REAGAN NATIONAL DEFENSE FORUM

PEACE THROUGH STRENGTH IN AN ERA OF COMPETITION

NOVEMBER 30 - DECEMBER 1, 2018
THE RONALD REAGAN PRESIDENTIAL LIBRARY
SIMI VALLEY, CALIFORNIA

DECEMBER 1, 2018
1:00 PM – 1:45 PM

PANEL 7
WINNING IN THE GRAY ZONE: COUNTERING RUSSIA & CHINA BELOW THE LEVEL OF ARMED CONFLICT.

Panelists:
• Congressman Jim Langevin, U.S. House of Representatives, Rhode Island
• General Robert Neller, Commandant of the U.S. Marine Corps
• The Honorable Nadia Schadlow, Former Deputy National Security Adviser for Strategy
Moderator: Mr. Julian Barnes, *The New York Times*

Video:
https://www.youtube.com/watch?v=4VrQQ1YLmso&t=0s&index=11&list=PLHNOi2zcxo7sBxM7HfhmB_tf6QXeqj48K

Barnes: Welcome everyone to the best panel of the day. I'm Julian Barnes with The New York Times. We have a really interesting topic here to discuss how the United States has found itself in this gray zone between peace and war. Operating against adversaries or would be adversaries, who appear more adept at competing just below this zone of armed conflict. China and Russia have been able to apparently alter international borders through operations calibrated just below the level to trigger a military response. So, we have a great panel today.

Barnes: I'd like to introduce them, and then we're going to dive in. To my right is Congressman Jim Langevin, who's a senior member of the House Armed Service Committee. Former member of the Intelligence Committee, who's done important work on cyber threats. Then General Bob Neller, the commandant of the Marine Corps. Anyone who's wondering why I'm reading my notes, may remember last year about my miss introduction of a member of the Joint Chief. So I did not want to promote General Neller to the head of a new Space Corps.

Barnes: Finally, we have Nadia Schadlow, the former Deputy National Security Advisor, and author and architect of the National Security Strategy that General McMaster unveiled last year here at the Reagan National Defense Forum. I wanted to ask everyone to start off by weighing in for a couple minutes on this topic. Does the US have the tools we

need to compete in gray zone conflicts? How do we respond to Russian and Chinese provocations against the US, against our allies? Nadia, would you start?

Schadlow: Sure, thanks Julian. I think we have the tools. We have various capabilities, and they're sharp and lots of the departments and agencies have them. But we're not necessarily putting them together in ways that are effective for this type of competition. I'm using the word competition specifically, because I think it's actually a better term than conflict. Conflict sort of assumes the beginning and an end.

Schadlow: Conflict also implies that the militaries in the lead for a lot of these competitions that are going on. So if we think about this as a competition, that requires us to think a little bit about persistence, about persistent engagement, about sustained engagement. And a little bit about campaigning, which is a useful military term that the Joint Staff and others have started to developed. So it's more of a long term campaign that we're thinking about, and I can expand on that a little bit later.

Barnes: General.

Neller: I don't know how you define winning. I don't think you're going to win in the gray zone, and I agree with Nadia. I mean, this is a long term thing. As Americans, I use a sport analogy, we like the field to be lined. We like there to be referees all around. We like there to be a defined period of time. The game only lasts this long, and we want someone to come out on top. We call fouls, you know, "You cheated. That's bad." The rest of the world hates American football. They like soccer. They like soccer, they go overtime, and then there's extra time, and Neymar falls down, and we all get angry. And everybody else is like, "He's just trying to win."

Neller: They pull, they fake their injuries, and we're appalled. The rest of the world is like, "You guys are stupid." That's the way this competition is, and it's a competition. We've all been watching. The Russians have a different style of this than the Chinese. The Chinese is much more economic, but it's just as insidious, and we got to compete. The military, we have to engage, and we have to build partnerships. We have to build partner capacity, but there are so many other elements and national power, they have to be engaged in this.

Neller: Again, lastly, this is not new. War or competition between nations has always been, at least at some point, below level of conflict. With information, with violation of treaties, with abrogation of international law. So I mean this isn't anything new, but I think we have to change the way we think about competition.

Barnes: Congressman.

Langevin: Sure. I think definitely we have the tools to compete and to win. I say win, I mean, the General is right, how do you define winning? My mind, we confront the challenges that we encounter, but we don't let it, hopefully, ultimately doesn't morph into a full blown war, conflict. I think that's how we define it as winning, that it doesn't escalate from there. So, we have the tools. I think that the danger is and what needs to change, is that they no longer siloed. It needs to be much more of a holistic, whole-of-government approach to confronting the challenges that we face in the gray zone.

Langevin: Whether it's confronting things like that's going on in the Ukraine. The little green men if you will, and working with Ukrainians or maybe non-traditional military. As we've adapted on the waives version of the NDAA, granting 1202 authorities to allow soft to train in the non-traditional military components, or in cyber. It's not just siloed and that capability for it's sake, but taking out a whole-of-government approach so that we're using all assets and tools of state power to confront in the gray zone.

Barnes: We will take audience questions at the very end if you submit them through the app, and you can get that at www.rdnf2018.org. So, we haven't been getting a lot of questions. I know that this audience will be a little more active. Pull out your phones and type in some questions. The Reagan Library's done a survey. Let's see if we can, with my clicker, get up the ... Oh I can, okay.

Barnes: The biggest concern's with Russia here, and we can see that the public has said, 30% support for Iran and other regimes. Invading other countries is only 11%. I'm curious to ask the panel, is the public seeing the Russian threat accurately, or is the threat of Russia meddling with its neighbors greater than the public says here? Does anyone on the panel want to weigh in on a thought there? General, you seem to have something.

Neller: Well, I mean I think that we all know that Vladimir Putin and others that grew up in the then KGB and now the GRU. They don't like the way that the Cold War ended, and they're trying to reset the history book. So, things that they've done in Ukraine and Georgia. Tried or threatened to do or have the potential to do in the Baltic States. Things that they do in other former Soviet Union block states. I think it's understandable that most people aren't as concerned about that, but they are violations of international law.

Neller: They're at total disregard of Security Madison for international law, just like the event of them deliberately colliding with a Ukrainian ship and then taking the three ships. Holding the three ships, and then taking the crew off. Just like they've done in South Ossetia and Abkhazia and Georgia. Where they take advantage of where there's a Russian ethnic minority, and they use that as a basis for them being aggrieved, and they're going to protect their interest. And they go in and they use that as a pretext.

Neller: Then they're very adept and very capable in social medial, where they then blame the other person and the cyber domain is social media. The network allows you to be much faster with this; your ability to deny or obfuscate, or write your own truth, is something that's part of this. But I think they see more, probably on the news with their involvement in Syria, and we recognize the Syrian regime is an evil regime. So I'm not surprised by the results, but I think we need to pay attention to all these things.

Barnes: Nadia, have we been aggressive enough in confronting Russia in Ukraine or other places that it has sought to extend its influence where it's annexed? Are we too afraid of escalating the situation in confronting Russia? What is your thought?

Schadlow: I think not just in terms of confronting Russia, but I think in general in terms of the subject of this panel; hybrid competition. Concerns about escalation have been prevalent, I would say, over the past 10 years. And that's really hampered us from responding with the full range of instruments. I think that's changing now. I think a lot of things over the past year and half of this administration has explicitly changed in terms

of being more forceful about pressing back. Even calling out, for instance, the WannaCry and other cyber attacks that have taken place. That's been different.

Schadlow: I think our declaratory policy in those areas is also stronger. So I think that that's a good thing, because that flexibility on escalation, actually has implications for deterrence, right? If your adversary or competitors knows that you're wary of escalation, that's going to have negative effects on our ability to deter future activities down the line. So it goes full circle. So I think that is starting to change, and I think will continue. Especially in the cyber domain as well, which I think the Congressman has also has been a key part of in terms of understanding the importance of this domain. And in terms of what the Cyber Commission and Congresses Commission and thinking more flexibly about it.

Barnes: Congressman, will you weigh in on that, whether we are responding aggressively enough to the gray zone, whether it's a cyber attack or a hybrid attack?

Langevin: I think we need to respond more, and I think that we put ourselves in jeopardy or make it more likely that Russia will be more aggressive the more we look the other way or we don't confront. Doesn't necessarily mean confront overtly, again, this is where the gray zone comes in. By the way, it's a whole-of-government approach, and working with international partners and allies. When the Russians invaded Crimea, there was a international response with sanctions. I think it could, it should be stronger.

Langevin: Again, as Russian aggression continues, again, a whole-of-government, not just military, but whether it's through sanctions and calling them out, I think that's essential. I spend a lot of time on, of course on, the cyber security field, and that has a direct implications there. We can't let the Russians aggression of Vladimir Putin's aggression go unchecked, answered, because he's just going to be in bold to go further.

Barnes: Congressman, at the beginning you mentioned the importance of whole-of-government approaches. That's a term that's thrown around a lot. Journalist tend roll their eyes when we hear it. The reality is, the authoritarian regimes in Russian and China, very much have a whole-of-government approach. Where they can utilize their diplomats, their military, their industry, together for a concrete goal. How good of job has the United States done in responding to these hybrid, cyber information attacks with a coordinated response between military, diplomats, and industry?

Langevin: Well, it's a mixed bag, but if you look at just the examples of our Russian election interference, and also Chinese espionage. In both of those cases, we didn't let those situations go unanswered. Now, we were slow to act in the election interference. There was probably a failure of imagination to recognize the degree to which the Russians were going to use a number of different tools to try to interfere with our elections. We eventually, obviously, did respond with expelling diplomats and posing sanctions. I think we can, and we should, continue to do more. We called them out.

Langevin: Same thing goes with China's espionage activities, and finally President Obama confronted China. And again, whole-of-government approach, sanctioned but also in particular, inditing the Chinese individuals that we named as being key players in stealing our intellectual property. It resulted, of course, in an agreement between the United States and China to curtail that activity. Now I'm not naïve to say that it stopped it, but it did put the pause button on China's activity. So, those are two examples where by confronting, by outing, by imposing sanctions and with the Justice Department

indictments. That's what I'm talking about in terms of this whole-of-government approach to confronting in the gray space, the gray zone. So, it's a mixed bag. We've got to get better at it, and don't let things go unanswered.

Barnes: Dr. Schadlow, I want to take my question and make it blunter. Is the state department doing enough? Are American Diplomats doing enough in this kind of conflict to confront disinformation, deter hybrid war?

Schadlow: I don't want to be critical of my colleagues at the State Department. I think that the problem is a little bit broader. The whole-of-government hasn't effectively helped us as an operational concept. It's not an operational concept. We need to think in a completely different way. We need to think in terms of a campaign plan. How do we solve a particular problem set, and what capabilities do we need to bring to bear to solve that?

Schadlow: The whole-of-government approach has ended up just putting all the stove pipe in front of us in one room. It hasn't helped us, to use General Neller's analogy, and my friends in the audience will know I'm not a sports analogy person. But we're not working as a team in the same way as a soccer team or a football team are working with whole-of-government. So I think we need to shift our approach overall. I think the State Department, like other civilian agencies, they do not tend to think competitively, right? The agencies that think competitively in our government are the military-

PART 1 OF 3 ENDS [00:17:04]

Schadlow: The agencies that think competitively in our government are the military and IC community for the most part, so overall we do need a shift in those agencies, not just state but across the board, USAID as well, to think more competitively because they have pieces in this competition. We need to think about, ask ourselves, "Where is our Internet Research Agency? Where is Quds Force?" Obviously, we don't mirror those organizations. We're a democracy, but those types of capabilities working with new modalities. So, I think we need to spend the next year building on the National Defense Commission report that was just out that identified the need to improve in operational concepts, to come up with some new modalities and test them out.

Neller: There's a lot of stuff going on and it's very easy to get focused on what we would call the 'near fight': deploying people, bringing them back, doing what we need to do. This is a long fight. The Chinese wrote their plan in 1949. It was a 100-year plan. "In 100 years, we're gonna dominate the world." They've told us everything they're gonna do and they're doing it and we're sitting here and we're watching it. Now, I will speak to the military dimension. It's much easier, and I think we've been effective in blunting some Russian actions militarily in Europe because NATO's become more energized, they're spending more money. We've deployed three multinational task forces to the Baltic states. We provide foreign military sales to Ukraine and Georgia or other countries. We've increased the deployment of US forces back to the EUCOM AOR. So, I think there's a visible, tangible commitment, and in Syria we've had our bumps in the night with the Russians, but we have a de-confliction process where the chairman and other commanders work through that.

Neller: It's not unsophisticated, but there's really not an economic piece to this, kinda like the Cold War. There wasn't an economic piece. They're not economically a competitor with

us. China is much more subtle about this, but militarily, I mean it was a couple months ago they said they were gonna provide defense attaches to Papua New Guinea, Vanuatu, Fiji, Tonga, and some other islands out in the South Pacific, and that should concern us because our coverage is low, and so they'll come in there and they'll try to get those countries to gain port or airfield concessions, to try to sell them military equipment, to try to take their military and send them to school in their country and the Chinese will pay for the military officer, their family, and all their children [inaudible 00:19:51] to China.

Neller: I'll just end with this story: so, I went to Thailand, and Thailand has a military government. They had a coup d'etat. They overthrew a duly elected government, and because of that none of their officers can come to school here anymore because of our laws and we should hold them to account for that and we should make them hold an election, but I went there. I was the first [inaudible 00:20:12] to go there in 25 years, and now all these Thai generals remember Captain Neller. The Thai Marine generals, remember Captain Neller when I taught them at the basic school. So, they were all proud that I was their captain and they're now generals, but for the last five years there have been no Thai Marine officers come into the Marine Corps school, and if that goes another five years and instead they go to China, what does that gain to us? Granted, we need to hold their government to account.

Neller: So as an observer, I would say sometimes ... You know, remember the second line of effort in the National Defense Strategy is 'maintain and build alliances and partnerships'. We can't make it too hard to be our friend. We should hold people accountable for human rights and illegalities and trade, I got that, but we can't make it too hard to be our friend because otherwise there will be others that will step into that void and then we'll wake up one day and we'll be where we are.

Barnes: Congressman, what do you think to that very specific example? Should we find a different way to hold the Thai government to account and continue the military-to-military ties in the name of a strategic competition with China and not letting them drive a wedge between our friends? What's your view of that?

Langevin: I agree that engagement is the best defense. We can't be the isolationists and we have to figure out a way to deal with the Thai situation, and I think the general is right, the engagement and having people come here to study here. I think, by the way, our best way of staying relevant in the world and also having our best defense, having people around the world understand our principles, our values, what we stand for, is by coming here, studying here, and whether it's the people in the military or the student population, because then they'd come back, and even even countries in the Middle East, they can't just get their news, if you will, just from Al Jazeera or we've already lost the ideological war. We need to have people come here. Engagement is, I believe, the best policy. So the tight situation, I agree with the general. We've gotta find a way to engage with them, allow people to come here, but at the same time not compromise our principles and values. So, we've gotta continue to re-look at how we're engaging

Barnes: General, you have some Marines in Norway right now, and there are those who say ... It's not a large number, but it provides a complicating factor for Russia. There is a deterrence. It's not just training for those Marines up there, but it's also a measure of deterrence against Russia. How has that worked out? Do you feel like that has increased

American security? Would you grow that force? How do you think it has been employed so far?

Neller: The United States Marine Corps as a long standing relationship with Norway from the Cold War, where we established a pre-position equipment set in some caves over there, which was part of the NATO US response to potential Soviet aggression. So, through a number of evolutions since the Benghazi consulate attacks, we've ended up deploying a small number of Marines up there, and this year we increased it. It's rotational presence. There's no base. The Norwegians politically have agreed to this and if they ever told us that it was not acceptable to them then we would leave, but it gives us great opportunity to operate there in that environment, particularly in the cold weather, which is something we haven't done for a while, and the Norwegians, their military is very effective and they're great partners and financially they take care of us really well.

Neller: So, if the Russians are afraid of 700 Marines in Norway, I'm a really happy guy. We just did a large exercise there, NATO did, tried in juncture. We had about 8,000 Marines go there and there was a reaction by the Russians, both informationally and militarily, and it was good. It was good. It was good they were paying attention. I'm glad they were paying attention. I'm happy they were paying attention, but that's not why we're there. We're there to train and those Marines that are there, they're gonna operate throughout ... Some of those Marines that are there previously had been in Romania, so we'll go back to Romania to train. Those Marines are go to every NATO country. They'll train with Sweden. They'll train with Finland. So, it's part of the second line of effort to maintain and build alliances and partnerships, and our friends and NATO allies are glad that we're there and it's a great opportunity for us to get experience and expose these Marines to the different parts of the world.

Barnes: Dr. Schadlow, have we done enough in Europe to deter Russia? 700 Marines and US forces in Poland, NATO forces in the Baltics. Is it enough? Should we have more? The Pols would like a permanent base with another armored brigade from the United States. What do you think?

Schadlow: Our spending in Europe has been maintained and it's even at higher levels. I don't know the exact number. I don't know, General Neller or Congressman, if you know, but the European Reassurance Initiative is at higher levels than it was in the previous administration. You know, I personally, not part of the administration anymore, think I understand the Pols' argument. I think that could be very powerful in terms of deterrence. I think it's something we should consider. I know my colleagues in the audience from AI and other think tanks have thought hard about different kinds of deployments in Europe, so I think we're doing a lot. I think the president's successful efforts to get NATO allies to spend more has been a big factor also in improving our deterrent posture there. So, I think we're doing pretty well on that area.

Schadlow: Where we're not doing so well, again, is in the subject of this panel, the sort of hybrid competition, which one point I would like to make just because I think it's relevant almost to the whole day of discussions across the panels at the Reagan Defense Forum. is the degree to which the private sector is a part of that competition, the degree to which the private sector is an asset or an ally to the US government to proceed in that competition, and I think that this is a big area and it's been a subtext of many of the panels today and it's one that we haven't quite answered, although you and the audience from different parts of the private sector will have different views, obviously.

Barnes: Congressman, how do we get the private sector to be more active in this, whether it is improving their own cyber defenses, cooperating more with the Defense Department in developing new technologies, or other endeavors?

Langevin: Well, certainly we've tried to incentivize closer work with Silicon Valley and take advantage of the unique and innovative 'off the shelf' technologies that they have developed. The DIUX is one example of how we're trying to engage more with the private sector. On the security standpoint, on cyber, is there's a number of things that the private sector needs to do to kind of [inaudible 00:28:25] the low hanging fruit of cyber threats and challenges, so protect their own intellectual property, and then as things escalate, as things get more serious, that's where you engage more with the Department of Homeland Security or ultimately the Pentagon, which they're now changing strategy and leading forward more. I applaud that.

Langevin: The private sector can be a part of the effort to secure our networks, if that's where you're going with that and I'm interpreting your question right, that ... Take care of the low hanging fruit. They're not gonna be able to defend against those exquisite nation state attacks or intrusions or capabilities that nation states bring to the table, but with there's low hanging fruit where we can protect and secure the supply chain, protect their own networks with robust security, and by the way that goes especially for protecting critical infrastructure. It's gonna make us all more secure and limit our adversaries' ability to cause us harm. I know it's a high bar, but again, not only the whole of government, but [inaudible 00:29:38] industry has to be a partner in this security effort as well.

Barnes: Dr. Schadlow, why is Russia better than the United States in competing in this gray zone? General Neller began with a metaphor of Neymar or Ronaldo on the field sort of faking an injury. That's part of it, but why else can Vladimir Putin, who does not have the economy of China, does not have the economy of the United States, has a lot of things going against him, is still able to set the agenda in some places to drive some change in the gray zone?

Schadlow: Yeah. I mean, he doesn't have to coordinate in an inter-agency process, right? Being not a democracy, not bound by rule of law or by, certainly, democratic rules, he has the flexibility to create agencies. You know, the Internet Research Agency to order Russian hackers, to pull them together, to order them to do certain things. So, he has the flexibility that comes with an authoritarian leader. We live in a democracy. Obviously, there are great strength to that democracy and I think that if we think more creatively and look hard at what we can do better, and I think we can do a lot better, we'll use our democratic advantages and openness to compete more effectively, but he's just not bound by the same rules we are.

Barnes: I'm gonna go to the other slide here, if I can. All right, and this slide talks about Americans' concern about cyber attacks, and we've got a 92% here, far more than a conventional military attack or attack on satellites or nuclear war. Congressman, I want you to react a little bit to this. Does this feel right to you? Why do you think Americans are so concerned about this? What do we need to do to deter cyber attacks more effective;y?

Langevin: It doesn't surprise me, in the sense that probably almost everyone has been impacted by some type of a personal data theft or their identity is stolen, getting caught up in the

Equifax breach. My Chief of Staff in Rhode Island just had his bank account hacked and thousands of dollars were taken out of his account. So, I think at this point ... You know, when I started ten years ago talking about cyber security being a significant national security threat and challenge, there were very few who felt the same way, or not many people were paying attention. I kind of felt like one of the guys running around with the tin hats and wondering if this was ever gonna get the attention that it needed or deserved.

Langevin: Mike McCaul and I started the Cybersecurity Caucus ten years ago. I served on the CSIS commission for cybersecurity for the 44th presidency, and in all that time both then and since, I recognize [inaudible 00:33:16] modern warfare has forever changed. We're never gonna see any kind of conflict again without some type of a cyber component to it. The American people, they've been sensitized to the issue of cyber, I think because of this personal connection because of data theft and compromise. So, cybersecurity and the challenges [inaudible 00:33:39] here to stay. The American people, I think, obviously are sensitized to it now. We [inaudible 00:33:45] need to continue to double down and do more to secure our own networks.

Barnes: General, a question to you in your role on the Joint Chiefs. The Trump administration loosened the rules around a offensive cyber operations earlier.

PART 2 OF 3 ENDS [00:34:04]

Barnes: ... around, offensive cyber operations earlier, cut away some of the bureaucracy around that in order to make the ability for cyber command, the United States military, other aspects of the government react more nimbly to cyberattacks on the United States, threats to elections.

Barnes: There have been reports that Cyber Command has done some operations in Russia. What is your view of the balance? Are we doing enough to counter overseas cyberattacks on democratic institutions, should we do more?

Neller: Well, if General Paul Nakasone, head of NSA and Cyber Comm were here, he'd be the one, if he could say anything, he would answer it. But, I think ... everybody's concerned about this. And you've talked to people, the private citizens are concerned, I ... in the LPM hack, I lost all my stuff. And then if you saw, yesterday was a large hotel chain, of which I happen to be a member, I'm sure I lost all my stuff in there, too.

Neller: So, I don't know what the ramification is, and like you, I mean, the network is very seductive, because we expect it to work all the time, and when your phone doesn't work, you know, you get all upset, and angry. And when the insurance company makes you take the text and type in the thing, and you're like, "Why are you doing this to me, I used to be able to do this work in five minutes." But they're doing that to protect your data. So we're in a different place.

Neller: I mean, the people I talk to that are in this business, they say we're in phase two of combat every day. They're fighting, they're pouring boiling oil over the wall of the castle every day, because somebody's trying to put a ladder up there and climb in. Even though they may be able to see them forming in the woods across the stream, a couple miles away, their ability necessarily to keep them from running up to the wall of the castle is limited, dependent upon certain authorities, and policies.

Neller: And that's probably right, in a democracy, but it's a complicated issue. I only speak from it militarily, because my concern is, we have developed a way of fighting that is very net-centric. I mean, if I were going to fight the United States, the first thing I would do, is I'd go up to space, I'd kill all the satellites, and then I'd shut down the grid. And then I would ... the military, we'd lose satellite communication, I'd lose all my data, I'd lose all my unmanned aircraft, I'd lose all my globally positioned system air weapons, and I'd lose all my position, location, and navigation, timing for all my radios.

Neller: So in the next fight, whoever can protect that, or bring it back up faster, and take it away from the other person, is going to win. Without a shot being fired. Without a shot being fired. And so, you'll see all the military forces developing these capabilities to not just defend themselves, which is much easier legally, and policy-wise, than it is to do offensive stuff. Dependent upon where we are. If we're in a designated area of hostilities, we have much more latitude with what we can do, but there still has to be rules and legalities and things like that, and coordination with other agencies because you don't want to screw up with what somebody else is doing.

Neller: And but as the congressman said, as the Doctor Schadlow said, the Russians, the Chinese, they're already in a campaign, they've already got a team put together, they've already set the rule set, and they're ... they have the ability to go faster than us. And that's really ... I think we've got the capabilities, but we've got to be able to go faster. I mean, it's a battle, but just with different capabilities.

Barnes: Congressman, what do you think about whether we are doing enough, in cyber, offensively, or in a sort of ... at least in terms of overseas operations, is there enough oversight on this? And also, do we talk enough about it in so that we can have a cyber deterrent? Should we talk more about the, as Senator King mentioned, this morning, about the sort of kinds of weapons we might have in our arsenal in order to deter Russian or Chinese interference?

Langevin: Sure. So, because I think it's the right thing to do, to lean forward more than we have, and I think that the new National Defense Strategy and National Security Strategy that was outlined, is a good place to start, but I would say this is where congressional oversight, of course, comes in. We don't ... it's already kind of done. Too much of the Wild West out there right now, we don't want to make it, we don't want to make it worse. We want to make sure that we are, again, taking a Whole-of-Government approach. We can't look at this as a silo thing. Now, we're getting better at securing our networks, we're not where I'd like us to be yet, whether it's an US government in a military perspective, or what we're doing with the Department of Homeland Security.

Langevin: Obviously the private sector, where most of the damage could be done, is a critical infrastructure. I'd like to see more robust cyber defenses there, but we're getting better, the US Cyber Command just has now 133 cyber teams that are trained, and reached FOC, as of May of this year. So we are getting better at both defending our networks, and then leaning forward, and being able to better confront our adversaries.

Langevin: But again, this isn't just a siloed ... you can't just do this in a silo. It's going to be the Whole-of-Government. Whether it's through treasury and sanctions, so the Justice Department, in indictments, by the way, intelligence community is incredibly important, because cyber forensics are essential. Being able to know who the bad actors are, how and where to confront them, you wouldn't just do cyber forensics on its own, and saying

you could be able to understand who did what, it's going to take good intelligence and a number of other things come to being brought to bear. So that we can hold the bad guys accountable, and confront them where we need to.

Barnes: Doctor Schadlow, I don't ... while I'm waiting for the audience questions, do you want to weigh in on that at all, on this issue of Cyber Deterrence or where we are good enough at attribution and how ready we should be to attribute to a cyberattack?

Schadlow: Well, I think a useful concept, so I would be probably more assertive in the offensive realm, and think about defending forward. What is offense, what is defense in the cyber realm? So essentially by not defending forward, you know, is it offense to go, to move ahead, and use that as a deterrent posture, which is to defend ourselves, so what is that relationship? And there are experts in this audience who are, you know, know way more. But I think the government in some ways is still thinking in terms of offense, defense, and that space has changed. It's a continuum of conflict ... a continuum of competition within that domain.

Schadlow: And to go to General Neller's point, you know, sort of, it's not just the episodic moments, right, that we're thinking about, it's this continuum, that we need to be continually in there, competing across that domain. I think we also, need to, as the National Security Strategy pointed out, think about deterring through other means. You know, sanctioning actors, creating uncertainty, and thinking about cyber-enabled economic warfare as an act of war, or certainly an act of conflict, or certainly is a serious challenge. So going after our banks and our economic system, matters.

Barnes: The first of the audience questions is a follow-up to this. Do the difficulties associated with identifying the origins of cyberattack make deterrents futile? Who wants to weigh in?

Langevin: No, I don't think so. So, cyber forensics and understanding actually who did what, is hard, and you may never be able to do it just by cyber means alone, knowing where the attack came from. Especially if you talk about use of proxies, which is something that surely worries me. However, you wouldn't, if ... if it was a crime scene, and the murder, say, that took place, you wouldn't expect the FBI or law enforcement to just understand who was responsible in bringing that person justice, just on the evidence out there at the scene itself. You know, you'd use all-source intelligence, right? You'd use video surveillance, you'd do witness interviews. And that's what I'm talking about, in terms of identifying perpetrators, in the realm of cyber, it's all assets of state power that you bring together to hold those individuals accountable.

Langevin: You'd have high enough confidence that you can take action from there. I mean, the ... Chinese espionage issue was an example, and ... you know, WannaCry is another one. We had high enough confidence that we called them out, and responded. But this, by the way, it goes to the heart of, response, also not just a US issue, but it needs to have engaged the international community as well, so that we confront our adversaries that use cyber as a weapon against us. That there's an international component in response and we work closely with our allies to deter.

Barnes: We ... our time is growing short, we have one last audience question, and I'm going to throw it over to you guys, and then you can also append any final thoughts you have. The question is: did we see substantial Russian or other foreign nations say interference

in our mid-term elections, if the interference was limited, was that the result of any US actions? Doctor Schadlow, do you have a theory of the case, even though you're out of government?

Schadlow: I think it's clear that there was Russian use of social media and the internet to pursue a form of political warfare, which the Russians have honed over ten years now, at least, right? I mean, even earlier, the Cold War period as well. But in terms of the context, overall, the Russians in Europe, in the Baltics, have been honing the use of the internet for information operations, which again, the antecedents are political warfare. So, I think it's clear that the Russians were using their trolls and their bots to place ads on Facebook, and we saw all that.

Schadlow: You know, the US government is having trouble thinking about what is its role in protecting those platforms, right? We're seeing Facebook sort of fall apart over this issue about how do you ... what's the role of platforms such as Twitter, such as Facebook, in letting all of that unfold. The US government doesn't own those platforms, so that's to go back just to ... and to the original point, what's our operational concept in the information operations domain, it's not just a military problem, it's part of putting those pieces together.

Barnes: General Neller, 15 seconds for your final thought.

Neller: In my last comment, I want to leave anybody with the impression that we're not able to execute our mission. You know, the first thing in solving a problem is recognizing that you have one. And so I think the adversary has the same issue we do. They're dependent upon the same things we are. And so, as we go through and change the way we train, and create capabilities to defend our network, and then potentially offensively address theirs, we're doing that now. At the same time, we're training to be prepared to operate without a network. Yesterday, I was at 29 Palms at our combat center, a lot of paper maps out there. Lot of paper ... you can't hack a paper map.

Schadlow: Good.

Neller: You can't hack a paper map. Works every time. Even in the rain, never runs out of batteries, it's a good thing. So, it creates extra work, because you've got the digital picture, and you've got the analog picture. So, we're kind of back to the future on this. And so, I think we recognize what we have to do, we're developing capabilities to do that, I think the Department of Defense ... I saw Mr. [Desi 00:47:16] here, you know, we're trying to improve our own security and our own offensive capability.

Neller: Everybody's investing in the cyber protection teams that the Congressman was talking about, and cyber teams that do other things. And so, everybody's growing that capability. And because that's where the fight goes every day, and that's where the fight's going to start, it's going to continue below the level of combat, but if there is a kinetic fight, it'll start in a non-kinetic way in that venue.

Barnes: Congressman, you get 10 seconds, a real 10 seconds, because that wasn't a real 15 seconds, to finish us off today.

Langevin: So, I would say this. Surely cyber-resiliency has to be ... a forethought, not an afterthought. Engagement with the public is important. Everybody's going to do their

part, do your basics, apply your patches, have robust passwords, those are the basics you can do a lot. Just by doing the basics, you're not going to be able to defend against the exquisite, high-end things, but then the United States needs to be, again, continue to be better organized, we're investing in the right resources, for example US Cyber Command, and what the DHS is doing. But then working closely in an international partners to make sure that this is a unified effort if you will.

Langevin: We will be able to defend against the challenges that we face. But, you know, I liked what the General was talking about, cyber-resilience, and we have the nation's most dependent on the internet. We created it, we make use of it, but we're also most vulnerable to those who find ways to exploit it. And we've got to get better at closing those avenues of opportunity before, or I'm sorry, so confronting, being aware, and not letting go when things go unanswered. That's where I believe that we will continue to stay strong in this area and protect the country.

Barnes: Please join me in thanking our panel.

PART 3 OF 3 ENDS [00:49:29]