Assessing The China-Russia Threat Nexus in Technology and Information Warfare

January 22, 2026
Featuring David Shedd and Ivana Stradner
Moderated by Craig Singleton
Introductory remarks by The Hon. William Evanina

EVANINA: Welcome and thank you for joining us at today's event hosted by the Foundation for Defense of Democracies. I'm Bill Evanina.

China and Russia continue to deploy sophisticated information operations and systematic technology theft to undermine U.S. national security, reshape global norms, influence public opinion across the West. Both regimes have spent decades stealing American intellectual property, trade secrets, and advanced technology, all in an effort to support both military and civilian ecosystems. And now, they are weaponizing artificial intelligence and the emergency – I'm sorry – the energy dependency which goes along with it to accelerate their espionage and influence operations.

A bit more on China. China is the most sophisticated, complex, and persistent threat the United States has ever faced. It is an existential threat which transcends our national security, economic dominance, and stability, our global leadership, and every pillar of our democracy and capitalism. The impact is undeniable and is felt from Wall Street to the cornfields of the Midwest, through our universities, and has permeated every fabric of American society.

Back in 2011, the FBI, the Department of Justice indicted five members of the Chinese People's Liberation of Army – People's Liberation Army. They arrested them for economic espionage against U.S. companies, numerous companies. It was the first such criminal indictment of its kind and the first such indictment which named U.S. companies as victims.

The global ramifications were immediate. Over the past decade since that indictment, there have been hundreds of similar indictments with thousands of victim companies, universities, and research institutions. The estimates have ranged from $400 billion to $600 billion dollars per year in economic loss just from the theft of intellectual property and trade secrets and just from the Communist Party of China. This equates to approximately $4,000 of economic loss to the – every American family of four after taxes. The cost of China's industrial espionage campaign is real and is felt across the entire American landscape.

Secretary Rubio, when he was chair of the Senate Select Committee on Intelligence, said that it is the largest and most sophisticated theft of intellectual property in the history of mankind, and it just happened in one decade. Additionally, over the past decade, we have seen both Russia and China becoming even more brazen with cyber breaches, insiders, and utilization of non-traditional collectors. One needs to look no further than the recently-identified Volt and Salt Typhoon malware deployment onto our critical infrastructure, which depicts a mosaic of nefarious strategic intent and vicious capability.

I have said for more than a decade that the threat posed by China and Russia will require a whole-of-society approach to defend against. And while- what do I mean by this? I mean defensive efforts not just from our national security apparatus and law enforcement but including the education of board rooms, business schools, corporate leadership, and at every American university and college campus, as well as elected officials in the United States.

In closing, Beijing and Moscow's espionage and influence campaigns expand and evolve, especially with technology proliferation. The U.S. and its allies must keep pace. We must understand their methods, and more importantly, their intent. What is the intent of these authoritarian regimes which are resulting in real world consequences and impact? The why matters, and we are all a vital part of the solution.

So OK, to discuss all this and more, we have – join an expert lineup today.

Please join me in welcoming, to my right, David Shedd, former acting director of the Defense Intelligence Agency. For over 30 years, until his retirement from government in 2015, he's been a seminal part of defending our nation. He recently co-authored the newly published Harper Collins book "The Great Heist: China's Epic Campaign to Steal America's Secrets," which will be available for purchase immediately following this panel.

Ivana Stradner serves as research fellow with FDD's Barish Center for Media Integrity. She studies Russia's security strategies and military doctrines to understand how Russia uses information operations for strategic communications. She also serves as a special correspondent for the *Kyiv Post*.

Moderating today's conversation is Craig Singleton, senior director of FDD's China Program. Craig spent more than a decade serving at a series of sensitive national security roles with the U.S. government, where he primarily focused on East Asia.

Before we dive in, a few words about FDD. For almost 25 years, FDD has operated as a fiercely independent, non-partisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, FDD does not accept foreign government funding.

Craig, over to you, buddy.

SINGLETON: Bill, thank you so much for those opening remarks and for being here today. You have done more than almost anyone to bring these issues to light, out of the SCIF, and into public view. So, we really are grateful for you being here today.

David, it's wonderful to see you, as always. Let's dive right in. First, congratulations on "The Great Heist" co-authored with Andrew Badger, who was unfortunately unable to be here today.

I want to dive right in, big picture. It feels like every day, there is a drip, drip, drip of new revelations about Chinese espionage; a new human recruitment, an issue you and I are both very familiar with; a new cyberattack – Salt Typhoon, Volt Typhoon, whatever the next Typhoon is going to be.

How serious, in your view, is this China espionage threat against the United States today? And what do you think most Americans still misunderstand about the threat?

SHEDD: Well, I'm delighted to be here today, and I thank FDD; Bill, for your opening remarks. It really, in large measure, contextualized the question, Craig, that you're asking.

It is by and far the largest illicit wealth transfer in history, when you look at former Director Wray's estimates in terms of what was publicly shared, of somewhere upwards of that $600 billion annually, $700 billion, and that's probably understated because a number of companies either don't report it or it goes – it's – it – that intellectual property is stolen in a stealthy manner and we don't even know it – that it's been taken.

I go back to, as an intelligence officer – and I always would ask the question, what's the context? Understanding the context of what China is presently doing and has been doing for a number of decades now takes me back to a mid-1984 speech with Deng Xiaoping in which Deng Xiaoping really laid out for his successors in Jiang Zemin and others, and now post-2013 for Xi Jinping, a qualification or a rubric in which China would pursue the co-existence of a socialist state – I would call it communist, Marxist single-party state, in terms of the Chinese Communist Party – alongside managed capitalism. For those who have a background at all in China, if you've visited China in the '80s – and I might be dating some people in the room – '80s and '90s there were the knock-off piracy products out on the sidewalks and that sort of thing. That was the beginning of, really, the manifestation of it.

By the time Xi Jinping, now fast forward, comes to power and sort of consolidates his power in the 2013 period, there is the launch of “Made In China 2025” in 2015, a 10-year plan in where us old types of the Intelligence Community would say, would say the requirements were laid out, and then those requirements – he was going to primarily – not exclusively, but certainly primarily, use the Ministry of State Security [MSS], which has doubled in size since Xi's period to an estimated 300,000 today – which, for your audience, the MSS is the CIA/FBI. So, foreign and domestic security and intelligence, along with the National Security Agency capabilities; Cyber Command; geospatial, in the case of NGA; and all under one roof in these 18 bureaus or departments, of which Bureau 18 focuses on the United States. It’s important to get that context in mind in terms of the size and the dependency of the CCP and Xi Jinping and the leadership position that he has in driving this.

So now really to your question, now we have the context. The context is Xi is determined, as is his CCP, to come out of the century of humiliation...

SINGLETON: Right.

SHEDD: ... an era or a period of time in which China would – and I don't mean to put words in Xi's mouth, but in an essence, he would be saying, “We were weak when the international order was put in place – Bretton-Woods and all the other aspects of the international order after World War II, post-1945 – and you put these rules in place to dominate us.” The great rejuvenation – “make China great again” might actually be a phrase you might think about – is then the counter-response to it.

And it's so interesting, having worked the Chinese target for many, many years, it was evident to me that the idea of what we would call stealing our intellectual property, our data, our know how, and expertise that goes with it as well is not seen as stealing. It's actually making a course correction to the oppressive West, particularly the United States, in response to that. The magnitude has only increased in terms of the dangers in the presence of the CCP, through the MSS in their operations, and we may get into the Typhoons, as you said. The sophistication today of the MSS versus the MSS that I worked in the '90s in that period of time in particular is dramatically different. It is perhaps the best first-rate intelligence security service in the world today at what it does. That's how serious the threat is.

SINGLETON: Yeah. That context is so important, and in Chinese bureaucracy, form usually follows function.

SHEDD: Right.

SINGLETON: I'm always reminded of something actually Bill taught me many years ago. The “rob, replicate, replace.”

SHEDD: Yes.

SINGLETON: I love – we're at a think tank, so anything with alliteration we glom onto here. But that's an easy one, right, for policymakers to understand as we're sort of talking about this.

SHEDD: Yeah. The “capture, cage, and then kill.”

SINGLETON: That's even better.

SHEDD: There's the image.

SINGLETON: I think we'll have to –

SHEDD: And I develop that in the book in terms of how that's done.

(LAUGHER)

SINGLETON: That's exactly right. I'm thinking a little bit now as you describe the form and the function, the targets. Right? You mentioned intelligence requirements. You triggered me a little bit. I thought you're going to be like NIPF [National Intelligence Priorities Framework] or something. We're going to go into our old world. But as I think about it a little bit, they're going after certain targets to get the information. We talk about universities; we talk about businesses. They're in our critical infrastructure, obviously. Our defense industrial base, huge part of this.

I'm curious, do you think there's a most underappreciated target from that list or something I haven't mentioned yet? As the Chinese are starting to think about what they need from us and where they want to be positioned on our networks.

SHEDD: It's fascinating to me that like any good intelligence collection plan and apparatus that supports that plan, in this case the MSS, as they collect the data, they are actually quite agile at shifting their requirements because they're identifying, for example, our research on quantum. Where's quantum going in the Shanghai Institute in terms of quantum in Shanghai? You know what would keep me up awake – keeps me up at night is this whole idea of a surprise breakout on quantum, as an example.

The other thing is, Craig, is I think we are under the misunderstanding, or the erroneous impression, that when they did their hypersonics test in August of 2021, as one example, that somehow, they stole a hypersonic vehicle or a hypersonic capability all wrapped up with a bow. The under emphasis and where we don't fully look is that in fact somewhere on the upper ends of 170 to 180 Chinese scientists were doing co-research in the cradle of the Manhattan program at Los Alamos 70, 80 years ago.

On what? Wind tunneling and all sorts of other aspects that are – were the major contributor, or certainly a significant contributor, to the fact that their hypersonics has been advanced to where it has. My point is, is that when you ask where is it, maybe underappreciated, undervalued in terms of Bill's background and the counterintelligence, is that they take piece parts; they then bring them together. The corollary to that is they're happy to work with a huge net in terms of what they collect. In other words, they may need it.

It doesn't mean that everything – and it's a whole of society Chinese approach to doing this. And because of the National Security and National Intelligence Law of 2017, Article VII – look it up – every Chinese citizen and every Chinese entity today, when called upon to support the CCP, must. There is no – there is no loose language, “may,” “perhaps,” “should,” or anything like that, in terms of doing it.

Am I ever suggesting that 280,000 Chinese students in the United States are all spies? That's not what I'm saying at all. But when called upon, and we might talk about ByteDance and TikTok, they will, as a quasi-independent company, be called upon to support. I think that's where we miss a little bit of the linkage between what their requirements are and how they're meeting those.

SINGLETON: Yeah, it's a great point. The legal and regulatory scaffolding that Xi Jinping is established and codified into law. It's – it can be coercion, it can be cooperation, but it has to happen and there's no choice. You – the name of the book is “The Great Heist.” So, we've talked a little bit about the structures that they're using to get the information. We'll get into some of the tactics that they're using and then we're seeing this evolution.

What are they trying to steal? What's the great heist? How did you come up with the title? What do you think is the big – is it one thing they're trying to steal? What is it? How do they – how do they think about it?

SHEDD: The backdrop to the title comes from essentially, like some in the room perhaps, certainly some in the audience, that had their security dossiers taken in May of 2015 from the Office of Personnel and Management, as I like to say, 22.5 million of my best friends of the past and present at that time had their security dossiers taken. So, my motivation on the heist and title came from a very personal experience. And subsequently we had the 170 million documents taken from Equifax and Anthem Health and many others. So, we'll talk a little more perhaps about the data piece of it.

SINGLETON: Yes.

SHEDD: And so, the heist is this blend of the Chinese focus not only on the technology, both cutting edge and futuristic, but also in acquiring through programs that they've rebranded, which in 2019 was the Thousand Talents Program, but essentially going on university campuses and finding them, in our national laboratories and in the research and develop world with the data. And so, it's this – I always often said when I was at CIA, I would have stood up a separate freestanding division if I had gotten those OPM records, because all I need is to find the vulnerabilities in .001% for my targets. So, imagine that.

So, the heist is really as broad as anything that isn't, as one pundit said to me, they'll steal the buttons off your shirt if they need to. And in many ways, all kidding aside, there is no limit to it, and as I said, the proverbial net that they will capture this information whether they need it now or not. Very different than our history with the intelligence community. If it wasn't a requirement, you walked away from it.

The second aspect, and I want to underscore this, and Bill you alluded to it in your opening comments. It's that China is, in their whole of society, is applying intelligence to their economic, military, industrial base, the PLA, the People's Liberation Army's modernization, space programs, underwater, and all the rest. In the sense that everything's a requirement then. So, that's really where the great heist, and that's the epic campaign. And these are about campaigns as again we'll mention the Typhoons. They're not single events, and that's where it comes from.

SINGLETON: Yeah, it's a great point, right? Chairman Xi Jinping says that data is the 21st century oil.

SHEDD: Exactly.

SINGLETON: Right. And there's – I'm curious though, why do you think that they are so fixated on the data? What do you – what do they think they can do that we can't see or understand?

But it is to your point, we usually say we have to prioritize in the intelligence community. We have to have a list of requirements. If it's nonpublic information, it's one thing. If it's publicly available, this is not for us. They have a very different structure and function. But this obsession on data, this fixation, I would think about it. Why are they so fixated on collecting it and what do they think that they can do with it that others simply can't?

SHEDD: Briefly, three points. First is they're going to be building or are already building, more and more sophisticated large language models with the data.

SINGLETON: Yeah.

SHEDD: So, that the AI – and the battle at present and in the immediate over the horizon is artificial intelligence. And so, we know that. Secondly, they mine the data even when they don't know what they've collected in terms of its value for applicability to something that will be either used in their version of deterrence in countering the United States and the West, economically or militarily, but also to go on offense for it. They will have knowledge. Data is power in terms of having it.

And thirdly, there's an element of CCP control then. What I have by way of my data storage and what's in there gives me a certain power. I may not know how to use it precisely today, but I have something on you that you don't know that I have. Or if you know that I have it, you can't do anything about it. And I will go out on a limb. Every adult American has had their data already taken in some form or another, not because you did anything wrong, but precisely because they're obsessed with the collection of data. Even if they don't have a “right here and now” moment application for that data.

SINGLETON: Yeah, no, it's a great point. I mean, it's down to the personal level with genomic data.

SHEDD: Exactly.

SINGLETON: Our genomic data sets that they're collecting and then –

SHEDD: For DNA purposes, for their microbiology –

SINGLETON: – advanced biologics, specialized medicines.

SHEDD: Yes.

SINGLETON: Building that supply chain centrality. Build the data, apply big data capability to it, have breakthrough. I'm curious. It's always fun to play a little spy on spy analysis, because it's like respect meets respect, right? Was there a case study or an example from the book that you looked at and you said, "that is truly impressive"? Like one that really blew you away, maybe one that we – you don't think maybe we would pull off naturally, but they have developed these skills and capabilities.

I'm just curious. You have so many great examples in the book. I encourage folks to read it. It's a little scary when you read it. But is there an example where you said, wow, that's so impressive?

SHEDD: Digging little holes in the Iowa fields to take out Monsanto seeds, I sort of scratched my head, what in the world? But as a student of China, when you think back in the Mao Cultural Revolution and the Great Famine, all of a sudden it makes sense.

Remember, the century of humiliation is countered by what you go and do. And so, you have these, I don't know how many, of you know Iowa, but to go out there digging seeds out of it would not be my first choice of something I'd be interested in doing. And I just said, wow they one, will stop at nothing. And two, it's clear there was some form in some manner, a requirement put out there to go after these advanced seeds, which by the way, is millions and millions of dollars associated with the research and development associated. So, there's that kind of operation.

Another one is Tesla in 2019. Elon Musk inks the deal in the summer of 2018. And well, there's groundbreaking Mr. Cao, back in the United States as an employee is thumb-driving the download of about a billion dollars in source code to autopilot. It's in every BYD today. So, you have sort of these – sort of extremes. And when you – the panoply of the attacks or capabilities of collection just leave you stunned in telling these stories, because all of a sudden you have Intel on Intel, as you say, the arc of the story.

SINGLETON: Yeah.

SHEDD: And that's really what's – that's what stands out to me.

SINGLETON: Yeah. It's a great point. The food security is national security for the Chinese Communist Party. And if you understand the historical roots of the party and its development, you understand why it's so prioritized.

Ivana, I want to bring you into the conversation because I don't think we can talk about Chinese theft without talking about its no limits partner in Moscow, which is a topic of your research here at FDD.

When we look at Russia's acquisition of this technology, illicitly, sometimes above board as well, I'm just curious, where does Moscow prioritize its efforts here? And where do you think the U.S. is most exposed when it comes to the Russian target?

STRADNER: So, first of all, thank you, FDD, for organizing this event. Thank you, Bill, for your opening remarks. And as David emphasized, really, context matters. And humiliation just for China, that's exactly how Russia also thinks about the 20th century. As a matter of fact, Putin openly stated that the greatest catastrophe of the 20th century was the collapse of the Soviet Union.

So, before diving into tiny details, I'd like to zoom out why it matters, because Russia has been trying to compete with the United States on so many fronts, and Putin has promised probably himself that he wants to put Russia back on track as a great power.

But one thing is Russia's wishes; second thing is what they can do. But while reading your book, I was – first of all, it's really terrified what's going on there in China. But it's so interesting how Russia fits into this picture as China's junior partner, because their methods and their targets are sometimes very similar.

So, my favorite example when it comes to universities, which is Russia's favorite game. Putin, as a KGB guy operating below the threshold of war, was also their cooperation with universities. And a lot of people in the West thought that Russia would be able to go back on the trajectory of the West. And why not to trust them? So, almost 15 years ago, actually, a Russian oligarch was in a partnership with MIT, trying to build a Russian Silicon Valley. And back then, why not? That's a great opportunity for the West to actually build partnership with Russia when it comes to new technologies. Luckily, the FBI immediately started warning about how different private companies can leverage that. So, that's really nothing new.

Second thing, I love to read the Cold War history. And all you really need to know, to do is to go on the CIA website and actually to read all documents how the Soviet Union was stealing American technology.

And why it matters today? Well, it matters because very little things have changed other than Russian methods when it comes to digital things, which brings me to the next point on how Russia has been leveraging cyber. There were numerous attacks on the U.S. critical infrastructure, how Russia has been trying to steal data, access to our financial system. So, this is also nothing new.

But the third pillar, which is really interesting related to Russia's war in Ukraine, how come that still Russian weapons are operating, thanks to Western chips, semiconductors? That's something that I really want to know. And the easiest answer is because Russia has been leveraging third parties and different legal loopholes to accomplish that.

And there was a famous 2022 case when the DOJ actually exposed a Russian acquisition of certain military technology. And as everyone is nowadays focusing on what's happening with Greenland, that's another fourth pillar that is really interesting to observe how actually Western technology also ended up in a Russian advanced naval system.

But again, the big question is why? Because Russia has been trying to compete with the United States. Second thing is Russia needs Western technology for Russia's war in Ukraine. And the third thing is the Russian government doesn't even hide that. They openly talk that they are very much reliant on Western technology.

So, it's really past time to also look at Russia's threat when it comes to this because this can truly undermine our national security, but also national security of our partners who rely on our innovation.

SINGLETON: Yeah, I think that context is so key. The Cold War context, in particular, just like we talk about the context for how China sees the world and sees the United States. I always say, if it ain't broke, don't fix it. So, obviously a lot of these Cold War era tactics, clandestine operations, using cutouts, they continue to employ them because they work.

STRADNER: It worked.

SINGLETON: If it didn't work, they would – they would try to break it.

STRADNER: Correct.

SINGLETON: Right. And I think that's just something we have to recognize that the Cold War ended for us, but not for them.

You can't throw a stone in this town without hitting someone talking about AI. We've got to talk about AI. We do a lot of research at FDD on AI and what it means for the emerging threat landscape and cutting off China from advanced chips and what does it all mean?

We don't hear Russia in that conversation as much. We're talking about DeepSeek. We're not talking about the Russian competitor. I'm curious, how is Russia thinking in leveraging AI for strategic competition? Is it just propaganda disinformation? Is it cyber operations and intelligence? What's the Russia side of that conversation?

STRADNER: So, we don't hear much about Russia probably because Russia is a second-rate AI power. But more importantly, almost a decade ago, Putin actually stated that who leads AI will rule the world. And the real question is, how come that we are in 2026 and Russia is far behind the United States and China?

There are numerous explanations for that. But in large part, there is also the issue of Russian full-scale invasion and sanctions, and the limitations of partnerships, right, with the West. Because that has been one of the key components how you can grow in AI.

But there are two things that I want to emphasize, something that is very interesting we were talking about Russia and AI. Just a few months ago, Putin gave another speech and erections on Russian trajectory when it comes to AI. And he emphasized two important things.

Number one, that Russia absolutely needs to divorce itself from Western AI. And the second thing is where Putin emphasized the role of, the role of ideology. And I understand it for a lot of people in the West who love to talk about nitty-gritty details when it comes to AI and tech, I think this is very important because, just think about Russia has been developing something is called AI sovereignty, which means – and China also believes in that – that they want to build a system where actually Russia can control, you know, their own information space when it comes to AI. And they have been building numerous blocks to do that.

It's a similar thing when it comes to why they banned Western social media, because Putin firmly believes that the collapse of the Soviet Union was because of, in large part, American influence operations. And, frankly, he is not wrong on that. And that's precisely the lesson that he learned, why he wants to know completely control the AI system.

But here is another caveat over there. The way that they're also building their internal models for AI, divorcing themselves, you know, from Western models is very much based on Russian history, Russian far-right narratives, Russian narratives related to a war in Ukraine, et cetera, et cetera. So, they have been leveraging that thing extensively. While at the same time, Russia has been leveraging AI in the West. So, for example, this is, again, nothing new because we already saw Zelenskyy's deepfake video where he allegedly was trying to convince Ukrainians to give up on the war in Ukraine.

And I can name numerous other examples, but we love to focus way too much on AI that it's going to completely change the trajectory of influence operations. I don't think that that's completely true because it's just another new technology, just like during the Cold War, you know.

There was everything in a paper, then social media, and this is the third pillar. But I think it's really worth understanding how the Russian military understands AI from a very different perspective than we do – or when I read your book also in China, because it's not purely about technology, it's also about their ideology.

SINGLETON: Absolutely, right. Two authoritarian regimes who are focused on control.

STRADNER: Correct.

SINGLETON: Like regime longevity and stability. The challenge for them as they grapple with AI is it's unpredictable. How much can you control the output from the AI model? We see it in the China space a lot where you can put things in about Tiananmen or the regime. And you can see it almost self-correcting in real time when you play with the models. And I think there's a deep-seated fear in Beijing, but I would imagine in Moscow, too.

STRADNER: Absolutely.

SINGLETON: That, can they actually control these models? Which I think ultimately will keep them second and third place for a while. But I want to get a little bit into now connecting these dots. Technology is the tool for them. They want to accomplish broader objectives I would imagine. They're not doing this for nothing. They have strategic objectives, narrative control, propaganda. You guys have written about this a lot. Some excellent articles in Foreign Affairs. We have some copies out front. It's great reading.

David, I want to start with you a little bit. Why is China using espionage and emerging technologies? How are they doing it to shape outcomes? What is the end state that they are seeking here? They're not doing it for nothing. So, what's the goal?

SHEDD: China's goal unequivocally is to surpass the United States and dominate, in the first order, it's near abroad. Taiwan, 110 miles off of Fujian Province, is clearly in Xi Jinping's sites for as he stated 2027. And the technology that they are seeking in the modernization, that I referenced earlier, of the People's Liberation Army and then the production that goes with it, of course in terms of capabilities, is such that their objective is if there is a bellicose engagement – that's a very diplomatic term about a Taiwan invasion – that they can win and they can win decisively.

SINGLETON: Right.

SHEDD: So, that is sort of priority number one. If you go to their military industrial complex, if you use that terminology. Their other objective is, you've seen when China joined the World Trade Organization in December of 2001, which was a bipartisan objective of our political side, whether it was the Clinton administration driving that to it. And it's addressed in foreshadowings in the book in terms of the complete stand down on any operations that could jeopardize that. And then George W. Bush and the administration that I served in, in the NSC staff, very much committed to believing that you could change China's behavior through the WTO as a result of them then having to play by the international rules. Most favored nation status actually gave them the ability to get market access to do what we're seeing today.

And so, the foothold really goes back 26 years, 25 years ago, with that expectation. The other expectation that the United States had, and I believe it was bipartisan from the standpoint of the people that I was talking to then, was that it would lead to democracy in some form, maybe not Jeffersonian, but somewhere along that spectrum of an opening. And of course, we see that completely moving in the other direction. And Ivana mentioned it. And what is it? It's about the preservation of the CCP.

And so, if you take the last three weeks of what's occurred in Iran, three to four weeks, in terms of the protests and all of that, the thing that keeps Xi Jinping really focused on security is the domestic situation. June 1989 in Tiananmen Square was an event that he does not want to see reoccurring. And so, the espionage machinery, with this collusion of domestic and intelligence, we would call it "positive intelligence collection", versus the protection piece of it is a behemoth that controls then the domestic population and at the same time is seeking to create that decision advantage in the event of an armed conflict with the United States.

SINGLETON: Yeah, the Iran context is so important because it's impossible to divorce the CCP's domestic aims from its foreign aims, right?

SHEDD: You cannot do that.

SINGLETON: You can't do it. And I think in the Iran context in particular, it is Chinese technology, including CCTV cameras, that are being used in Iran today to track protesters down to their door.

SHEDD: Exactly.

SINGLETON: Shocking, and we just haven't done enough on this as a target. But it's built on domestic CCTV cameras and a lot of U.S. stolen technology. I think the Taiwan part is so important too. The Chinese are hoping to – they're preparing for a war they hope to never fight and they're doing that through capability development which the book explains beautifully. But they're also, there's a cognitive warfare component to it as well where they're saying resistance is futile.

SHEDD: Yes.

SINGLETON: "We're so big, we're so powerful, this is going to happen." Russia plays in the information warfare space too. They're thinking about this as well. Both – you mentioned in your remarks, capability development. But they're also thinking a lot about information warfare. I'm curious, what's Russia's goal here? What's their outcome in all of this?

STRADNER: So, when we're talking about Russian information warfare, I always like to cite how Russian military thinks. They believe that who has information superiority is going to win this war. And they value 4:1 non-kinetic to kinetic efforts. All you really need to know, is to just go and take a look at how much money Russian spends on information warfare. How much (inaudible) – it gains money. I think last year it was 1.5 billion. So, and why it matters, as I mentioned, context again matters because let's call a spade a spade. United States during the Cold War, we were the superpower when it comes to information warfare, were unapologetically using a very powerful tool to win the Cold War, to win hearts and minds.

And as soon as Putin came to power, he started strengthening domestic information system, completely trying to close it down. As a matter of fact, Russia just announced that this year they are going to ban officially on WhatsApp, let alone other social media. So, Russia has developed a very powerful tool, not only to strengthen domestic information system but also to put the West on the defensive. And as an authoritarian country, Russia doesn't have to use any ethics so they can spread lies, they can spread propaganda, they can leverage social media influencers. You can go on and on. But the most important thing is really to understand that this is a very serious weapon.

For many people, this is a weapon that you cannot see, you cannot touch, you cannot feel. But it's really powerful enough that it can destabilize countries. And I think it's very important, two things. Number one, to understand how Russian command and control works in this environment. Because, with all due respect, the world doesn't revolve around Brussels or Washington. And we always like to think that American adversaries think like us, process information like us.

SINGLETON: "Strategic narcissism" is what H.R. McMaster calls it.

STRADNER: Exactly, exactly. And the second thing is, in the United States we shut down a lot of efforts in the information environment, whether we – Global Engagement Center, the Voice of America, and all those places had numerous problems. Let's call a spade a spade. But we still need very, very powerful toolkit actually to put our adversaries on the defensive. So, they spend time managing resources, defending themselves.

And with all due respect, like, I understand that for a lot of – it requires risk tolerance and risk aversion is rewarded in Washington D.C. So, that's another, you know, pillar that we need to figure out if we want to win this war, how to do it. But that's something that really, really Russia has been very good at.

SINGLETON: Yeah. No, that's a great point. I mean, I often think about this no limits partnership less as an alliance, but more an alignment. And it seems to be really rooted in just a mutual grievance and loathing of the United States. I want to hit both sides of that coin then. There's the cooperation side and then there's the skepticism that exists between the two. I want to start with you, Ivana, a little bit. Where do you think you're seeing China and Russia cooperate in this space?

And then we'll pivot, David, to you. Like there is deep skepticism at the working level between China and Russia. Again, long rooted, historical, despite the bromance at the top between the two leaders. I'd love to hear your thoughts, then about where you see maybe China keeping Russia at bay or at arm's length, as they acquire this power and this technology. But we'll start with maybe where they're working together.

STRADNER: So, I think that Russia and China are actually frenemies. They cooperate on one side, but they also fear each other. Especially Russia is not happy with China's developments. And – how to answer your question? I mean, there is so many reports on their cooperation, whether military and tech, whether in cybersecurity, they're publicly available. In 2015, they signed officially Information Security Agreement just last year. Even through BRICS they signed a new AI agreement.

So, I can go on and on listing all those things, but I want to actually zoom out and to explain where they're purely aligned. And I would like to emphasize BRICS. I understand that for a lot of people in the West, BRICS is just another crazy institution, financial, that is going to collapse. Who cares? For Russia and China, it's very important because it's an ideological institution where they're aligning on creating what I like to call a "multipolar world." And they have been doing that, especially in the Global South, quite successfully. So, they have been cooperating on that front in particular.

And every speech that I read by Vladimir Putin or Xi Jinping, they love to talk about the creation of a multipolar world and the end of the U.S. unipolar world. So, when it comes to new technologies, there are so many official bilateral agreements that they signed. But to me, it's even more important that big question where they are ideologically aligned. And that's why I cannot emphasize enough why we should be paying more attention to BRICS.

As matter of fact, as someone who deeply cares about influence operations, they have been also developing something that's called like a BRICS TV, a new effort to launch influence operations in the Global South. And they are perfectly aligned over there. Russia is much better than Russian influence operations, but China is learning and has clearly better technologies.

SINGLETON: Yeah. The world order component of this is key, right? A world order that reflects their values and their interests. They push this multipolar moment. I get the sense that our current president believes quite strongly that it's a unipolar moment and he's going to foot stomp that, I think for the next three years, that's for sure.

But David, pivoting then to the skepticism, this exists – the bromance at the top, but the working levels are deeply concerned. Russians are worried about becoming Chinese vassals. The Chinese wonder, "What's the value proposition from the Russians? They seem behind. The brand is bad globally."

I'm curious, like, where you think the Chinese are maybe keeping them at bay. What does that look like? How do they balance that?

SHEDD: I always like to think of nation states rising and falling to their self-interests. And the self-interest, and Ivana's touched on this, in terms of the junior partners, certainly – that was the implication of Russia to China – of deep concern to Vladimir Putin in that relationship, notwithstanding the appearance at the top, of course, of collaboration. Need you only see the military hardware march in – three months ago or so in Beijing…

SINGLETON: In September, yeah.

SHEDD: ... of doing that. The issue is that there is a long, a much longer history of conflict between the two countries than this – than this aspect. My fear is that both China and Russia see vulnerabilities in the information space as it pertains to the United States, and that's where the cooperation may take place.

You also see it in some very cutting-edge technologies, where almost at a tactical level the drone sector – of the development of the drones is something – and then I think you have to bring in the North Koreans and the Iranians when it comes to this technology.

A little bit of the jingoistic view in the United States has often been that "these people aren't nearly as smart as we are, they certainly don't have the resources to do X, Y, or Z, and they're just second rate." Well, North Korea's attack on Sony showed that in fact, it can do very sophisticated operations in terms of the cyberspace.

SINGLETON: Right.

SHEDD: So, I don't want to go down the path of North Korea and Iran, but I think there's a commonality of an archenemy, which is the United States, where that cooperation would exist.

Going back to my three decades-plus of the intelligence business, I'm not here to say though that the intelligence cooperation at the working level – as you describe it, bureau to bureau or department and department – is one that there is profound trust. There isn't.

And so, intelligence – we used to call them the tear lines, what you would share with the other side in terms of doing that – is the Chinese aren't going to let them in on that, and the Russians likely are going to put up obstacles to that kind of sharing. However, the directional – and I liked the way Ivana describes it in the context of BRICS and sort of the international order piece – I think there's a lot of synergy between the two that can sort of override the distrust that's down below in that.

As the book tells the story, it was in fact advanced aircraft out of the SU [Sukhoi] family of Russian MIGs [Mikoyan-Gurevich] that were stolen by the Chinese. And it is one of the earlier versions of – before they got to the F-35 and the FC-31, which is the cover of the book, by the way. It's a digital twin. I mean – so that's what they created with that.

SINGLETON: Yeah.

SHEDD: Much earlier, they stole it from – and it was the Russian military that never wanted to go into that arrangement, believing, and proven in time to be true, that the Chinese would steal it.

SINGLETON: With friends like China. The other great example recently is submarine-quieting technology.

SHEDD: Exactly.

SINGLETON: And what's interesting about that one is that the Russians provided, reportedly, submarine-quieting technology to the Chinese in the last few years, and the Chinese will probably – they wanted this for a long time, but they were able to ask for it because of Chinese support for the war in Ukraine.

SHEDD: Yeah.

SINGLETON: And so, there's almost a – how much can the Russians hold the line in terms of providing this information, at the same time that we all accept the Chinese are penetrating the Russians? But is there now an imbalance in the relationship, where perhaps the Chinese came to the table and said, "We keep supporting you. It's time for you to hand over what we really need, which is the submarine-quieting technology against the Americans?" And you wonder whether that balance just fosters more grievance and distrust between the two sides. It's going to be fascinating to watch this play out.

You had something else you wanted to add, though?

STRADNER: Yes. I actually wanted to just add one more example, which is – which actually tells you all you need to know, how their cooperation works and how cynical it is. So just take a look at the United Nations in the last year, when the United Nations adopted a new UN cybercrime treaty. Sounds great in theory, right? Like, who doesn't want to have a treaty that can stop cyber criminals? Except for the fact that this treaty was written by Russia and supported by China. And that treaty was, in large part, later on supported by many countries in the West.

So that's very concerning because we in the West, we have legal obligations to follow certain rules. Do you really believe that Russia and China are going to follow those legal obligations? Absolutely not.

And make no mistake, very soon, you will see a new effort coming directly from Russia to regulate information security and hybrid warfare. So, hope we will not repeat the same mistake.

SINGLETON: Yeah. Before we pivot to Q&A – and so if you have questions in the audience, someone will come around with a mic for you. David, we always say at FDD that we come with a headache and the aspirin. We're very focused on solutions. Going to policymakers and just saying, "Here are all of your problems" is frustrating for them usually. And you've been in the Chair and you're like, "What a should we do about it?" It's the prescription.

You lay out seven excellent pillars in the book. I'm sort of curious, if you had five minutes with a policymaker, are there two or three that you'd really highlight? Like, what do we need to do now to cut off and sort of challenge and stymie what China is trying to do?

SHEDD: I think you have to parse it in terms of what areas you want to tackle it, but in the macro sense and that strategic sense, it's really a policy of partial decoupling around what crown jewels you want to protect at all costs.

SINGLETON: Yeah.

SHEDD: And those may be in the six to 10 to 12 areas of where you – where you do that. So that would be sort of number one, in terms of the recommendations.

Secondly, a much stronger public-private relationship in terms of the sectors working together.

SINGLETON: Yeah.

SHEDD: I would like to see a national economic security council stood up in which there would be, as 1947 built the NSC out of that, in terms of the National Security Council that President Truman did, around the ability to bring together both the private sector and the public sector on these issues.

Why? Because this is economic warfare. So, it's going to be – it's going to be different as to what you're going to address than guns and bullets and ballistic missiles, in terms of the threats that you're – which also has to continue in parallel on the traditional national security side.

And finally, I think a Department of Justice, and supported by Bill's former organization, in terms of the bureau, really given additional tools associated with countering the heists from a – area of emphasis. There was a task force set up in Trump one, in terms of the administration and DOJ focused on that. It was dismantled in 2020. It's not returned though either.

SINGLETON: Yeah.

SHEDD: And so, I think that the greater emphasis that addresses the lawfare piece of this on the part of the adversary, in the case of China – by the way, I don't call them competitors. They're adversary, in the – in the context of everything we're talking about – is then being able to give law enforcement and the counter-intelligence people the kind of tools to really go after it.

SINGLETON: Yeah. I love the phrase "crown jewels" because I think the Chinese use similar language. They say they want to control the drivers of the 21st century industrial revolution, and whoever controls them will control the future...

SHEDD: Right.

SINGLETON: ... so AI and quantum, biotech, chips, drones, increasingly robotics.

SHEDD: Exactly.

SINGLETON: These seem to be the areas that we need to start to cordon off.

SHEDD: Exactly.

SINGLETON: We talk a lot about chips in this town, but we need to start thinking about tomorrow. And I think that tomorrow threat, particularly biotech, is where we need to start putting a lot more attention.

We're going to shift to Q&A now. I'm going to ask folks to please raise your hand, state where – your name please, your affiliation. We'll try to get to as many questions as we can.

And we'll start right there, I think. Michael Gordon, *Wall Street Journal.*

GORDON: Thank you. Just a quick question on the China and Russia side. How do you assess Trump administration efforts in countering Chinese and Russian cognitive warfare information operations? Where have they been effective and where may they be dropping the ball?

SHEDD: Yeah. Do you want to start with Russia?

STRADNER: With Russia? Yes, I can.

So, the Trump administration decided to shut down several important platforms that we had to defend ourselves from Russian influence operations, including Global Engagement Center, the Voice of America, et cetera, et cetera. As I mentioned, there were numerous problems over there.

What the United States is doing on the offensive side, I really don't know, but I can tell you if we were doing a better job, we would not have this panel. So that's something that I really worry about because regardless of the administration, for more than a decade, we struggled a lot when it comes to countering cognitive warfare.

And we always like to talk about are we winning or are we losing? So, let's call a spade a spade. We are in an information war with Russia. That's exactly how the Russian military perceives this. What we really need to do is to perceive this as a protracted war, where you can have information superiority on a day one but information – to lose information superiority on a day two.

So, we have to be very patient, and we also need to really develop offensive capabilities but not only develop but to deploy them, because make no mistake, Russia already believes that we are doing that. So, if they believe, maybe we should.

SHEDD: I would characterize a significant difference from the Trump first administration to where it is today, with much more of a present-day sense that everything is negotiable. In other words, that it can be either at the tactical level – I don't know what strategic would look like in this context of your question – but tactical.

In other words, so you'll negotiate TikTok, as an example – and I think there's going to be an announcement very soon in terms of what that deal is – you just have to work with ByteDance, the parent, and you can sort it out in who has what percentage of ownership.

And I think we've concluded TikTok, and you can all sort of land where you wish to on that being a wise decision or not. I believe it's a terrible decision to keep TikTok open – collects on 160 million to 270 million Americans using it, and 1.6 billion worldwide, which obviously we don't control and that data, back to your earlier comments and questions about data. So, I think it's much more tactical and all sort of a business negotiation on it, and I think the Chinese are loving it.

STRADNER: And I think one other quick thing, which is the question of free speech. President Trump is absolutely right that we should be worried about free speech in the United States. But one thing is, when you have adversaries, whether they're working directly with intelligence, sitting in Beijing or Russia, conducting those influence operations, then this is not a question of free speech. It's the question of protecting American national security, because information is a weapon for them.

SHEDD: Did our conversation answer everything? No questions?

BERTEAU: David Berteau, and for the first time in half a century, I represent only myself, which is a delight.

Craig, I want to follow up on your question and your implication about you bring the headache and you also bring the aspirin. And I really want to ask the two panelists, you've talked a lot about what China and Russia are doing. You talked a lot about our response to that, but that response is mostly reaction and defense. It's not offense.

And you know, my history says you don't win. You may prevent losing through defense, but you never win through defense. What does winning look like in this case and how do we get there?

SHEDD: I'll jump on that as a first issue. In the now four decades of association with the intelligence community, we have never really come to terms with economic espionage, both on the requirements side as well as to the distribution then of that information. That is the identification of a sector that would require that information. How do you do it? The French have had a long-standing model of doing that, and the Chinese obviously are doing that as well.

The question for me on going on offense is when and how are we going to have a national debate about this economic warfare when it comes to both the intelligence collection capabilities and requirements? That's the easier part. There will be cultural issues of pushback at that I'm sure of, but it's really then how do you use that?

How do you use it when you have that detection of where the Chinese are going in the AI sector, because you're now collecting on it? And to whom are you passing this to in order to respond to it? That, to me, would be going on offense. And I think it's desperately needed, but we have no public debate on this. And having been with the Select Committee on China yesterday, I can tell you they asked me exactly the same question. I gave them exactly this answer.

The other one is the Typhoons – and we haven't had the time to really unpack the Salt Typhoon, in terms of telecommunication side, and then Volt in terms of our infrastructure – is we have got to be ready to counter that in a material way on the other side.

Obviously, I cross a classified line if even knew what to say about what we are doing or not doing. But I think that's the other aspect of going on offense in cyber – in the cyber domain.

SINGLETON: Before we jump to another question, I want to lean into the Typhoons, because it's so bad that Chinese are still operating on our networks, most–

SHEDD: Actually in 80 countries, by the way.

SINGLETON: Right. Beyond us.

SHEDD: Yes.

SINGLETON: Capture this. We've known about this now since the Biden administration. There – they have the capability means to read text messages, unencrypted text messages, to listen in our phone calls. This is all public. Now it was sort of hidden in the SCIFs, in the shadows. Now it's public. How bad is this? How exposed are we here?

SHEDD: Totally exposed and pervasive. That, I mean, the fact of the most recent story is, of course, on the four or five committees on the Hill...

SINGLETON: Right.

SHEDD: ... in terms of reading, you know, the mail and the email, all the rest. To me, I think our understanding of it, and of course, the nomenclature comes from Microsoft on Typhoons. Would have loved to have thought of that as a code name back when I was in government. It's great run, because it really is – as a Floridian, I would call it big hurricanes, but Typhoons, that's fine.

SINGLETON: Yes. It's more Asian. I like...

SHEDD: Yeah, exactly. It's very, very focused. It really represents the enormity of the threat and it's ongoing. And the ability of our telecommunication companies to really ferret out and clean this up really doesn't appear to be taking place because it is ongoing.

In the infrastructure side, known as the Volt Typhoon, that to me, is the multiplicity of kill switches that are put into it in the event of potential conflict, or for some other reason, rather than predominantly collection.

SINGLETON: Yes.

SHEDD: So that's sort of the distinction between the two, and both are profoundly worrisome.

SINGLETON: Yeah. No, it's absolutely frightening. We know we have some experts actually in the audience who track this closely. So, the Stanford professor in me might start just calling on people. You've been warned.

I want to give another chance to other folks to ask some questions. If not, we have one over here.

SPARRELL: Hi, Duncan Sparrell, speaking for myself, but retired as AT&T's chief security architect, so I'd like to follow up. And I worked in the intel community for a decade back in the '90s.

So, I'd like to follow up a little on the Typhoons in particular and tie them to the Taiwan Strait 2027. And not just telecom, but also, you know, water, electric and everything else. What are practical things we can do in the near future? Because also none – 2027 is just next year.

SHEDD: So, I'll start with my biggest concern is we're completely underinvesting in the cyber/public side of it. And FDD can talk a lot more to that in terms of the concerns that Admiral [Mark] Montgomery and others clearly are tracking here.

And so even to that earlier question about going on offense, what are we doing to counter it in advance of – because knowledge is power. And now the fact that we know that they have these capabilities. And this isn't the C-team, or even the B-team doing it in cybersecurity on the Chinese side, is how are we going to respond to it?

And back to this collaborative relationship with the telecommunications companies and as well as the infrastructure side of it for Volt is we know on – without a shadow of a doubt that capabilities are being manifested inside our systems. So, what are we going to do about it in terms of a public-private partnership? I'm getting the clock message.

SINGLETON: I think we have time for one more question. If not, I'll – oh, here we go.

MULLINAX: Hi, my name is Jim Mullinax. I'm retired State Department. I have a question about how we can better protect ourselves against some of the collaboration that we see ongoing with respect to Chinese and Russian military technology and other things.

Where do you see – I mean, obviously the issue of chips going to Russian military defense production is a crucial one. We know a lot of that goes through China or through other third countries into Russia. Where do you think the emphasis should be in terms of trying to stop that? Is that U.S. government solution? You know, solve problem? Is that something that we need to work more closely with private industry to resolve? And is that something that the U.S. can do by itself?

SHEDD: Yes, no, no, yes, no. Yeah. Yeah, it's a tough one. Starting with the last part of your question, no, we can't do it by ourselves. That's fairly clear to me.

And if you were to talk to Jensen Wong in terms of NVIDIA in the age 200s and beyond, in terms of these qualified chips that they go up the ladder in terms of security. That the idea, and I sort of draw from the Elon Musk story – and this isn't about going after Elon Musk or anything like that – and Tesla was sort of this idea that the Chinese aren't going to reverse engineer it. Or as you suggest in your question, pass it to the Russians and the technology sharing.

I think we have an antiquated export control mechanism in all of this, and an underinvestment in counterintelligence in terms of addressing it. And I think it's a crisis point that we need to address. Because at the heart of it, the AI, and as it goes into quantum, as well as the large language models, the dependency on this, and then Huawei's 10-G or 767, to 10-G as well in ZTE [Zhongxing Telecommunication Equipment Company Limited] are all going to rely on these as well.

And so, there's a – there's I think the requirement for consortium of private-public sector. What are we going to do about it? In answer to your question.

STRADNER: No, no, no thank you…

SHEDD: "I'm not touching that one"?

(LAUGHTER)

SINGLETON: All right. I think it's a great question to end on.

I want to thank everyone today, but especially our panelists for a great conversation. David is going to stick around to sign copies of his book in the back. I recommend – it's the stuff of nightmares. I don't recommend reading it before bed, but maybe during daylight hours, if you want to get smart on this topic. But for more analysis from us, please go to fdd.org.

I want to thank everyone again, and we'll see you soon.

SHEDD: I recommend reading it before your final caffeinated coffee.

SINGLETON: There you go.

SHEDD: Make that your cut off.

SINGLETON: Thank you.