department for that.

But it has certainly been a piece of our efforts that I think you see us increasing, especially with regards to the Indo-Pacific. The conversations between US technology companies, State Department, Commerce in that region. I think we've seen an increase in those conversations. And a demand signal from partners, allies and partners in that region for greater US industry help in that area.

It's a little difficult to I think compare Europe to Asia in this. I do think that there has been increased conversations from our European and NATO allies about how they incorporate cyber into their warfighting capability. Obviously the fight for them has become much more concrete and real in terms of its possibility, and I think the same is true, frankly, in the Indo-Pacific. There is a rising concern about the possibility of armed conflict. I often talk to industry or various audiences and say cybersecurity has a risk management framework to it, and while people may disagree about how likely or on what timeline conflict may occur, it should certainly be in your risk management framework as something you are thinking about in advance of to manage. I see a lot of people shifting their thinking that way, to say okay, if this were to come, how am I going to deal with it? Which has led to a lot of increased conversations with industry.

Moderator: Thanks.

Before I give you the floor for final comments, I want to thank everybody who came today for your smart questions. I want to thank your staff for your support. And mostly DASD Eoyang, thank you for a thoughtful and thought-provoking discussion.

Now the floor is yours for wrap-up.

DASD Eoyang: Thank you. Thanks, Thom, so much for doing this. I did this at the beginning of my tenure here, I think some of you were there for that. And it's nice to be back because I feel like this document in particular reflects a lot of the thinking that's changed in the Department of Defense as we deepen our understanding of cyber's role I armed conflict. And the hypothetical versus the real of what has occurred in Russia-Ukraine I think really underpins a lot of what we're doing here.

I have been really impressed over my tenure here in the Department of Defense about the seriousness with which the department is grappling with cyber in that armed conflict and the urgency with which we are applying those lessons into our activities.

But I really appreciate all of you for being here because I do think as our perspective on this shifts, it's really important that people understand how that has shifted. I recognize that there has been a lot of suspicion of the Department of Defense and some of our agencies about what our role is in networks. And a lot of concern about the apocalyptic nature of what cyber could have been. I really appreciate all of your help reframing that conversation and understanding based on our real world experience what cyber is or what we observe it to be that's not informed by the hypotheticals.

I would also say that, not to throw shade on those people who believed where it was before, I think that historically as we look out at the range of vulnerability, across the US technology space, we did worry about that kind of catastrophic disruption. But recognizing how very hard that is to pull off, what that means in the context of better defenders, and the network defense has improved dramatically, I think that we are recalibrating how we think about cyber. So I really appreciate all of you and your excellent questions in helping us tell that story to the American people and to the world.

Moderator: Great. Thank you for your time. I enjoyed it very, very much, and as always, learned so much.

Thank you all for coming.

# # # #