Center for Strategic and International Studies

TRANSCRIPT

Online Event

"Book Launch: Three Dangerous Men with Seth Jones"

DATE

Friday, September 17, 2021, at 12:00 p.m. EDT

FEATURING

David E. Sanger

White House and National Security Correspondent, and a Senior Writer, The New York Times

CSIS EXPERTS

Seth G. Jones

Senior Vice President; Harold Brown Chair; and Director, International Security Program, CSIS

Emily Harding

Deputy Director and Senior Fellow, International Security Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Emily Harding: Hello to our two panelists and to all those joining virtually. Both of our panelists today have added substantially to the public record on a critically important topic: gray-zone warfare and the future of great-power competition. The launching pad for our discussion today is Seth Jones' new book, "Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare." We'll cover some really compelling stories from the book, but also talk about the future of conflict in a broader sense. So, first, let me introduce Seth Jones. He is the senior vice president at CSIS, the Harold Brown Chair, the director of the International Security Program, and the director of the Transnational Threats Project. In his copious free time, he also teaches at Johns Hopkins School of Advanced International Studies. He's held a wide variety of roles in the national security business, including the representative for the commander of U.S. Special Operations Command to the assistant secretary of defense for Special Operations, which is a long title meaning he was the link between the military and the civilian side of Special Operations. He also served as the advisor to the commanding general of Special Operations forces in Afghanistan. So, he has had many opportunities to view irregular warfare and gray-zone activity up close and personal. We also have David Sanger. His official New York Time bio calls him a senior writer, which seems about the understatement of the century. He has a 38-year reporting on top national security issues. He served on three teams that have won Pulitzers. His latest book – and I'm sorry I don't have a copy with me here, but I have been reading it – is called "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age," which was also made into a very compelling HBO documentary. Both are a thoughtful exploration of the implications of the new tools of warfare in the cyber domain. For me personally, in my previous roles in the intelligence community we often referred to him as, David "how the bleep does he know that" Sanger. (Laughs.) We're pleased to have him here today as a guest. So, "Three Dangerous Men." This book is a serious topic, but a fun and approachable book. It uses the stories of three military intelligence leaders to describe how adversaries are using measures short of war to frustrate and undermine the U.S. It talks about Valery Gerasimov, who's the Russian chief of staff of the armed forces – you know you've really made it when you have a doctrine named after you, and he has one: the Gerasimov Doctrine – Qassem Soleimani, the now-deceased head of the IRGC Quds Force; and Zhang Youxia, who's the vice chairman of the Military Commission in China. So, as we read the stories of these three men and their approaches to modern warfare, it occurs to me proxy forces, mercenaries, propaganda, all as old as warfare itself. So, Seth, talk to us about what's new here. What's new about the Gerasimov Doctrine, about China's whole-of-society approach, and about Iran's proxy warfare?

Seth G. Jones: Thanks so much, Emily. As you note, there is – the use of irregular, asymmetric, gray-zone tactics and strategies is as old as war itself. You just have to go to books like Sun Tzu to see the importance of deception, the importance of how to win without fighting that comes from those very influential documents. The Chinese have also given us Mao Tse-tung, for

example, and his pathbreaking work on guerilla warfare. So, what's new? This is a – it's a great question. I think there are a few things. One is the U.S. is shifting now from a focus on counterterrorism to great-power competition. So, we saw that first in the Trump administration's National Defense Strategy. We saw it with the interim strategic guidance from the Biden administration. But I think the question, though, is as the U.S. focuses on competition with the Russians, the Chinese, and even the Iranians, what forms is that likely to take and how do we think about competition? In the military there's a lot of focus on, understandably in many ways, large conventional wars, whether it's with the Chinese in the Taiwan Straits or the South China Sea, with the Russians in the Baltics. How much of that is really going to be the domain of future warfare and how much of it is going to be in the irregular side? So, I think the shifting strategic landscape has changed. There are also a number of new elements and how they've been utilized. One – and I defer to David when he talks – but you know, one is certainly the cyber side of this, and the use of social media and digital platforms for information and disinformation campaigns. That's certainly not something that we saw during the Cold War between the U.S. and the Soviets, even though the Soviets – Service A of the KGB was heavily involved in active measures. In addition, we certainly have also seen the increasing use of various types of private military companies, shells, and fronts that have gone on – gone along with that, including the Russians' use of the Wagner Group and others in Africa, in the Middle East, in Latin America including Venezuela, and overlaying those activities with Russian intelligence – both military intelligences, GRU, as well as the foreign intelligence agency, the SVR. So, there's a bit of a new dynamic with how private military companies are used for influence and how they're also used on the economic side. There's also some newness to – at least new developments on the economic side. I'm going to call it economic coercion. So, the use of the Belt and Road Initiative not just for – by China – not just for economic investments in countries, but also using the leverage from that to pursue issues of interest to the Chinese regarding Taiwan or the Uighurs or Tibet – so issues of strategic importance to the Chinese – and then, you know, how this is done. So there have been new elements in this even though the – just the concept of irregular warfare, Emily, is – as you point out, it's not new.

Ms. Harding: So, David, with that I will turn to you to talk about that cyber issue that Seth raised. In your book *The Perfect Weapon*, you wrestle with the analogies between conventional warfare, nuclear warfare, and cyber warfare, and you talk about how these inapt analogies; they don't – they don't always work out. So, what's the closet analogy that you did find? What bad habits in our thinking do we need to break here? And if you could especially focus on the lessons for deterrence theory, I think that's a ripe topic for conversation here.

David E. Sanger: Sure. Well, first I wanted to say how much I enjoyed reading Seth's book and how the technique he had used, which I just admired as a writer, of encapsulating these three really fascinating different national approaches through three very difficult kinds of intelligence and military officials, it's

just a great read. And I think, Seth, not only congratulations to you, but I think it's going to become required reading in irregular-warfare courses in universities maybe even beyond just SAIS. (Laughter.) So, it's terrific, and to our audience here today I would commend it. So really great question that you've raised here because in the early days of cyber there was this tendency for people to say, well, this is like the new nuclear weapon, right? And by the way, we could – why can't we deter it the same way that we deterred nuclear weapons, where it took us 10 years, but we came up – or 15 – but eventually came up with a mutually assured destruction kind of approach? In fact, it is, as you say, an inapt analogy, just doesn't apply. All the questions about deterrence in the nuclear arena also arise in the cyber arena and every one of the answers is different. And the reason for that is that cyber is available not just to nation-states and not just to terrorists, but to criminal groups and, worse yet, to teenagers. And you know, outside of the nation-states, those three groups don't tend to sign arms-control treaties, right? So, the whole concept that we ultimately had, which was that we got the two largest possessors of nuclear weapons – the U.S. and the Soviet Union, and ultimately its successor state in Russia – to diminish the size of their arsenals just will not work in cyber. The second misapprehension we had, I think, was that cyber would be used initially just as a surveillance tool. And if you think about it, it makes sense that we started thinking about this because, you know, the post office was created and we learned how to open people's mail; and then the telephone system was invented and, you know, not long after Alexander Graham Bell went to all that work, we figured out how to intercept phone conversations. So when people first saw cyber they thought, terrific, you know, we can read each other's emails, and that falls into sort of traditional intelligence collection. But as Seth points out in his statement and as he does again in the book, the really interesting uses of cyber are not surveillance uses. So, there is the social media side, which is really more understood as more like propaganda than a cyber operation. I mean, Stalin used to put ads in farm newspapers in America in an effort to go try to influence Americans, you know, in the 1930s. He just couldn't measure his results the way you can if you're having the Internet Research Agency go at it. But to my mind, the most interesting uses of cyber are closer analogues to what Seth is writing about in "Three Dangerous Men." You can use cyber to manipulate data. So, you know, it can be as basic as trying to recalibrate the aim of a missile but as pernicious as getting into the Pentagon's health database and changing the blood type of every soldier and sailor. Imagine the havoc you could wreck. You can try to conduct attacks that previously you could only do through sabotage, putting somebody on the ground, or bombing them from afar. So, when the United States and Israel decided to go after the Natanz nuclear enrichment plant, they considered the sabotage and the bombing effort and decided in the end that if you could use cyber it's much harder to go trace who's doing it, but more importantly you may not prompt the kind of military reaction you would get from bombing. And then the third arena in which you can use cyber is as an influence operation. And as Seth points out very well in his chapters on Gerasimov, to the Russians this is all on a spectrum. You know, we think of information operations separately from using cyber as a weapon. They think of it all in a continuum. And interestingly, the Chinese

are beginning to as well. So, to the deterrence issues, you know, we just went through a lot of panels on 20 years after 9/11. And you know, the most remarkable thing is we actually managed to improve our defenses so well that we got a fair bit of deterrence by denial, by it's hard to get a bomb up on a plane or into Times Square or through the – through the tunnels or whatever. It's not impossible, but we've just done a much better job at early detection and defense. And frankly, that's where we've done a crummy job in the cyber arena, where we are just so vulnerable as a society – as you could see with the Colonial Pipeline case, a ransomware case in which the attackers didn't even plan to cut off the flow of gasoline up and down the East Coast but it happened anyway as the company cut it off – that that's really where we've got to begin to think about a true national effort.

Ms. Harding: Well, so on that happy note – (laughs) – Seth, we're talking about this continuum and how our adversaries think about war not as war and peace as we tend to, but as war, measures short of war, an entire continuum of possibilities. How are we set up to respond to this? You have – the last chapter of your book you devoted to some recommendations. How is the U.S. set up or not set up to go about combatting this approach to warfare?

Dr. Jones: Good questions. Let me just start off, Emily, with talking about warfare because there are a range of different ways that one can refer to this. It's been called gray-zone activity or asymmetric. I think the term "warfare," I use it deliberately for a couple of reasons. One is I think it – this is – this is the use of warfare that's much closer to Sun Tzu than it is of the Prussian soldier and theorist Clausewitz. If you read Sun Tzu, the supreme art of war is to subdue the enemy without fighting, so it's without actually having to resort to violence. And I think in particular when you – when you look at the terminology used by a number of the countries, I looked at here, China uses terms including "three warfares" to describe important components of this. Three warfares are the use of media, propaganda, psychological, and legal warfare for the export of states' power and influence. So, it is warfare. It is a component of warfare. The Iranians have a term that they use, which is "jang-e narm," which is "soft war." Probably not too different from the concept of soft power in the U.S., but again defined in part using ideological information means as warfare. And then even as – the U.S. military historian Charles Bartle's referred to this as the important point for understanding how the Russians use these instruments, he said, is "while the West consider these non-military measures like information operations, covert action, support to nonstate actors including proxies – while the West consider these non-military measures as avoiding war," the Russians consider these measures as war, as a component of war. And so that's why I think the terminology here important, because, I mean, the whole idea here is to be understanding how they view warfare and competition. So these instruments are critical as part of warfare. And in kind of understanding the way the Chinese think about it, I mean, I found it quite – I found a great movie. I wouldn't – I wouldn't suggest that people start running to go watch "Wolf Warrior 2." The general explosion scenes are sort of like 1990s Hollywood. But it is still, I think, the highest-grossing film in Chinese history. This is "Wolf Warrior 2." And what's interesting here is the signals that the

Chinese are sending. The movie character is not a Chinese infantry officer; it's a – it's a former special operations soldier. So, it's someone who can do both kung fu and he's part Rambo. In addition, it takes place not in the South China Sea or in the Taiwan Straits or even in Taiwan; it takes place in Africa. And who's Leng Feng's enemy? It is Big Daddy. It's a – it's kind of an American drawl – it's actually an American character in the movie. And the message of this – of the second version of "Wolf Warrior" is, at the end, as Leng Feng kills Big Daddy, is basically the United States is the past and China is the future. "You are history," he says. So, this gets to your question about what do we do about it. And I think, you know, this aspect, Emily, that you talked about at the beginning on warfare as really a continuum, not as dichotomous, gets to the way the Cold War was at least partially conceptualized by some of the more influential individuals like George Kennan in the U.S. That's the way Kennan conceptualized warfare between the U.S. and the Soviets, as operating – not dichotomous, it starts and its ends, but as a continuous, hourly, certainly daily activity. And I would say particularly with the Chinese, the U.S. is just – I mean, it's just not prepared, really, at all. It's not structured this way. It doesn't have the resources. I mean, what I find most concerning in many ways is even how U.S. competition with the Chinese is conceptualized in the Department of Defense. The OPLANs or operational plans, you know, the scenarios used to plan for future competition, the weapons systems, you know, almost entirely envision conventional fights with the Chinese, whether it's in the Taiwan – in the Taiwan area, in and around Taiwan, or the South China Sea. In addition, I mean, I find it striking how the U.S. from an information standpoint is nowhere near prepared. We don't have translations of Chinese material, the entire open-source enterprise. During the Cold War, we had the U.S. Information Agency and as part of that the Foreign Broadcast Information Service, translated huge amounts of Soviet-Warsaw Pact radio programs, television, you know, magazines, newspapers to understand what was going on not just inside of the Soviet Union, but also in its Warsaw Pact allies. And we've got – we've got nothing along those lines. The Global Engagement Center at the State Department is underfunded, under-resourced, and I mean, in many ways is considered a backwater. So, I think we have to get really serious about this. Beijing has not made the same mistake. The Chinese newspaper with the largest domestic circulation is a compilation of foreign news articles, including English-language reports that are translated into Chinese. That is the largest domestic-circulated newspaper in China. So, I think what it shows is there's a huge focus on understanding us, from the Beijing side, but not a lot from the U.S. towards the Chinese. There's also, Emily, a lot that we did in the 1980s in beaming in Radio Free Europe and Radio Liberty into the Soviet Union and Warsaw Pact, which was, frankly, very successful in opening up dialogue in those countries. We see in China, Russia, Iran, all of them are closed societies. They're not democratic. They don't have freedom of the press. They don't have freedom of religion. So, you know, part of the focus, I think, has got to be beginning to open them up, and there are both technical tools that the U.S. can use but also just a constant campaign. And thankfully from a U.S. standpoint, it doesn't have to be disinformation, but everything from the assassination of defectors – we've seen it on the Russian side – to, you know, the international coercion

campaigns that have gone along with the Belt and Road Initiative, to the massive doping scandals that both the Chinese and the Russians have been involved in, to the extraordinary pressure the Chinese put on companies including in Hollywood, the NBA – which they put significant pressure on the NBA, including executives, not to criticize the Chinese government or Hong Kong or they will take NBA games off of television in China, which they did and which the NBA leadership paid a big economic price for doing – I think there are a range of tools even from the last decade of the Cold War that the U.S. could do differently.

Ms. Harding: Right.

Mr. Sanger: I'd add – I'd add one more to those, Emily. I agree with everything that's on Seth's list, but I think in some ways the most important move the Chinese have made and that the Russians just cannot, and it's sort of the difference between their approach – and the Iranians cannot – is that they were well on their way, and still are, using Huawei to wire the world, right? So, you know, if you think about the first real pushback by the United States and some its reluctant allies on the Chinese, it was in the effort to block Huawei from building 5G networks. And initially, our allies were quite reluctant. Some still are. And the Chinese have made great inroads in Africa and Latin America and so forth in building these. But why is this important? Because we were looking at this, as Seth suggests, as a commercial project. And frankly, we didn't have a whole lot to offer. And the Chinese were looking at this as both a commercial opportunity and an opportunity to make sure that the information that flows around the world flows not through the United States, which built all the initial networks, but instead would flow through Beijing or Shanghai. And that has made a huge, huge difference. And only in the past two or three years have you seen the United States begin to push back. Even President Trump viewed this half the time as a trade issue – well, maybe I'll give away the 5G thing, you know, if I get a better deal on something else – which was a fundamental misreading of what the importance of 5G was to the Chinese plan. And it's interesting, this week, you know, we've spent our time discussing Australian submarines up through the region, which is important and an important way of pushing the Chinese back. But if you made me choose between control of the submarine routes and control of the – of the submarine cables flowing around the world – the two have some relationship – I'd pick the cables any day.

Ms. Harding: Yes, because of this information warfare piece that we've been talking about and because if you control the information, you control the world. I have to give –

Mr. Sanger: And you have the ability to turn – not only to listen in, which, you know, the Chinese are good at doing now, but turn it off.

Ms. Harding: Right. Some of those tables get snipped and we're all in trouble. I have to give a small bit of kudos to my former boss, Chairman Burr, and Chairman

Warner for their leadership on the 5G issue. I think that that was a real wakeup moment for the United States government.

Mr. Sanger: Yeah, and they managed to do it together and it was relatively bipartisan. And there's a huge amount of work – most of it classified so it's, you know, hard to go dig out – about U.S. efforts to protect those undersea cables, and it's part of what that Australian submarine deal is about.

Dr. Jones: Well, this is – this is the whole reason that you focus a lot of your activity on irregular activity. It's not – this is – this is how you take islands in the South China Sea, turn atolls into essentially military bases. You do it with dredgers, not with – by bringing in PLA Navy forces to control the islands. I mean, this is – this is – the whole use of underwater cables for information, 5G, 6G where we're headed next, I mean, this all off of the overt radar screen. And this is part of the point that I think both David and I and even Emily are making now, is these are less publicly aware activities but they're extraordinarily important components of competition.

Mr. Sanger: And they are not even – they're not the side issue as they were once considered to be. They are the central game. And you know, you were asking me for better and worse – you asked me at the beginning, Emily, what's the – what's the better analogy. I think the better analogy is the invention of the airplane, right? When Wilbur and Orville Wright first showed aircraft to American military officials in 1909 up at what is now the University of Maryland at College Park out on what is now the soccer field, and they flew their – they flew the Wright Military Flyer around, the initial reaction of the Army was this is a great surveillance device. You know, we'll fly it out over enemy troops, and we'll see where their openings are and we'll send in the cavalry, right? So, they were thinking of it all as surveillance. What's this like? It's like the early days of cyber. And it took about five or six years for the Germans to catch on and say, hey, we could drop bombs from this thing, right, or we could – or we could arm these planes. And at that time there was a lot of discussion, including in Britain – I've got a great British book published in 1910 called "Aeroplanes in Peace and War." And the question was, could London ever be bombed? Well, we answered that relatively quickly, OK?

Ms. Harding: Oh! (Laughs.)

Mr. Sanger: So, by World War II, airplanes moved from being this sort of interesting sideshow to being the central strategic weapon. And the question here is, is cyber and the other irregular techniques that Seth has laid out so well in the world, are – will they in 20 or 30 years be the central game? And my guess is the answer to that is yes, because no one wants to take the U.S. military on frontally nor do they see that as particularly advantageous.

Ms. Harding: Right.

Dr. Jones: David, if I could just jump – if I could just jump in one time – sorry, Emily – just to – just to highlight the point here, I mean, I think there's this interesting period when the Soviets and the Americans are close to war during the Cuban Missile Crisis where it dawns on both leaders that a nuclear war, if that's where this goes, now you're talking about, you know, threatening cities in both the U.S. and in the Soviet Union. The reality of nuclear weapons – and you know, one of the ironies of participating both in classified and unclassified wargames with the Chinese is when you're fighting in and around the South China Sea and you're flying F-35s, part of your suppression of enemy air defense almost inexorably includes striking targets along the Chinese mainland because that's where they're shooting missiles or that's where their radar systems are or electronic warfare. That raises the prospect of nuclear war, because when you start conducting strikes in and around someone's homeland it becomes very difficult to distinguish are these – are these measures that you're doing so that you're protecting your aircraft or your forces on the ground in Taiwan or your submarines or your aircraft carriers, or is the next step you're going to start hitting Beijing and you're going to attempt to overthrow the government? It becomes very hard to distinguish offense and defense and that balance. So, the issue is, I mean, that looming issue of escalation to nuclear war I think will be very concerning to both leaders in Washington and Beijing. And you could – you could also extend this analogy to Moscow and Washington in the Baltic states, which is why it's partly what David said, which is that the U.S. is conventionally and from a nuclear perspective continues to be quite strong but also now all these major powers, they have nuclear weapons. So conventional or nuclear war, I mean, you're talking about huge economic impacts. I mean, one scenario that RAND ran, the Chinese GDP in a war decreased by 25 percent just because of the destruction that was caused by the war. So, what I think this means is the day-to-day activity gets pushed below that threshold.

Ms. Harding: Absolutely. So, on that note, our adversaries very much seem to be playing a long game. They are looking to undermine America in various ways. The Russians in 2016 did a masterful – probably a better job than they expected to do making us question each other, making us question democracy, and really undermining the roots of what makes us function as a society, and that's a very long-game kind of strategy. As Americans, you know, we tend to be optimistic and go get 'em, but it often means that we tend to think a little bit more short term than our adversaries. How should we be adapting to this long-game perspective? And what do you see as the potential inflection points in this long game?

Mr. Sanger: Do you want to go first, Seth?

Dr. Jones: No, no, no, you go ahead first.

Mr. Sanger: OK. Well, the first is they are playing it for the long haul and that's not something democracies do really well. Because we change presidents every four or eight years and because in that time period you can have major

changes of policy – and you know, that's just the way democracies operate – we have a much harder time setting 10-, 20-, 30-, 40-year goals. If you want to look at the best example of this – and again, it goes to competition with China – look at the China bill, the infrastructure bill that went through the Senate early this summer, still has not passed the House. So, all of the technologies that we are thinking of putting money into, billions of dollars into in sort of new industrial policy – AI, quantum computing, semiconductor lithography, autonomous vehicles, long battery life issues, encryption, all of that – the list matches up almost perfectly with China's Made in China 2025 list. The problem is they started their Made in China 2025 list in 2015. And so, they're in year six. They'll make it on some; on others, like semiconductors, they are behind. You know, so it's not going to be a 100 percent success. We shouldn't say they're 10 feet high. But here we are, like, just getting our long-term government involvement strategy together in 2021. And it's entirely conceivable, if you have a change in government come the next presidential election or even the one after that, that that whole effort gets interrupted. So, one thing that's common to the three societies that Seth writes about in "Three Dangerous Men" – China, Russia, and Iran – is they don't go through this process. Their downside is they don't have the kind of entrepreneurial energy that we do. They've got greater focus and probably less content. And I think the race of the next few years is going to be which of those turns out to be more important.

Ms. Harding: Seth, do you want to chime in there?

Dr. Jones: Yeah. Just to add to that, so let me – David focused on the Chinese. Let me just start with the Russians. You know, the Russians are starting with a much weaker hand. You know, they're not the economic power that the Chinese are, and they won't be. But when you look at the long-term strategy, I mean, it's important, I think, to look at where the Russians came out of the Cold War, and they lost out in so many different ways. They lost the Warsaw Pact countries, virtually all of whom went to the European Union and NATO. They lost their southern flank. The U.S. deployed forces to Afghanistan, obviously where they had invaded at the end of the 1970s. They lost partners in Libya after the U.S., the French, and the British overthrew Gadhafi. So, they were in pretty tough shape over the next two decades after the end of the Cold War. So, what does the Russian long-term game plan look like for individuals like Gerasimov? You can see it starting to happen in 2013, 2014, 2015. And again, look at the annexation of Crimea. It is done in ways that look a lot like Sun Tzu's use of the tools of warfare to subdue the enemy without fighting. The Russians didn't fire a shot, really, in Crimea. They used Spetsnaz and Russian special operations forces, disinformation campaigns, intelligence, individuals, so in that sense – SVR as well as GRU. So, starting to take back territory and influence. Look at supporting Assad. I mean, there was – there was grave concern during the Obama administration that the U.S. would back rebels and, just like they had done in Libya in 2011, overthrow the Assad regime. Well, what did the Russians do in response? They did not do what they did in Afghanistan starting in 1978 and '79, which is deploying over 100,000 infantry soldiers, armor into Afghanistan. Instead, the maneuver force – so they conducted strikes from

maritime vessels – caliber, cruise missiles. They also dropped some bombs from fixed-wing aircraft. But who was the maneuver force for the Russians in Syria? It was Lebanese Hezbollah, a U.S.-designated terrorist organization. It was Iranian-trained militias from Iraq, Palestinian territory, Afghanistan, and Pakistan, among other places, I mean in addition to some Syrian forces. It was a very different way of protecting an ally and then using bases in that country for power projection. How do we see the Russians attempting to expand not just their influence, but also their economic activity in Africa? So China has its Belt and Road Initiative. You know, not saying this is going to be a particularly effective strategy, but the Russians have deployed their private military companies and their shells and fronts to Central African Republic, Madagascar, Mozambique, Egypt, Libya, and a whole – Venezuela, Nicaragua. We've seen the Russians deploy these kinds of forces – again, not large numbers of Russian infantry but also a heavy focus on Wagner Group with the support of Russian military intelligence, the GRU, and the SVR. So, what we see in the long game is the Russians trying to expand influence in Eastern Europe, in South Asia, in the Middle East, in parts of Africa, and even in Latin America, primarily through irregular means. I would say on balance it's actually been fairly successful with the weak hand that the Russians have had. And I would wholly support David's comments. I mean, look at Made in China 2025. It is – it's a 10-year plan to transform China into a leading manufacturing power by 2049. That's the 100th anniversary of the founding of the People's Republic of China. But look at how they've been also doing it. It's significant stealing of technology to be competitive, both from a defense industry perspective as well as business perspective. What makes the Chinese nervous – and I think this is – this is kind of the last issue I wanted to raise, Emily, is what makes the Chinese nervous about its approach. I think it feels nervous about Hong Kong. You know, it's an area that it needs to watch very closely. It feels a little nervous – and we've seen it in the last couple of weeks with the overthrow of the Afghan government by the Taliban, that the Chinese have basically said both to Mullah Baradar on his trip to China in the summer as well as to senior Pakistan leaders that with the rise of the Taliban: You must take care of the Uighur problem in China. We do not want to see East Turkestan Islamic Movement sanctuaries/base camps operating from Afghanistan. They can conduct attacks inside of China. So there certainly are concerns about some of these internal dynamics that I think makes the Chinese a little worrisome as part of their long-term strategy.

Ms. Harding: Absolutely. So, I want to turn back to the idea of this book as part biography and part lessons for the future of warfare. There are three very different men that you describe in the book, but they do have some similarity. So, I'm curious as to what you – what your takeaways were on the personality characteristics that made them successful at their jobs, how they went about it, what you see as the similarities and differences. And, David, then I'll turn to you and ask a question sort of from the flipside, which is that, given what we know about these men and the way that these countries go about irregular warfare, what are our options for trying to push back?

Dr. Jones: So, I think there are a couple of things that I was particularly interested and in many ways surprised by Qassim Soleimani, by Zhang, as well as by Valery Gerasimov. All of them actually studied pretty carefully the last several decades of warfare by the United States. I mean, they were – they were – I mean, it was almost like Ph.D. exercises in understanding both the U.S. weaknesses and its strengths. U.S. overthrows the Taliban regime not by sending in large numbers of forces, same thing in Libya, but using small numbers of Special Operations forces, CIA paramilitary on the ground, and some airpower that went with it. Also, a recognition that the – some of the U.S.'s weaknesses – the large deployment of forces on the ground, the 100,000-plus in Iraq and Afghanistan. So, you know, what did the U.S. do well? What did it not do well? There are also some interesting, almost bizarre lessons. You know, reading Gerasimov's historical overview of the past several decades, he gives a lot of credit where credit really isn't due to the U.S. for its involvement in the Arab Spring, in overthrowing multiple countries across the Arab world, as well as the color revolutions. So, I mean, my guess is that if you asked a range of individuals at Langley, they would have loved to have been involved in more of those than the U.S. was ever involved in, but you know, the Russians saw U.S. hands in everything from Ukraine to a number of other countries in Eastern Europe and across the Arab Spring. So, I mean, that's one big theme that cuts across all of those. And I think a second we've already highlighted to some degree, which is a recognition that – certainly true in Zhang and Gerasimov, but also Soleimani and his successor Ismail Qaani – how powerful the United States is from a conventional and a nuclear standpoint, and how weak the U.S. has even just looked in Afghanistan at the hands of a pretty well – or pretty poorly-equipped Taliban force that wore the U.S. down, conducted guerilla raids, like, almost directly right from Mao's guerilla warfare book, almost directly from Sun Tzu. So, the U.S.'s weaknesses are in these areas. So, I mean, just to summarize is how much really students of history all three of them were. I mean, their own interpretations of history, but all three historians of the U.S. experience and trying to pull lessons from that, I mean, I found – I found quite surprising.

Ms. Harding: One of the really frustrating things about trying to conduct diplomacy with the Russians is saying "but that wasn't us" and them absolutely not believing us that it wasn't us. And if you say you didn't do it, then they say that's exactly what you would say if you did do it, and there's just no convincing them that our hidden hand is not behind everything. So, David, over to you. What options do we have for these men?

Mr. Sanger: Well, first, in – when you turn the mirror around, we don't believe they're not involved in a lot of these operations as well. And so, you know, the most recent great example of this is the ransomware craze, right? So, you know, the other day General Nakasone, the head of the NSA and Cyber Command, said at a conference here in Washington, you know, six months ago if you raised ransomware, I would have described it as a criminal activity, which was his nice way of saying not my problem, right? I got plenty to do in all the areas that Seth just described, hand the ransomware characters over to the Justice Department. They want to go indict them or block their funds, you

know, that's their job, not my job. Now, all of a sudden, we view ransomware as a central national security threat, by President Biden's own description, if it's emerging from Russia the Russian government must either be tolerating it at a minimum or encouraging it as a way to undercut us. Which takes us to your question, Emily, who is, what do you do to begin to deter this kind of activity? And the – what it hinges on is, do we come to define national security in a much broader way than we did? That if the Russians are going to determine that our greatest vulnerability isn't what they can do to us in the South China Sea but the fact that they can get into the electric grid or they can get into Colonial Pipeline or they can execute the kind of attack – Seth makes a brief reference to it at the beginning of his book – that they did in SolarWinds, where they basically got into the update system of a piece of software that was used across corporate America, even at The New York Times, and across the federal government, then they can do far more damage than they could do with a conventional kind of – with a terror attack, much less a conventional attack. And that takes me back to my first point, which is we have to think about the cyber defenses for our own society the way we thought about securing airports and so forth after 9/11, and we're not at that point yet. And we're not at that point yet because our adversaries, including these three men, have figured out that if you calibrate the attacks at a low enough level, you're not going to get a kinetic response and you're probably not going to get much of a response at all. And that's what's happened. And so, we keep talking about raising the price, raising the cost. How many times did you hear that when you were on the Senate Intelligence Committee? Seth, how many times have you heard that, you know, in meetings with Special Forces? But clearly, we have not raised the cost to the point that it's led to a diminution of activity. The president of the United States just went and spent most of a meeting in Geneva in June with Vladimir Putin and spent it warning him about ransomware, and we had a nice abeyance in the summer while some of their best hackers I guess decided to go to the Black Sea and enjoy the sunshine. But all the evidence is they're back at this point. And so, the answer to that has got to be some mixture of much higher pain and much higher defenses.

Ms. Harding: That's absolutely right. And this question of deniability, I mean, this underlies a lot of what's in the book – both of your books, actually. You know, it's an adversary conducting activity that is an arm's length removed or several arms' lengths removed, and the Russians in particular are really outstanding at this idea where they can say, well, they're not under our control even though we know that generally speaking the way the Kremlin operates is that people are allowed to do things as long as they are in line with the Kremlin's interests. We see this with the PMCs. We see this with some of the ransomware groups. They get a little bit out of line, and they get a quick correction, but as long as they're operating in line with Kremlin interests then they're allowed to continue, and the Kremlin gets the opportunity of the deniability. That also makes it much harder for American policymakers. One of the things that we saw with the Russia report in 2016 was the Obama administration really struggling because they wanted to know for sure that this was Russian activity before they tried to deploy any of these carrots and sticks that you're talking about, and this gray-zone

activity is just not the kind of place where you get that kind of certainty. And I think that is going to be a huge challenge for American policymakers operating in this realm where you are not going to be sure, but you still have to respond in order to preserve these tools of deterrence. So, Seth, I'll throw that to you to see if you want to react at all, and then I have a couple more questions before we wrap up.

Dr. Jones: No, I think I would actually agree with what both of you said, so I don't have – I don't actually have any more to add to that.

Ms. Harding: Well, then, that's a win. (Laughs.) We all agree. We're all set here. We're done. (Laughs.) Seth, I wanted to ask you a little bit about your original document use in the book. It was really fun to see you pull from some of Gerasimov's PowerPoint presentations, some of the Chinese documents that you found. Can you talk a little bit about how you went about finding those and what you did to translate them and make them usable?

Dr. Jones: Emily, this is – this is a much bigger issue than I had anticipated. There actually was – you know, there was a fair amount of Russian documents available. I mean, I identified a bunch of what Gerasimov had said. I do speak a little bit of Russian, so that was helpful. What I found particularly discouraging was the – well, were two things. One is during the Cold War and even in graduate school and afterwards I had relied on translated Cold War material from the Foreign Broadcast Information Service. That's the open-source enterprise that the intelligence community made available publicly. It's now all closed. So, U.S. government not providing public translations of documents writ large, that was one, you know, discovery that was frustrating. The second is how little publicly available information translated for Mandarin there exists, major documents. None of the science of military strategies. These are momentous Chinese documents. They are not publicly available in English in the U.S. on Web services. So, I actually had to get a lot of information translated. In fact, just the lack of information translated from Mandarin to English, it's so bad that CSIS, as part of a major effort which I think we're going to make publicly available in November of this year, 2021, is an open-source China analysis center so that we are translating, you know, substantial amounts of Chinese documents. And you know, the purpose is that it's not pro- or anti-China; it's more just to understand what is going on inside of China. I mean, I think eventually it will include key debates going on digital platforms inside of China, as well as journal articles, media, government documents. Even on government documents, what I noticed is – in the translations is when the Chinese – you know, they may actually translate a white paper into English, but what you find pretty quickly is that their translations are designed entirely for their audiences. So, they may have a white paper in Mandarin largely designed for a Chinese-speaking audience. The English version, which is designed for a different audience, actually is different in many ways. The phrases are different. It's a lot less aggressive in talking about the United States. So that just – that whole process of translating Chinese documents to me was a huge epiphany on how far behind we are on understanding what is going on

inside of China. I mean, the easiest way to classify a Chinese document is to keep it in Mandarin because nobody in the U.S. can speak – can speak Mandarin. I mean, I say that a little bit of tongue-in-cheek, but there is definitely some truth to it. So that was – that was actually one of the more interesting findings from the book, is how much we had to translate from Chinese.

Ms. Harding: Right.

Mr. Sanger: The only thing I'd add to that is on the one hand it's terrible that the U.S. is not putting more of this stuff out, you know, and the good news is there's a lot of technological solution to this of automated translation. It's not perfect, but you know, we'll make up for the high labor cost of doing this. The good news about all of this – and I know sometimes, Emily, this can drive people crazy in the intelligence world – is that there's a huge amount more open source available for us to go follow our adversaries, right? I get every few weeks satellite photographs of North Korea which we can hand off to, you know, outside experts that give us sub-meter view of the major nuclear facilities and people can come to judgments. You know, a decade ago, you know, that was only available through highly classified systems. So when President Trump was declaring after his meetings with Kim Jong-un that he had had phenomenal success in getting them to stop their nuclear program, we were able to go out and write stories that established that, no, they were building new bases; there was activity in Yongbyon, the main nuclear site; you could see when they turned on and off the reactor because of thermal heat slides and all that kind of stuff. And this is highly frustrating to people in the intelligence community who were accustomed for a while to a monopoly on this data, but it's a wonderful thing for bringing people into an awareness of the degree to which this is a constant – a constant struggle back and forth. And it at times, I think, is fairly useful even to the U.S. government because something that is classified at their end can still get some public discussion.

Dr. Jones: So, David, just to highlight that point, how did I even for this book get information on Russian private military company Wagner Group activity in Africa? Well, we conducted satellite-imagery analysis – commercial, off-the-shelf satellite-imagery analysis – of found Wagner Group bases in Burango Central African Republic. Could do analysis of ranges there, the airports that they were flying into. You could look at the classrooms, the buildings, the infrastructure. Same thing on the Iranian side, could look at satellite-imagery analysis of IRGC – Islamic Revolutionary Guard Quds Force – training facilities outside of Tehran or along the Lebanese-Syrian border and actually see the ranges on there, see where they're exploding ordnance. I mean, it's a wonderful capability. But again, the U.S. is not in – government is not in the position it was or hasn't made the decision on open source to provide some of that information the way it did during the Cold War. But the private sector has definitely – has definitely kept pace, and I think this is where we had to go for the research on the book. And David's exactly right.

Mr. Sanger: I'd give one other example, again, that's been a bit uncomfortable for the U.S. government. You will remember the strike – the drone strike a few weeks ago on the car that was allegedly heading for a second strike on the Baghdad – I'm sorry, on the airport on Kabul, and our –

Dr. Jones: It just feels like Baghdad. It feels like Baghdad.

Mr. Sanger: Inaudible.) Sorry about that. And we published out of our video investigations unit last Friday a reconstruction – a devastating reconstruction of the activity of the main target of that attack, which ended up killing a lot of kids and so forth, that strongly suggests that the activity that from satellites looked to the U.S. like he was gathering explosives was, in fact, him going around gathering fuel for his family and for his activity as an aid worker. And then we went back biographically and discovered he had had 10 to 15 years of work in aid work and certainly did not look like a classic terrorist to all who knew him. And this has caused a real issue inside the Pentagon because it has raised new questions about whether or not, in our last act in Afghanistan, we ended up using a drone to strike the wrong target. And you know, 5 or 10 years ago it would not have been possible for a journalistic enterprise, even one with the reach of The New York Times, to go out and in a matter of days pick a part the U.S. government's rationale for a drone strike.

Ms. Harding: Well, so, Seth, I will turn to you for the last word on that in just a second, but I do think that it's important to note that the commercial enterprise is going to be the future of the intelligence community. A little competition now and then is a very good thing, and then in addition there's just things that only the intelligence community can do and then there are things that the commercial sector is phenomenal at. I mean, companies like HawkEye 360 or SpaceX or a lot of these other firms that are coming up with really brilliant ways to attack some of the same problems, it's insane for us to not be working together. We could do an entire separate discussion about the ways that the U.S. government needs to reform itself to make that really happen, but it's something that has to happen. Yeah, David, go ahead.

Mr. Sanger: We should do that. (Laughs.)

Ms. Harding: We should do that. We should do that. So, Seth, in the minute we have left before you and I actually have to head off to test some of these theories in a tabletop exercise, do you want to say anything about the book and about your recommendation on building on America's core principles and that being one way to push back on this kind of behavior? We talk a lot about the mismatch between America being an open society and some of these countries being highly authoritarian, being able to marshal state resources just by snapping their fingers, whereas, you know, we on the other hand have a kind of bright line between the commercial sector and the

government sector and the public and the private. When you think about marshalling our core values as a nation, what does that really say to you?

Dr. Jones: Well, I think at the end of the day the U.S. and Western, open, democratic societies, I mean, are very competitive. And people around the globe, when we've gone through waves along these lines, they – our values, our economic systems are attractive. And so, I think that in looking forward the U.S. has to continue to operate based on its core principles – its democratic system; its commitment to freedom of information, freedom of the press, freedom of religion – and that actually is its strength. I mean, you know, one of the things that's interesting – I looked a little bit at this in the book, but if you look at how countries responded to COVID-19, I mean, what was interesting about the U.S. response was that the private sector led the way in the vaccines and that when it came to the effectiveness of those vaccines they were – you know, they ended up standing the test of time, at least so far, including the exports of them. And this is an area that has probably been understudied, but where the Chinese have definitely struggled, and the Chinese vaccines have definitely struggled. It's the innovation that comes from an open, effective, competitive economic system that the U.S. has. And I think, you know, this, on the – to shift to the political side, this is also an advantage to the U.S., and it was an advantage during the Cold War. I mean, the Soviet Union in the 1960s and '70s and even very early '80s, I mean, it was an imposing force. We saw Marxist-Leninism take hold across the globe in Africa, in Latin America. But at the end of the day, when you start to close off sources of information, when you make it impossible for individuals to choose their own leaders whether they're good or bad, you know, people get frustrated over time. So, I think, at the end of the day, it's – I mean, I expect the Chinese over time are going to struggle to keep up with U.S. competitiveness and innovation. Silicon Valley remains a dominant competitive industry. And I think, again, COVID-19 was one good example of that. In addition, I think the Chinese are going to have problems in Hong Kong. They're going to have problems in Xinjiang. They're going to have problems in and around Tibet. And I think this is what happens at the end of the day when you try to close off society, when you don't – when things go poorly, and you have an authoritarian regime. And again, this is – you know, it's interesting to see how Solidarity emerges in the 1980s as a strong force as the Polish economy starts to collapse over the course – and you know, interesting – and I'm not saying that the U.S. should conduct this kind of activity – but it was also one of the most successful covert action programs of the CIA during the entire Cold War to keep Solidarity alive. This was not providing weapons, bullets to Solidarity. It was printer cartridges. So, I mean, that's kind of the part of competition that I think, you know, that I'll be looking at over the next decade or two.

Ms. Harding: Great. And with that, we are a little bit over so we're going to end. I want to give a shout-out, though, to our colleague Bonny Lin. You say that's an understudied question about Chinese medical diplomacy. She and her colleagues are looking at this question and I think are going to have something out in the next few months, so we're all excited to see that. I want to thank David Sanger for joining us today and I want to thank Seth, too, for

his book, “Three Dangerous Men.” Highly recommend. Like I said, it’s a very serious topic but also highly approachable and I really enjoyed reading it. So, thank you, gentlemen, and I hope to talk to you again soon.

Mr. Sanger: Thank you.

Dr. Jones: Thank you.

(END)