Center for Strategic and International Studies

TRANSCRIPT

Online Event

"Cyber in the Ukraine Invasion"

DATE

Monday, March 14, 2022 at 11:00 a.m. ET

FEATURING

Mark Warner

U.S. Senator (D-VA); Chairman, Senate Select Committee on Intelligence

Chris Painter

Former Coordinator for Cyber Issues, U.S. Department of State

Greg Rattray

Partner and Co-Founder, Next Peak LLC

CSIS EXPERTS

James Andrew Lewis

Senior Vice President and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James Andrew Lewis: Thank you and good morning to everyone. We are going to be talking about events in the Ukraine. Our speaker will be Senator Mark Warner, followed by a brief discussion between he and I where we'll take a few questions, and then a panel with Chris Painter and Greg Rattray, whom I'll introduce at the time.

I'm not sure Mark Warner needs an introduction because for a long time now people have thought he is the most tech-savvy senator in Washington. And you could say that perhaps senator is a low bar, but in his case that's not true. He's been a leader in the cybersecurity efforts. And so we're very pleased and fortunate to get his take on the events in the Ukraine, the implications for cybersecurity in the U.S. Senator, the floor is yours.

Senator Mark Warner (D-VA): Well, Jim, thank you. And thank all my friends at CSIS for having this forum. I think we all have been mesmerized, not only as Americans but as, you know, frankly, just citizens of the world, to see the conflict as it rolls out daily on our screens and in Ukraine. I remember – I think it was three weeks ago I was in Munich, meeting with Ukrainians, foreign ministers, intel service leaders. This was a few days before Putin launched his unprovoked aggression against Ukraine. And even at that moment in time, while our colleagues saw the intelligence, knew we were on the precipice, I think the vast majority of them still didn't believe that Putin would literally pull the trigger.

He did, obviously. And again, I think the world has been really taken by the courage of the Ukrainian people, taken by the courage and resoluteness of President Zelenskyy. I remember prior to the – prior to the invasion a number of us were talking on the Senate Intelligence Committee, you know, was Zelensky going to be a Ghani, the way the Afghan leader who cut and run once the Taliban got close, or was he going to be a Churchill? And, boy oh boy, at least in my mind, he is kind of a Churchill on steroids. Not only in terms of the incredible use of social media showing him in Kyiv and in his presidential palace visiting, I saw this morning, his wounded soldiers. But also even using Churchillian language when he spoke to the English Parliament. I'm glad that the U.S. Congress has formally invited him as well, and I think he will make an enormously important presentation on Wednesday to the U.S. Congress.

A couple quick points I want to make before we get to the conversation. First, the American intelligence community. I know over the years they've not always been right. We can all point to critiques. But on this one, boy oh boy, did they never just nail it. Starting last fall, as Putin started to bring up his forces, they have been able to monitor and relay to us policymakers in America, but also to our NATO allies what Putin was going to do, how he was going to do it. And candidly, I think, by being willing to lean in – I mean, this

got them way beyond their traditional comfort zone of relaying intel almost real time both to allies and to the public – I think they've done – they've been very effective in two ways.

One, I remember back about a month ago when there was some evidence that Russia would stage – have a coup staged, put in a new leader. American intelligence said, hey, watch this coup coming; if it comes, it'll be the Russians. Then the British intelligence, who we work hand in glove with, said here's the guy that the Russians are going to put in. I think it was a brilliant use of forward-leaning intelligence. There was efforts of trying to – the Russians were going to put out a series of videos. Again, the American intelligence laid out what those videos would look like, even pointing out where the Russian cadavers would be that would be used as the bodies, again throwing Putin off-guard. And then, by relaying this information – again, almost in real time – to our allies, it built the case so that when Putin then did attack almost to the day that intelligence predicted, we've seen, again, an unprecedented unity.

I mean, if you'd asked me a few weeks back, Jim – and I know you and I have talked about this in the past – that we'd see the Germans take the lead on Nord Stream 2; the Germans would change their whole approach in terms of defense spending, unity with NATO; Sweden and Finland agreeing to send arms; sanctioning Putin individually, the central bank; the Europeans taking the lead on kicking Russia out of SWIFT; and then even the Swiss – I mean, it's almost become a bit of a – of a, you know, a pause line – but you know when the Swiss get off – get off the fence and side with the – side with the alliance that we have – we have done a good job. And again, kudos to the intelligence community.

In terms of the conflict – and then we'll touch on cyber and then go to the conversation – while clearly the Russian military traditional forces I think we're all scratching our head at their disarray, their ineptness, the fact that about half of the Ukrainian air defense systems are still – are still operational – I think I saw in public reporting today that the Ukrainian air force has got about 54 airplanes left – really remarkable, and also again showing that the Russians – there was not much shock and awe in their shock-and-awe area.

The area that has – that has surprised me, though – and I don't think we should take – believe that it's lack of capability – while there may be lack of capability in terms of traditional military efforts, in the cyber domain we know the Russians are first rate. The cyberattacks so far that have taken place, the so-called wiperware that has been malware that literally has stayed within individual networks, has been relatively mild.

I know I've had both – in the worldwide threat hearing we had last week with the American intelligence community in a public setting and then even

in private settings, I've, you know, questioned our leaders: Why haven't we seen the real A-team? Why haven't we seen out of the GRU some of the – some of the entities that we know have the capacity to, frankly, shut down entire systems, shut down the internet? The fact that we're still seeing these videos coming out of Ukraine surprises the heck out of me. You know, the fact that they have not launched a NotPetya-type attack where – with a software that includes worms that go from one network to another, we don't have an answer.

I mean, the conventional wisdom is maybe at first we thought that – you know, that the Russians assumed they would win so quickly; or, second, they didn't want to use the really malicious malware because if it really destroyed some of the Ukrainian infrastructure it would take much longer and be much more costly to re-standup. But now that we're seeing, you know, whatever has happened – day 17, 16 on the war, and Russia potentially even talking about chemical weapons or other more egregious forms of conflict, I still am relatively amazed that they have not really launched the level of maliciousness that their cyber arsenal includes.

Now, will we see that in the coming days? I think that remains a possibility. Are they holding that for potential use against them the West and/or America? Again, we'll see.

The two comments that I, finally, at the end want to make is I was very concerned in the early days that Russia might launch such expansive cyberware attack or cyberattack that it might bleed beyond the geographic borders of the Ukraine and bleed into eastern Poland where, you know, if you shut down Polish hospitals and Poles die, is that an Article 5? Or if you had American troops, you know, getting in a traffic accident because the lights have gone off could that be an Article 5?

So far, we've not seen that effort of bleeding into other geographic areas. I hope that will remain the same. And at the same time, I think we, in the United States, need to keep, as CISA has said, our shields up and we all know, again, with the cyber experts we have on your panel, you know, we know we can't be a hundred percent effective in our defense so we have to have resilience.

And I will make one comment. As Chris mentioned before we went online, one of the pieces of legislation that was included in the major budget bill that was passed last week was finally, finally, finally, we have mandatory cyber reporting that will become – I believe, has become law now. I think the president has signed the bill. And, again, that will require mandatory reporting to CISA if you are the victim of a cyberattack, we'll give that company immunity. We don't want to go – you know, we don't want to hold the company accountable. We do want to be able to go after malware actors.

I think this is a giant, giant step forward both in terms of the challenges vis-à-vis Ukraine but on a broader basis to make sure that, you know, the current level where we only have about 30 percent of cyberattacks actually being reported to the government, this, over the long haul, will give us a much greater tool to have that reporting at CISA and, again, and mostly so that we can then share it with our other private sector partners. So a big win in the budget bill for those of us who are concerned about the cyber domain.

So with that, Jim, I'll turn it back over to you. I know I hit a lot of topics very quickly but I do want to make sure we get time for plenty of questions.

Jim, I think you are on mute.

Dr. Lewis: It wouldn't be a Zoom conference if somebody didn't make that mistake. So I apologize. But demonstrating, once again, why you're such a leader in this field.

Let me – let me start with a couple questions. You mentioned something called forward-leaning intelligence, and I thought that was really interesting. We're watching a shift from the CT focus of the last couple decades to great power conflict. What are the lessons from what you saw in the lead up and during the Ukraine crisis for budget, for intel strategy, for the organization? So what are the broader implications for intelligence?

Sen. Warner: Well, I think, and one of the things I would also add, and I think this is a little bit on purpose, but one of the things that we attached to the so-called omnibus bill – the big piece of budgetary legislation – was we included our intel authorization bill, which, because of the craziness of the sausage making, was not able to be attached to our defense bill, but it is also becoming law.

In that bill there is, again, added resources and increased shift to both beefing up NSA and Cyber Command. There were efforts in trying to up our cyber capabilities across the whole intelligence community, and for so long, understandably, you know, the intel community, because they're crown jewels, guard sources and methods, and under the guise of guarding sources and methods they have been, you know, traditionally very unwilling to share intelligence outside a very small group of policymakers.

I've got my theories. I don't have the answer of who was the impetus of actually having this information shared in such a different matter vis-à-vis Ukraine and – although I do want to give a great shout out to General Nakasone at NSA, because a lot of this did come from signals intelligence and he actually owned that intelligence, so his willingness to have that shared.

I think it has really shown in an information-driven world if we can share intelligence with the public and with our allies in a more real-time basis, it puts us back in the game in terms of information warfare. I think over the last number of years, frankly, Russia has been a much better – has been much better at using information warfare or, particularly, disinformation. We all saw the Russian involvement in 2016 in our elections. We've continued to see Russia use social media in a much, much more aggressive way. The fact that we were able to get this information out into the bloodstream, you know demonstrating and taking away any ability for Putin to claim that there was any Ukrainian provocation that started this war, it really has left Putin exposed as being the absolute culprit in starting this war. There's no credible claim otherwise. So that, I think, is important.

And also, the willingness to share with our allies. Obviously, we share a lot of times with our Five Eye allies. But this one, the information sharing with the balance of NATO and in some cases even beyond NATO, it's not by chance that we ended up, I believe, with 142 votes in the U.N. General Assembly a week ago. A lot of that was because the American intelligence we were sharing with a lot of folks. I hope this will be a precursor to a much more ongoing, active intelligence network. And, candidly, again, the power of information sharing ought to be a stronger part of our, you know, military, diplomatic, and overall statecraft.

Dr. Lewis: Thank you. I think that's really a neat point that intel sharing is something that lets us get an advantage in the intel – in the information conflict. So useful. I'm going to ask for a crystal ball moment. I almost saved this for last. You can dodge it if you want. But some of us have been following the CHIPS Act for however long it's been in play – is it a decade now? I don't know. But – (laughs) – that's not fair. But has this changed the dynamics on the Hill vis-à-vis the sense that we are now in a much more immediate conflict with Russia, and I would say with China? How has it changed the dynamic?

Sen. Warner: Well, Jim, again, a great question. And not to get too grandiose here but, you know, the last three or four years, you know, it's been tough in this country. It's been tough in the West. You know, we went through some of the challenges with the previous president. We went through January 6th. We've seen social media break us into tribal efforts. We've all had to live through COVID. And I think at moments, and we see this reflected in our press, right? And obviously where I work is sometimes dysfunctional.

There's been this real question, can liberal democracy literally succeed in the 21st century? Or are these authoritarian states – and I look at China as being, you know, the kind of – you know, an economic power beyond a military power. Russia is a military power but not much of an economic power. You know, the Chinese model's been very successful. What I think we're seeing

play out in Ukraine is the Ukrainian people are literally voting with their lives to try to obtain the kind of freedom, democracy, freedom of the press – things that we all take for granted. They are paying with their lives to try to have that system. So with all of our problems, I think we acknowledge we have the best system in the world. And we need to improve, but we ought to reflect a moment on that, and maybe a little less internecine political warfare inside our own system would be a good sign.

In terms of how we stand, though, on the competition standpoint – and you mentioned the CHIPS bill – this is so long overdue. I mean, I know in America we have been appropriately reluctant to do anything that appears to be industrial policy. But we are seeing the semiconductor shortage in this country right now play into inflationary tactics in terms of – inflation, in terms of automobiles. The fastest-growing component of inflation in our country. We've also seen, if we can shut off the flow of semiconductors to Russia, their ability to maintain their own military industrial base dramatically is undermined.

So this long overdue CHIPS legislation, which I was proud to be along with John Cornyn the original sponsor of, puts $52 billion – and, by the way, it's not just in the semiconductors. It's also into 5G and ORAN, Open Radio Access Network. We may all recall we were focused a few years back on Huawei. This is kind of how we move beyond Huawei in the 5G area. Both the House and the Senate have passed it. We need to get our act together and get that bill to the president's desk, because that will also – that's national security, that's jobs, that's American innovation and leadership. All things that I think, frankly, the world is calling out for at this moment in time.

And if we can take the lead, for example, on this semiconductor space, I think we will need to make similar investments in artificial intelligence, quantum computing, and others. And I would argue from a macro point that what we may need – what we need to have happen now in the 2020s and beyond is start to build technology alliances. If we look back historically, post-World War II, it's military alliances; then we look at the common market in the '60s, economic alliances. I think in the 2020s and beyond, we need a coalition of the willing amongst democracies around technology alliances. Part of that manifestation is around investments like chips. Part of it would also be having America and the West writ large really engaged and involved in the standards and protocols, setting up all of these new technology developments. This is another area where I think, unfortunately, we had a massive lead for years and we've let that slip a little bit, so I hope CHIPS is a starting point for a level of innovation and technology alliances that will go way beyond just the semiconductor industry.

Dr. Lewis: Thank you. Yeah, it'd be nice to see the CHIPS Act actually land. So we had you here – I don't know if you remember – two years ago to talk about it and at that point I assumed it was within grasp. Everyone makes mistakes.

Let me ask a general question –

Sen. Warner: Just one thing. This is a case again where people, rightfully, who don't follow the sausage making of Washington all the time have got a right to, like, rightfully complain. You know, the bill passed the House, the bill passed the Senate, it's time for us to stop the squabbling, get it done, get it to the president and make those investments, because as you know, if we don't have this kind of tool, there will not be another semiconductor fabrication facility, manufacturing plant made in America. Even though we saw the Intel announcement, even though we've seen TSMC in Arizona or Samsung in Texas, a lot of those investments are, frankly – again, you read the fine print – are contingent on America making this investment that's coming from the CHIPS Act.

Dr. Lewis: Well, let me use that as a lead-in to the final question, then, which, again, a little outside but putting on your budget hat for a minute: Are we spending in the right places? Are we spending enough on cybersecurity and technology? Where would you want to see us move, say, over the next three years in terms of a budget for these activities?

Sen. Warner: Well, first of all, I think if you look at us on any kind of historic basis, our investment in basic R&D and innovation is dramatically smaller as a percentage of our GDP than it was, you know, 40, 50 years ago. I do think that whether we take Huawei in 5G or the shortage on chips, you know, it's kind of our generation's Sputnik moment. So I absolutely believe we need additional investment in basic R&D.

On the cyber domain, I think we are ramping up on the federal spend side; I do think there's lots more we can do, especially among smaller governmental entities. Some of this funding ought to be coming on the public side at the state and local government. The number of K-12 school divisions that have been cyber attacked – I think most people would flip out if they actually had that number. I think on cyber what we actually need to do is – it may not be just government spending; we, frankly, need the private sector to ramp up dramatically, and we need to acknowledge and be – you know, I need to be straight with the voters and business leaders need to be straight with their customers. We probably cannot be 100 percent effective on keeping the bad guys out but – so we shouldn't aim for 100 percent perfection on defense, but what we should aim for is this information sharing so that we can then share with private sector if we see a cyberattack so we can then warn others in the private sector. And where we really need

to invest, as well, is in resilience, how we bring our systems back up to speed as quickly as possible, and I do think we're making progress there.

Final comment on this, and I've made this comment before and it's a little bit, you know, uncomfortable in a state like mine, Virginia, where we have per capita military spending about as high as any state in the nation, I do worry at times that we are investing way too much in traditional legacy platforms when, you know, thank god, so far, we've not seen the more malicious cyber tools that Russia has brought to bear. You talk about things that can keep you up at night; if you look at – particularly vis-à-vis China, some of our overhead competition. You know, I think there are a host of areas – you look at hypersonics. There's a host of areas where traditional tanks, planes, and ships may not be as effective when we're thinking the real domains of the future may be cyber, overhead, and, frankly, other tools that we can't – we can't even get into in this kind of conversation today. So I would shift a lot of our defense spending much more into future domains rather than simply some of the traditional domains.

Dr. Lewis: Well, Senator, thank you. That covered so much ground – intel, defense spending, cybersecurity. Great points on all of them. We really appreciate your taking the time. And I don't know if we'll have any follow up, but thank you for what you're doing.

I liked the point about conventional spending. We're really good at building the weapons of the 20th century.

Sen. Warner: (Laughs.)

Dr. Lewis: Maybe that needs to change.

But again, thank you.

Sen. Warner: Thank you, Jim.

Dr. Lewis: OK. That was great. You never know what you're going to get because he's such a broad-ranging intellect, so we covered most of my questions.

But we're now going to go to a panel. Let me note that you can ask questions following this discussion. The panel is easy for me because it's two old friends, both of whom are true experts in the field.

Chris Painter. At this point, is there anyone left on Earth who doesn't know who Chris Painter is? Well, if you don't, he was, of course, the first cyber coordinator at State, before that at the NSC, and before that, of course, at the cybercrime units at DOJ, going back in law enforcement all the way to being a prosecutor in Los Angeles. So, extensive career.

Greg Rattray. We owe Greg a vote of thanks because he is the person that coined the term "APT" back when he started doing this in the Bush administration probably 20 years ago. Greg, of course, had been doing it well before then as an Air Force officer, but he is of course one of the leading strategists, along with Chris, for how we approach cyber activities.

I thought what we'd do is I'd have each of them make brief opening remarks on Ukraine, the implications for American cybersecurity, and then go to a little bit of back and forth. I invite people to send questions in if they wish to. But, with that, why don't we turn it over to Chris and Greg? Chris, do you want to go first?

Chris Painter: Sure. Well, thank you, Jim. It's great to be with you here today, and Greg, and Senator Warner as well, who as you said is a real leader. And I did congratulate him on getting the reporting bill through, which I remember working at when I was at DOJ literally 20 years ago. So it finally is there and I think that's a big improvement.

Look, you know, I think there are several things that the Ukraine crisis – the unlawful invasion – has illustrated.

One, you know, I think everyone's been somewhat surprised that we haven't seen a larger use of cyber in that conflict. Now, we did see it before it began. We saw attacks on Ukrainian government websites; some, as Senator Warner said, wiper software; other things that were launched. But I think many people predicted a massive sort of a cyberattack in Ukraine that would have gone after command and control and gone after communications, and that really hasn't happened.

We also haven't seen the blowback against Western democracies, including the U.S., so far. And I think the critical part of that is "so far." You know, it's not – we're still in the relatively early days, even though this has been several weeks now. It could well be that Russia is holding those in reserve – those capabilities in the reserve and haven't used them yet. They maybe thought and maybe one of the things this illustrates is actually physical invasion trumps cyber. You know, you don't need cyber as much when you have tanks and planes on the ground and men on the ground. So maybe cyber isn't as – you know, to paraphrase David Sanger – maybe it isn't the perfect weapon. Maybe it's not that. Maybe it's used only in certain circumstances, when you really have pre-planned and you've thought about it.

So there's a host of reasons. I'd say one reason that hasn't gotten a lot of play but I think actually has happened is, you know, Ukraine is in a different place than it was five, six years ago, when we had the attacks on the power

systems – the Ukrainian power systems and even other Russian attacks back then because they have spent some time trying to build their infrastructure, trying to build cybersecurity. Ukraine is one of the founding members of the – or one of the early members of the Global Forum on Cyber Expertise, the group – the capacity-building group that I help run. The State Department in the U.S. is dedicating more than $40 million to Ukrainian capacity-building in this area and, since the conflict has broken out, has worked with – across both the U.S. government and other governments to provide assistance, both more tactical assistance and also larger capacity-building assistance, and even worked with private-sector companies to get them involved.

The private sector has done quite a bit, even social media platforms in taking down content, Ghostwriter or other things that have – that have been – that deal with disinformation. So we've seen a lot of defense activity, but you and I and Greg all know that, you know, with a dedicated adversary like Russia you could be very good at defense they're still going to get in. And that's what's been odd that we haven't seen. And I do think that we will see that, that that's being held in reserve. So I – you know, I think shields up is really the right approach for the U.S.

The last thing I'll note right now, and we'll get into a discussion, is – another interesting thing is, you know, Jim and I have long said, well, we should be stronger in terms of Russian activity that we've seen. We should react stronger. We should do things like have meaningful sanctions not just, you know, willy-nilly sanctions, but meaningful sanctions. Things that would go after, say, Putin's money flow or his cronies. Up – the interesting thing about the Ukraine invasion is it shows that, you know, our toolkit's not that big. The kinds of sanctions we were arguing for are the exact kind that are now finally being used. However, you know, if you're going to use them for this big event, an actual invasion, are you really going to use them for a cyber event? So how do we deter, or at least affect, malicious cyberactivity in the future? And I think that's an open question.

So with that, I'll stop and turn it over to Greg.

Dr. Lewis: Those are great points. But, Greg, over to you. And we'll come back to them. Oh, you're muted.

Greg Rattray: (Laughs.) Second time. So yeah, again thanks, Jim, for the opportunity. And, you know, Chris, agree with your remarks, and Senator Warner's remarks. So, you know, maybe what I'll do is just try to amplify a bit on a couple points or mention a couple things I think are – have been less focused on.

One thing that my remarks is based on, I did, you know, have the opportunity over the last couple years to work with the Ukrainians, in part in implementation of the AID effort and, you know, help them with their cyber

strategy in the 2020-2021 timeframe, and then their national cyber response planning over the year – you know, the preceding year. So it's interesting, you know, for me now watching how well they've done reacting and, as everybody has said, how limited in cyber the Russian, you know, efforts have been so far, as well as, you know, the limited impacts.

One of the things that we haven't talked about yet that, you know, I heard a lot in the runup to the – during the crisis before the invasion, is: Would the Russians allow the ransomware groups to become more active again? That, we also have not seen in any sort of significant way. I mean, what I hear in terms of, you know, in the United States and across the globe, that the ransomware activities, you know, continues but at a normal level, maybe even a little bit less than normal. You know, and in terms of what's happening in the Ukraine, I think it's already – what we know has been reviewed.

One thing that I'm witting of, because my efforts to assist Ukraine continue to the day, including trying to help on the private sector side – is we are seeing this sort of interesting confluence between info wars and cybersecurity and digital identity theft. And, you know, the Ukrainians are having problems in their government of, you know, identities of government officials actually being misused in a disruptive fashion. So I don't think it's, you know, massive, but it's something that has been highlighted to me in the efforts I've got going on so far.

The other thing we haven't heard so much about is the Ukrainians have called for an international offensive cyber legion. And I think this is important to consider. You know, the things I've been involved with are clearly focused on helping the Ukrainians do cyber defense. But the notion of it, you know, basically relatively unconstrained call for offense against Russian, you know, internet systems is a challenging, you know, concept in terms of where the boundary is for those things that people are sympathetic for – you know, to help the Ukrainians, you know, against the Russian aggression, but then start to bleed over away from the Russian government and other systems.

I mean, the Ukrainians actually called for knocking the Russian country code off the internet, right? And so I think we've got some very interesting questions now. And the Ukrainians, as they have been in all things, have been very effective in mobilizing support for these causes. And, you know, one of the – one of the – I think an issue that we're trying to parse is how – why so little Russian effect. I mean, part of it could be, you know, the fact that the Ukrainians and others may be helping suppress some of the Russian offensive capabilities.

I am sympathetic to the notion that Senator Warner and Chris, you know, of the Russians are very capable. I guess I'll stop with, you know, as we learn from this – and I think we really do need to consider this a learning moment, because as we move to great-power conflict we are going to have to support other allies that are under pressure from – you know, from, you know, our major adversaries, is we don't have a great indications and warning system for Russian cyber activity. You know, we – the fact that we are all sort of working in the dark with a lot of hypotheses about how well the Russians have prepared the battlefield either in our ally or in the United States – you know, we know that they've done some work. I don't know that we know how dangerous they are. And that would be something that it would be worth getting a lot better at.

And you know, Senator Warner mentioned information sharing. I think these days I often use the term "operational collaboration," but I completely agree with the fact that effective defense is really going to be a matter of public-private activity. And even right now, the assistance to the Ukrainians as they move through this conflict should be a joint – you know, joint effort not just in the United States, but of the West to help them, and the private-sector entities in the West have a lot to add to that.

So I'll stop there, Jim.

Dr. Lewis: Great. Thank you, Greg.

Before we – there was a lot of good material in that and topics that are close to our hearts, but before we turn to them we got a question from Allied Maritime Command that touches on some of the things that you both raised. And the question is: We expected that the use of conventional weapons would occur in line with cyberattacks on critical infrastructure. Why did we see only limited effective Russian operations in cyberspace so far? And this is – we've touched on it, but I think this is really a crucial question. Did we misestimate Russian doctrine or the utility of cyber weapons? Or why are – why has it played out the way it's played out? Chris, do you want to go first? Or, Greg, do you want to go – Greg, do you want to go first?

Dr. Rattray: I'll go first, Chris, and then – yeah.

You know, look, I think, you know, we – one of the things we haven't talked enough about is the crucial nature of preparation in order to launch effective cyberattacks, particularly around critical infrastructures. So I think it's a very open question.

I mean, clearly, Russia for years has known how to go after critical infrastructure in the Ukraine, you know, but did – to Chris' point and others,

did the Ukrainians start to actually degrade that preparation, you know, and have they taken some of that option off the plate from the Russians?

The other things that have been mentioned a bit, I do think the Russians thought – in Greg's opinion, the Russians thought they would win easily. Massive miscalculation. Therefore, had reasons not to knock critical infrastructure off because they would – if they put in a surrogate regime, would have had to have that infrastructure there for the new government to operate. So I think, you know, as been mentioned, maybe they're recalibrating.

But I have this strong, you know – you know, belief, probably, that they aren't as deeply embedded and as capable as we – I mean, myself included – had thought going into this, at least in – at least in the Ukraine. I think everybody's right; in the West, we still need to keep our shields up as this crisis continues.

Mr. Painter: Yeah. I mean, I agree with Greg. I think there's several possible reasons.

One, it could well be that they weren't as pre-positioned as we thought they were. And pre-positioning on infrastructure, it takes a lot of time and effort. You simply don't – this myth that you press a red button and some way you have an effect, it's just not true. I mean, you need to have months/years of pre-positioning and presence on that critical infrastructure that they – and then activate during a crisis.

It could be also that when you burn the – when you do that, you burn that access. So they don't want to do that right now because they think they're going to take over the Ukraine. That infrastructure is going to be the same infrastructure that's going to support the country they take over. That could be part of it as well.

And it could well be that this was not a well-planned invasion, that maybe the cyber operators didn't even know this was going to happen on the time scale it happened. You know, it seems like this was very last minute, very from the top, and the cyber operators may not have been in the – in the club or in the clue.

I think another possibility, though – and I've seen this raised and I kind of agree with this – is, look, you know, even in Russia, the number of cyber operators is a limited set, the really sophisticated ones, and it may well be that they are using it for intel purposes now to look, to see what the intentions are of European, of U.S., of even Ukrainian leadership rather than destructive purposes. But whatever it is, it is somewhat surprising, but I don't think we're anywhere near out of the woods yet in terms of its potential use, and I don't think it diminishes – you know, I don't think this is,

you know, a Chicken Little story that because cyber hasn't been used that cyber has been overhyped.

I do think it's been overhyped in the sense that it can just be used willy nilly. But I think this does indicate that it will be a part of a physical conflict but maybe in the more limited roles.

Dr. Lewis: So I'm going to cheat. We're getting some good questions, and the three of us will talk. The Center –

Dr. Rattray: You'll talk now. (Laughter.)

Dr. Lewis: Yeah. No, I'm going to read the question from the Center for European Policy Analysis because it touches on some of the things we've raised.

What type of offensive cyber capabilities could the U.S. execute on Russia? Are there options on the table that have not yet been employed? If so, why not? And I think that's an important question. What are we waiting for?

So what are we waiting for? We all – like Russia, we assumed that we have tremendous capabilities. We haven't seen them on the Russian side, but we haven't on the Americans. What could we do? Why aren't we doing it?

Mr. Painter: Well, I guess one question is, you know, I, personally, don't know what access we have, what infrastructure we might be on. But assuming that we've prepositioned just like we assume the Russians are, you know, that's pretty escalatory to actually, for the U.S. – you know, it could be akin to a physical attack if we cause the kind of damage that, I think, that's being thought of. If we're just kind of fussing with their systems that really doesn't do much at the end. But if we're actually having an effect where we're taking down their command and control, that's a pretty major, major move on our part. It also burns those capabilities, as said earlier, to use later on if, for instance, Russia starts escalating against us or other things happen.

So, you know, I think that it's likely – I don't know, but it's likely we have those capabilities and they're not easy to come by, and the question is when and how to use them because they will have an escalatory effect and I think we're still trying to control this conflict or at least how it's being played out.

Dr. Rattray: I agree with Chris. The thing I'd add probably is and we wouldn't – we won't be able to answer the question, I don't think, very well, which is a good thing, about a capability to, basically, keep suppressing Russian offensive capability or ransomware capability.

It is possible that we have the capability to degrade their offensive operations and that that is underway and, you know, I wouldn't know one

way or another whether that is occurring. I think General Nakasone did mention in his testimony, you know, efforts to keep the ransomware groups suppressed at this time, which makes complete sense and, you know, again, to our comments, maybe has had some, you know, operational effect already.

But, you know, I agree with Chris that if we went farther and we're disrupting Russian life or even Russian command and – military command and control or defense systems, it could very much be seen as an escalatory step. So I just wanted to add that. So the offensive suppression capability, I hope, is there and it may be in use. So I just thought that would be –

Mr. Painter: Let me add just two quick things. There was an article today about the same actors – the Russian Internet Research Agency – are involved in a lot of this information now. We know that, at least it was leaked, that Cyber Command disrupted them before. So that's, certainly, potential to happen again. And the other is, you know, we're not going to do things like turn off the lights in Moscow. I remember when there was a story that came out saying that President Biden was looking at options being presented, options to do all these really destructive things in Russia.

You know, the U.S. actually does play by international law, and we're not going to have this disproportionate thing where we're going to go after civilian targets in Russia. I just don't see that happening. Nor should it.

Dr. Rattray: Yeah. And, you know, Chris, you and Jim and I have been in this discussion for years and years. But if we start to break down those norms, you know, and go after – the future conflicts just have even less limitations on the willingness of actors to bring those infrastructures into the game early on, you know, in a conflict, right.

Now, again, if you're the Ukrainians, I understand their call for offensive cyber action. But if you're the U.S. and you're trying to sustain a stable global cyberspace in the long term, it would be – you could, potentially, undermine that by some certain actions we could take in cyberspace.

Dr. Lewis: Yeah. I think the other part is that the pressure points in the U.S. and Russia are different, and Colonial Pipelines creates political pressure here. Putin could care less if there's a gas shortage or if the power is out in Saint Petersburg. So cyber – the cyber techniques that I think that article was talking about were probably not the ones that would be effective. But that does raise a question that I think both of you mentioned. The conversation's going a little different than I expected, but where we're talking about expanding the tool kit for responding to things like this, what does an expanded tool kit look like? It's not going to be turning off critical infrastructure, right, but – and I'm – to Chris's point, the sanctions are

relatively new. Let's see what the effect is over a few months. But what does that expanded tool kit look like for a more active posture in cyberspace?

Greg, do you want to go first?

Dr. Rattray: Sure. One thing that I think we could – well, we will learn and need to from this is actually how to help our allies, you know, perform effective defense, be ready, be prepared. Again, this situation has gone relatively well so far in cyber; we'll see how it plays out. You know, having been pretty deeply involved in Ukrainian efforts to be ready for these – the cyber piece of this, I think we could have done a lot more, and I think also the engagement by the private sector and being able to provide assistance now – we'll watch how this plays out as the Ukrainians operate under pressure and, you know, their communications systems may come under pressure. I actually think resiliency and readiness is a part of our tool kit that we need to put more into as opposed – you know, on the side of more offensive actions, the thing that I mentioned about being able to just keep attacks against Ukraine in cyberspace or keep ransomware groups under control, that is a capability. It's operationally pretty sophisticated to do, but I think that is something, again, that is less escalatory. You want to have a deep tool kit so that, you know, you can avoid our adversary sort of expanding these conflicts and coercing in cyberspace. You want to be able to suppress their ability to conduct cyberattacks, so I would put that in our tool kit.

Mr. Painter: So I've been heartened, you know – look, crises sometimes produce some positive silver linings and I've been heartened by the collective action that Europe, the U.S., and other allies have been able to bring to bear, and as Senator Warner said, it's surprising. You know, Germany and others who have been more reticent in the past have been coming out very forcefully. We've been acting collectively. The sanctions have been more collective so they have a better chance of success. We just have to now be able to use those sanctions in cases that are below this really high threshold, an invasion of another country. We have to figure out how that's used. But that collective action I think is key.

The other is how we can leverage some of the private sector capabilities. I mean, one of the interesting things – a lot of the private sector actors have pulled out of Russia without the U.S. telling them to do it; they just decided to do it, and so that's had an effect. We've also seen – it has been calls, as you said, Jim, to disconnect, you know, from the – Russia from the internet. I'm not sure that makes sense for Russian citizens and others, but I think a group of internet experts came together and said you can do more targeted stuff to go after particular Russian disinformation and other sites, you know, maybe black-hole some of that traffic, and that's the technical community I think can play more in that area. And the private sector has also been doing things to combat disinformation in the Ukraine and I think stepping that up. Now, the

private sector doesn't want to be on the front lines of nation state against nation state generally, but if we can find more creative tools that we can use, like that kind of black-holing and other things – you know, I remember having a debate with the former president of Estonia, Toomas Ilves, about this exact issue like six years and he said, unplug them from SWIFT and everyone said, you can't do that. Well, now we've done that, so I think we can think more creatively about both what our short-term and long-term tools and what the possible repercussions of that are and I think this – I think we've seen some of that activity.

Dr. Lewis: SWIFT thing probably accelerates the efforts of the Chinese to create an alternative universe, but in some ways that was inevitable.

Mr. Painter: We got a question, speaking of the president of Estonia, from the Estonian embassy, which is – it's a little off-topic from what we've been talking about but I'll drag us back. The EU has put sanctions on cryptocurrencies. What is the U.S. thinking about on cryptos in order to press the Russians? I will note that I wanted to have a CSIS cryptocurrency for some time now. It was after I read that the Burger King franchise in Moscow had a WhopperCoin. So if they can do it, we can do it. But what should we be doing on this? This is – cybersecurity has expanded. It includes stuff that when we started wasn't part of it, like information, like intelligence, and like cryptocurrencies. What do you think a good crypto policy would be? Greg, do you want to go first?

Dr. Rattray: Maybe two thoughts on that. In terms of this conflict, you know, I do see, you know, the emergence of cryptocurrency provides alternative, less regulated, less sanctionable means for all actors, including states, to potentially, you know, maneuver, you know, and avoid punitive action, right? So I think I've seen, certainly, that, you know, the constant discussion is, you know, having been at JPMC and, you know, watching the evolution of, you know, government regulation on cryptocurrency, we've been more hesitant in the U.S. to regulate heavily. It intersects importantly with also disabling criminal groups and cybercrime.

But now as cyber has become one of the dominant ways that criminal groups and criminal groups associated with states are able to make money, I think we have a major issue about how cryptocurrencies in particular are allowed to work, and whether we take off the table this sort of digital underground – dark, digital underground that's enabled by cryptocurrency. I actually think this is a very serious, long-term issue, you know, if we're going to have an impact on sort of the growth of cybercrime, you know? So I think I'm for it. And I'm not generally for a lot of heavy-handed government regulation. But in the crypto area, I think I am, for the reasons I just expressed.

Mr. Painter: So this is another thing that requires a global approach. Cryptocurrency is not going to go away. It is here to stay. And so the question is how do you –

you know, whether you understand it or you like it or not, it's here to stay. And there's some, you know, positive aspects of it is as well. So how do you – you know, I was one of the co-chairs of a ransomware task force. And one of the things we looked at – that came out just before the Colonial Pipelines attack, so it got a lot of attention. So one of the things we recommended on cryptocurrency was applying know your customer rules and anti-money laundering rules – which you should be doing anyway – to cryptocurrency providers and services. And that has to be a global approach.

And now that's starting to happen. Treasury – our Treasury Department's been actively going after some of the peripheral cryptocurrency players who are a little more shady. But again, you need a global approach, because they're not all based here. And then the Biden administration just had this crypto executive order come out, which is – you know, it's not clear what it's going to engender, but it's going to be studying different ways to deal with these issues. But I think that's good. I think we've kind of ignored the crypto issue for too long, and all the bad things that it's led to.

I think the major cryptocurrency operators don't want their services to be used for these nefarious purposes. It doesn't help them in the long term. You look back at other digital currencies – PayPal and others in the past – and they all evolve towards this more regulated and legal structure. So I think that's where we got to go. But we can't just do it alone. We're major players, but we have to work with other countries.

Dr. Lewis: I keep promising that I'll drag us back to the strategic topic we came here, but we're getting such good questions. Here's one of the Bahrain Cyber Police. Hundreds of thousands of Ukrainian technology workers have taken part in cyber actions against Russian's government, media, and financial institutions. OK, I accept that. I think we all do. But his question is – or, her question – how could something this huge be organized in the midst of war? Are they having an effect? And so I think both of them is how you organize this. The Russians and the Chinese tend to discount spontaneous reaction to their misdeeds, so that's part of it. But I'd be interested in your views. And then we can talk about effect after you answer that, to get back to a discussion of what a good cyber policy would be. But how do they organize this? Greg, you've been working with them.

Dr. Rattray: Yeah. And my efforts have sort of acknowledged, like you just did, Jim, that it's natural for them to call for this. And I'm aware that they've had a very large response across a – you know, not just Ukrainian, but even a global set of technologists being willing to take actions. You know, my insight would be – like, it's going to link to the effect thing. So it's not particularly difficult to call for, you know, disruptive action against websites or public-facing internet assets. The technology community knows how to find those and identify those as Russian, particularly Russian government, and therefore,

you know, try to, again, do denial-of-service attacks or hack those assets and, you know, deface websites. So it doesn't require a lot of command and control is maybe another way to put it, right, and my sense is it's probably not highly orchestrated in terms of, you know, seeking to degrade, you know, Russian military capabilities against Kyiv. This wave of cyber offense against the Russians is probably meant to be just broadly disruptive and to sort of just wear down the Russian will for continuing this. Could it become more targeted? You know, certainly it could. Don't have a lot of insight into that.

So I'll leave it at that.

Mr. Painter: Yeah. Yeah, I agree with Greg. I think it's hard to organize that in an effective way. When you see a real organized campaign like, for instance, against Estonia in 2007, I think there was more of a state hand there than just, you know, patriotic hackers who get together and organize themselves. So I think that's true.

You know, I also – you know, there's also the concern that even these patriotic hackers, these people who are trying to help Ukraine, they could be hitting the wrong targets. This goes back on the hack-back issues that we've dealt with in the U.S. So I don't know how much of an effect it'd have.

I certainly think it has an effect when you're exposing Russian disinformation, and I think that's what some of these actors in concert with, you know, established companies are doing. And I think that's a good thing and I think that's been effective.

Dr. Lewis: So maybe a final question, then, and building off some of the ones we've gotten and what you've said: What's the lesson here for the U.S. in terms of cybersecurity? I mean, this hasn't played out the way, I think, many had expected it to play out, at least in the initial weeks. And I agree with Chris that as the Russians get bogged down they're going to be tempted to do something nasty, maybe in ransomware. But what's the lesson we should take away from what we've seen so far when it comes to Western cybersecurity and American – the cybersecurity of the U.S. and our partners? I don't know who wants to go first.

Mr. Painter: I'll go. I think there's two things.

One, as I said, we're not out of the woods yet. We are incredibly dependent – probably the most dependent country – on computer networks and systems. And you know, and we don't want to self-deter as we did after the 2016 election interference where we had the DNI then saying, oh, we didn't want to do something because we were afraid of what Russia would do against us. I think there's a little bit of that still there, that we're afraid of our vulnerabilities, and I think that's bad. So we have to get beyond that.

But on the positive side, I think the collective action that's happened with Europe and other partners and the U.S. on sanctions and other measures is a really good thing that needs to be built upon, and that is a really strong international play that we can continue to do. And I think that has some very positive aspects for cybersecurity.

But I – but I don't think this detracts from the danger we face from cyberattacks. I think that's still there, even if it hasn't played out yet in this conflict.

Dr. Rattray: So I'll just put two in as well, building on Chris's second point.

That collective action can be in cyber and can be on, you know, cyber assistance. And you know, and I think we'll be doing that, and we're learning lessons every day right now about how to help the Ukrainians as they, you know, reconfigure and deal with this to defend their systems and to keep them up – which has gone, as you said, Jim, surprisingly well or it's been a surprise.

The other fact is to try to understand better what the Russians' intentions and abilities are in cyberspace. And as I started my remarks, like, indications and warning – getting a stronger ability, like we had on their mobilization to invade. I think we don't quite – we're not – we don't yet have our – the ability to understand what our adversaries might do in a crisis in cyberspace the way we do with conventional military forces, and that needs to be something we focus on.

Dr. Lewis: Great. Well, thank you both.

So the lessons I take away from our conversation and the conversation with Senator Warner is we need to support the Ukraine. We need to think of ways we can support them maybe more than what we've done now.

The other lesson is that Putin has really painted himself in a corner. I don't think Russia can win in this situation. I don't think they'll come out of it better. Even if they manage to establish a Chechnya-like control over Ukraine, they can only lose. So I hope that's a good lesson for anyone else who might be listening in in the Far East: invasion, a bad idea.

Let me thank Senator Warner for his very insightful remarks, and thank Chris and Greg for joining me in this discussion. Thanks to everyone. As usual, the recording will be online. Thank you and see you soon.

Mr. Painter: Thanks.

Dr. Rattray: Thanks.