MILKEN INSTITUTE | 2025 GLOBAL CONFERENCE TOWARD A FLOURISHING FUTURE

COMING IN FROM THE COLD: ESPIONAGE IN TODAY'S GEOPOLITICS

Announcer 00:02

Please welcome the panel on "Coming in from the Cold: Espionage in Today's Geopolitics" moderated by Simon Radford, director of Policy and Programming Europe at the Milken Institute.

Simon Radford 00:17

Thank you. Thank you. People might not know this, but I hire someone to introduce me like this into every room I go into, just to get the applause. But welcome, very happy that you're here. I'm going to go ahead and say, because we're up on stage, this is definitely going to be the funnest panel that you will see. "Us and Future of Private Credit," are going to be closely running. But anyway, very excited to be hosting this. We've got an absolutely amazing panel for you today. Darrell Blocker here from DMB, Anthony Camerino from the Burkle Center, Christo Grozev from the Insider, Katherine Mulhern from Restitution Capital, and Jill Popelka from Darktrace. Welcome and thank you for being with us today. Probably like a few of you here, I kind of grew up on John le Carre, on Ian Fleming, watching Orson Welles and The Third Man. But we're here to explore, I suppose, what is the truth of what's the reality in terms of when we from what we see on the screen to what we should know in real life, and how can we apply maybe, some of the lessons from what you've learned over a lifetime of looking into this topic in everyone's work here today. So the first obvious question was, I suppose, is where do you see the sort of major threats from today? Christo, do you want to kick off? What should people be concerned of when it comes to espionage, you can't sort of span every single country, every single threat in every single way. So where should we be concentrating our efforts when we think about it.

Christo Grozev 01:46

Well, I mean, I've spent 10 years investigating or 11 years investigating Russian espionage. Obviously I'm biased and I will have to say Russia is one of the sources. But that's a very general answer. I would say the main source of new risk from espionage activities comes from the fact that there's a disbalance in the perception of the playing field between Russia and the rest of the world. Russia assumes that it's in a state of hot war with the West, whereas the West does not assume that. The West assumes that Russia is still a country with a reputation cause that may be pacified, that may be brought into the sort of law of being a normal country. So we've looked at many leaked internal documents of the Russian intelligence services where they continuously caution themselves, we are at a state of a hot war with the world, and we should treat the rest of the world as an enemy. We should treat America, we should treat Western Europe, as an enemy And I think this is the main philosophical kind of—this balance which puts us at a disadvantage. In terms of what the recent threats are. I would say that it's it comes from a phenomenon that the rest of the world cannot—other than China does not have experience in which is commercialization of intelligence and decentralization creating a market for intelligence and intelligence not in terms of data gathering, although that is part of it, but intelligence in terms of kinetic operations as well—attacks, terrorism, assassinations—and in Russia, and to a much lesser degree in China, the state encourages that competition and that competition comes not only within different arms of the state security operators, such as the FSB, GRU, SVR, but also from private players. And we are all familiar with the Wagner story of Prigozhin running a private military company which is an arm of the state with some deniability. But the same thing has happened in the last six or seven years in intelligence—covert operations and oligarchs are running their own intelligence agencies, competing for results, competing for favor with the Kremlin. And the way this works is they don't get a budget from the Kremlin. They—some of them do, because some of them are running state owned operations, state run companies such as Rostec, who's the largest technology manufacturer in Russia and that runs its own intelligence company, including snipers and assassins, right? But other oligarchs are running operations that may deliver different type of results, such as influence operations on governments, on the American government, for example, on European politicians. So this market structure is something we're not we don't have in the West, and it puts us at a disadvantage. So these, I would stop at this, because these are two more generic and general risk sources that I would like to identify.

Simon Radford 04:37

No, that's fascinating. And there's everything from state run to privatize to semi privatized—right the way across that. And in terms of the targets of that, there's obviously not just government to government threats. There's also, you know, companies here are, you know, can, can have to reckon with that threat from all those range of actors. Darrell, what is, do you think if you're a CEO sitting here today or watching, how should you think about this in terms of the threat to your organization?

Darrell Blocker 05:03

I think most of the corporate sector, as Christo was saying, is United States didn't really think that they're still in a war, whereas Russia always did. I would say that the US intelligence community, writ large, might be, might be different from that perspective. I joined the intelligence community in the late 80s when the Cold War was just ending. And then, of course, the global war on terror was the next phase. But we never took eyes off of Russia. We never took our eyes off of China. Corporate America is still operating under an old paradigm. And if you are in a C-suite position, CTO, CFO, CEO, whatever it is, you are absolutely a target. And that's what I spent the last six years after I retired, trying to convince people who are just operating from the premise that they're not a target; they are a target, to not only state actors, but non state actors. And the state actors that are that have been surprising to me are the North Koreans are really, really good at what they're doing with almost no money, no budget and not a lot of guidance and background. So if North Korea, you know this isolationist state, can infiltrate US markets and pretend to be workers within your within your companies, then you know what the Russians, the Chinese and the Iranians are exceptionally good at it as well. So you are a target and you should consider yourself a target, because if you don't people like me and people who did the job that I do will pick your pocket. They will pick your family's pocket, and they will pick everyone that's in touch with you's pocket. So it doesn't have to be you as the as the bull's eye. They're just as easily get to you through your vendors or through you know, disgruntled employees, people who are happy don't spy. If you have people in your company that have access to your codes, have access to all your inside secrets, they are just as much a threat as these, as China, Russia, North Korea and Iran.

Simon Radford 07:12

Great. That's great. I mean, I occasionally get an email ostensibly from Mike Milken asking me to buy him a 10 pound Amazon card which I report to IT. I'm pretty sure we can buy his own. But Jill, you know, you know some of the statistics around this, about the what Darrell saying, what's the scale of that sort of threat to the corporate world when it comes to cyber security? And maybe, I don't know whether it's a question you might know the answer to, but when we're due diligencing companies you might want to buy, when IP is such a larger part of company valuations these days, what—how should you maybe have on your due diligence checklist? What sort of the—you know, what—is best practice look like, if you're thinking about, is this a company who takes this seriously?

Jill Popelka 07:32

It is pretty incredible, the scale. We're always looking at the threat landscape, right? And so it's so interesting to hear the real physical stories of where, just outside of the IT infrastructure, the threats are happening. But when we see cyber threats, cyber activity, the vast majority of those actually start with a phishing email. It starts in email. And so over the past month, I did a quick check before I left the office and 550 emails had come into my inbox just in the last month. Over the course of the last month we saw 300,000 VIP phishing emails. And the interesting thing is the velocity and the sophistication of these emails are incredible, because cyber attackers are using AI. And so just like we're using AI to protect and to make, you know, our businesses more productive, they're using it to make themselves more productive and, honestly, more complex. So there's all sorts of different threats that are happening today across the landscape. Again, generally starting with email. 92 percent novel social engineering attacks are the start for most of our cyber threats we see today. Well, I would say in very simple form—I mean, we could spend an hour on that and I'd rather spend an hour listening to Christos' stories. But two different types of cybersecurity—there's a tech centric and business centric and so most cybersecurity companies are looking at protecting you by indexing the threats that are out there today and protecting you from those. Darktrace looks at it a little bit differently. We look at it from a customer specific lens and so we understand what's normal for your company—so this is a business centric view - and that we protect anything that's abnormal, anything that looks unique, strange and threatening. And so if you have both of those approaches together you are fairly safe in cybersecurity land.

Simon Radford 09:31

Tony, maybe I'll ask you this question. We've been hearing a lot about DOGE slimming down government et cetera, yet it seems like the threat landscape, if you think about everything from pandemics and lab leaks to cyber security to nuclear proliferation, seems wider than ever. How should, do you think, government think about allocating resources when it comes to all the different threats that might be out there? How should we, and also, what should be our level of citizens in terms of, you know, both I guess, oversight and making sure that they're doing that effectively.

Anthony Camerino 10:04

Yeah, I think, I think the landscape has changed dramatically in the era of social media and the information age and the spread of the internet. I mean, before you had to physically protect assets, you had to surveil people, you know, out in the real world, you had to check their activities. You know I worked primarily in counterespionage, or preventing people from ever becoming a target, identifying their vulnerabilities before other people would identify them that so they could be exploited. And the, you know, propulsion of social media in our lives and how much of our lives is spent online, it just opened up this whole other field that now you have to protect, which is, you know, 30 percent probably of—if you take your average soldier, your average civilian who has access to classified systems, and you look at how much time they spend online, and how much time they spend on social media or other things, then you realize you have to take the all the resources you had in the physical world and take that same percentage and dedicate it to that, to that activity. But maybe even more because they're so much easier to access, and they can be accessed multiple times, in multiple ways, and it's much easier to identify. And Darrell, you would back me with this—it's much easier to identify those motivations, those disgruntled people, because they're putting it out there online. You don't have to go search for it. They're presenting it to you. And so I think it makes the recruitment effort, like, infinitely easier for adversaries to find and identify those weak points and those people and/or, if you start talking about disinformation, create them, create those motivations. And that's—that's a big difference nowadays. That's how landscape has really changed.

Simon Radford 11:49

Fantastic. I should remind everyone there's a QR code above my head, in a very rich conversation - but we'd love to start to try and integrate some of your own questions. So do feel free to ask some questions via the QR code which will come up on my iPad here. Christo, maybe I should ask you a similar question to the one I just asked. You covered the Salisbury poisonings in the UK committed by Russia in—against some of their diaspora. How can we tell whether our own democratic states are doing a good job or bad job? What should be the role of democratic oversight? There was a great article a few years ago in the New Yorker about Dianne Feinstein and the CIA and, you know, what should be the level of what's heard behind closed doors? What should be open to everyone? What's your role? About that—you know, we've talked about the sort of privatization and non-privatization on the other side. What about democratic oversight on this side?

Christo Grozev 12:38

It's funny. This reminds me—a couple of years ago I was at a think tank session in London, and one of the speakers was the former head of MI6. And I asked a question—at that time I was the CEO of Bellingcat, the open source investigation platform—and I was one member of the audience, asked the question of him what can we do? Because he was talking about China—how China is privatizing intelligence. And I said, what can the rest of the world, in the Western world, do to counter that? Is there anything we can do? And he, without knowing who I was, turned to me and said, you know the closest to that that we have is an outfit called Bellingcat. And it was hilarious because it was almost like a setup, but it wasn't. And that's the problem. We can't really do much other than have private initiative or, or private companies try to investigate for whatever reason, for whatever motive they have, financial or otherwise, but then make public. Because part of the problem is that, and this is changing slowly, that intelligence agencies are often doing a proper job in terms of data gathering and collection of trends and data on enemy states, but then sitting on that and just perpetuating their role as the holder of the choke point of intelligence information, without sharing that necessarily with law enforcement, who have some capabilities and mandate to actually prevent. And the case that you refer to, the Salisbury poisonings, the assassins, the would be assassin—actually they did kill a random stranger in the process because they left their bottle of novichok unaccounted for un destroyed. They had been traveling to the UK for about seven years under fake identities, and they would be using sequential passports for those fake identities and somebody in the British apparatus, intelligence counterintelligence apparatus, had not spotted that for seven years, and if they had made basic efforts to check whether every applicant for visa to that country exists in the real world, which is a basic, simple data job that I can do within 10 minutes, but if I had done that, they would have found out that these people don't exist in any Russian database. They had been created as fake personas, like just before they started traveling to the UK. I cannot imagine, I hope, that somebody in the counterintelligence apparatus had spotted that trend and were sitting on that because they were following their movements until, actually, it was too late, because they did strike. Because the worst explanation is that they didn't spot that trend, right? And this was something that we thought were protected. We, as the public, thought we are protected by competent counterintelligence agencies, but we're not. And I'm not sure which of the true is—which of the two is true. But by shaming them through publications, by investigative journalists, for example, you can change that—that dynamic. It can make them much more careful, much more diligent, and you can also make them be more proactive in exposing such operations, because that plays a role of alerting the public. When you just sit on it, and you know about malign operations by the enemy states, but the the public doesn't know, as we heard in the corporate world, you've only done half the job because—because even if you take action, if you don't have the self-defense reflex in the corporate world, in the public, then—then the risk is much bigger.

Simon Radford 16:11

Katherine, you run a very interesting company and fund. I'll let you explain it rather than me try to do it. But we're talking about democratic oversight and what we can do to better counter perhaps, what other people are doing. We've talked about Russian sanctions, how effective they are, how not effective they are. People have talked about financial centers and looking at property that might belong to people overseas. What is—first of all, do explain exactly what you do and then also maybe, then, what can the role—what can we push our representatives to do, to sort of clean up our own act when it comes to taking away the source of some of these funds which then go to fund some of these activities?

Katherine Mulhern 16:51

Yeah, no I'm happy to. And it's funny because Restitution really uses the tools of capitalism. And I presented this—one of our chief advisors is—is a fairly senior former Canadian government person who introduced me to the Canadian mission in Mozambique, and it was basically during a holiday. It was the Mozambican national holiday. So there was one person in the room, and he was just watching the Canadian mission, as everybody else was off, and I explained to him what we were doing and we had this mic drop moment where he went around the table, picked up an old fashioned phone and said, Alyssa, you have to get in here. And then five people from the Canadian mission came in and I explained this. And so apologies I'll give a little bit of an explanation as to what we do and also where we come from. Because in many ways what we provide and what the panelists have been describing is the shield element. So how do you protect yourself? What we are is more of the sword element of how do we actually become proactive in terms of getting money back? And money, I think is, and I think the panelists would agree with this, is very important part of the equation, right? So if you've got a terrorist organization, serious and organized crime, if you have people traffickers, if you have wildlife traffickers—they are using money, illicit money, to do the work that they're doing and that illicit money flows through the system in parallel with the clearer money, the commercial money. So how do we actually look for that and how do we get it back? So Restitution, essentially, is an asset manager. We use litigation funding and private equity models to work with newly democratic and post conflict governments to develop claims. So these could be fraud claims, breach of contract claims, they could be claims for corruption. And essentially, we go after the assets that have been stolen from these countries and return them to the countries in a way that's transparent and accountable. So we'll work with them to set up a sovereign wealth fund, an education fund to help human rights organizations and civil society. We work very closely with civil society and whistleblowers as well. Often our sort of whistleblowers, the first people who come to us with these claims, are civil society. So we're probably one of the few asset managers that are often contacted by archbishops or religious people who say, look, we've got an issue here, we need some help. Then what effectively we do is we work with these governments, end to end, to bring back the money. And the scale of that is enormous. So Bangladesh recently announced that they believe they've lost 100 billion, "B", billion in terms of kleptocracy and corruption. Angola came up with a similar number. So I think they said between 100 and 150 billion. So that sort of money can not only destabilize a country, but also destabilize the financial system as well. What we do is work with those countries to identify and develop ways to start bringing that money back in a way that's transparent, accountable, and organized through litigation, settlement, policy discussion, sort of government to government discussions as well. And so what we found when we've been doing this work is essentially we're seeing what I would call gray money, which is this fraud, tax evasion, other types of money, but side by side with that, is very dark money, which is essentially money for serious and organized crime, terrorism, also for movement of people and movement of animals. All of this is connected, and the gray money starts to move into the dark money very, very quickly. So one of the things that we really work with these governments to do is not only bring this money back to pay for schools and roads, to set up wealth funds and make sure that that wealth is returned to the people, but we also look at ways to stabilize and clean up the financial system. Because, as we know, if you come to somebody with a $100 billion claim and say, "you have to return this", hearts and minds do follow. So that's our work that starts to chase people around at parties.

Simon Radford 21:13

We're all gathered here so we'll come to you. There was obviously, a few years ago, there was revelations about the Panama Papers and other things. Have we made any progress?

Katherine Mulhern 21:25

Yeah, no, it's fantastic. Actually, this information goes to—and I have to say Bellingcat is incredibly important for us as well. So information from whistleblowers, document dumps, all of that information is useful in terms of building cases. And we've actually been able to build cases for countries. Very significant fraud cases just based on that information. But there's also information out there which the IMF and the World Bank is starting to work with governments on where Swift, for example, has information that's just out in the system. You can contact swift get information about sort of country flows in and out and then start to map where this money is going. So, for example, with a southern African country, their major trading partners are A, B and C, but then there's a money moving to D. D may very well be some place that's actually acting as a haven for illicit financial flows. So that sort of information, sort of top down information, is incredibly important. Although I have to say most of the information we get is from whistleblowers and witnesses. So—and you know, for example, somebody will be sitting at a port saying, we keep seeing, and we had this recently, pallets of cash being moved into a port, or being hidden in white goods in a port, and those pallets of cash are being moved into a place in a country that's unstable. That money is being used to fund terrorism or to fund warfare. So those are the sorts of things that we're able to pick up as well. So that human intelligence piece is very important.

Simon Radford 23:04

So just with tariffs dominating a lot of the last few days, US Lesotho trade seems to be like an example that keeps coming up. So maybe that's one of the D's, I think, in that A, B, C. Last question on this, because it's interesting, in terms of the West being a source of laundering a lot of this money is—are there steps that we should be pushing our representatives to, to close down the opportunity to have a lot of that money come our way?

Katherine Mulhern 23:30

Yeah. I mean, yes, 100 percent and there's a lot of sort of current legislation transparency that's sort of coming through the system now. So the UK in particular has been very focused on trying to close down the UK as a haven for some of this money. But I think for us, one of the key things, is the litigation settlement policy piece. The litigation piece is very important, because if you don't go after this money and return it, and actually make people think twice about it in terms of their bottom line, they'll continue to find ways to do it.

Simon Radford 24:06

In the spirits of, sort of, you know, the Milken Conference being great and coming up with financial innovation ways to solve social problems and I think Katherine is showing a great example of exactly that. We've been asked about cyber insurance and is that an effective tool in terms of, you know, is that something which you would advise in terms of—or is it a kind of a waste of resources and we're better spending that on internal controls? What would be your—

Jill Popelka 24:30

You know I don't know if I have a clear perspective on that. I was just thinking though about all the things that Katherine's doing to investigate and one of the things that cybersecurity, powered by AI, can do is investigate. And so we've just acquired a cloud forensics firm called Cato that even with ephemeral data, even with data that's moving and then disappearing, sometimes, Cato goes and grabs it if it appears to have a threat actor behind it and then you can go investigate. Where did that go? What happened? Where was the exfiltration of data or dollars? I think we should have a follow up conversation on how we might be able to work together.

Katherine Mulhern 25:01

Yeah, that's great.

Simon Radford 25:02

Yeah love that. We've already done a deal here on the—fantastic. You three need to up your game. So we've talked—we talked a bit about, about cyber, talked a bit about due diligence in companies, maybe, and seeing whether cyber is up. A lot of you use open source intelligence. There's been obviously a proliferation of data everywhere. If you're an executive trying to sort of use open source ways, trying to separate signal from noise, are there lessons from how intelligence operatives do this to how maybe executives should do this in terms of trying to weigh up and assess huge amounts of data in terms of their competitors, terms of them, in terms of the markets they operate, what would be—I happen to open this to anyone. Are there any lessons which you think separates good from bad when it comes to evaluating open source intelligence?

Darrell Blocker 25:52

Honestly, there are so many really good firms that are out there doing open source intelligence. And all INTs—I was in HUMINT, my job was to spot, assess, develop and recruit sources. Of course, NSA signals intelligence, but OSINT is the largest of all of them. Because it captures not only what we're saying in English, they're speaking Swahili, and literally, every language on the planet is all coming into this huge—it's not even a cloud. It's literally the atmosphere around planets. That's how big it is. You have to tailor it to whatever your business interests are. You could be in the retail business, you could be in the manufacturing, you could be in different space. So you might want to look at OSINT in that sense. But if you don't have an open source intelligence or OSINT capability within your company, you should, it already exists in some sense, you just haven't codified it, and you're going to be behind the curve, and you're going to be the middle of the bull's eye if you don't have some semblance of what it is that's available out there and the information some people—some you can sell it. I mean, you can go to different companies and buy what you're looking for so you don't have to create your own but you have to be able to tap into it. It's, it's too important to overlook.

Simon Radford 27:17

And Christo, Bellingcat is—we've talked about sort of a—you know obviously people are very aware of what Bellingcat do, anything like—There's lots of people who try and do what Bellingcat do, not nearly quite so well. So what are the skills and capabilities that Bellingcat has? I mean, I think there's now with lots of stuff on Netflix just being about every single murder that's ever happened. There's lots of people trying to solve all these things out there in the world. People think Elvis is still alive. What separates Bellingcat from sort of the amateurs or people who are trying to do this from their laptop.

Christo Grozev 27:46

The obsessiveness and attention to detail. I'm no longer with Bellingcat but I spent a better part of a decade working as a freelance as a volunteer investigator there, and it was the collective nature of the work that probably set it aside from everybody else, and also the lack of ambition to own the result, the willingness to share it with other crowd-sourced partners. And I think this set Bellingcat apart from everything else. There was a global community of people who could allocate a couple of hours of their day or week but had a particular competence in a particular area, whether that be photography or sound, as was my background, audio. And it was just this collaborative nature that created a virtual genius investigator, which wasn't one person, it happened to be five or 15 or 20. So I think that collaborative nature without the fear of being outscooped by a competitor, because a lot of the people were from other media and they collaborated, was one thing that set it aside. But what I think I contributed myself in that process, and that scaled with a lot of other media doing that, was the knowledge—finding the knowledge that actually bad actors governments are lazy and they make mistakes. Because before we discovered that, it was kind of assumed that intelligence agencies are not investigatable by the general public, they can be only investigated based on human sources by other governments. And we found out that actually they're just as lazy and just as bad as protection—protecting their own digital infrastructure as we all in the commercial world are. And that knowledge that they leave loopholes, that they have their subject corruptions or they—many of them like give a company—Well, this is an actual example. I have to hypothesize it. Imagine one of the scariest Russian intelligence agency outfits that has its own digital — offensive digital operation targeting American companies. But imagine the head of that organization starting a love affair and the woman—and she getting pregnant, and now she needs some money,. But he can't really give her money because he cannot acknowledge that he's had a child with her. And he gives her a company—gives a company that becomes a digital infrastructure provider for the GRU just so that he can allocate some money—some alimony through the government funding. But obviously that company is mismanaged and the end result is server logs become available to investigators like us. But the knowledge that there are these mistakes made along the way in a relatively—in a very corrupt system like the Russian government is what set us apart because we started pursuing such holes and many other media did not do that before that. And now every large media organization has its own open source investigative unit that looks for such holes in the data protection system of governments and finds them.

Simon Radford 30:55

I have a funny feeling that example didn't just come to you. It's coming up in an article next week. So in terms of—we talked about the role of the state and private enterprise, Darktrace has a really interesting origin story in Cambridge, England, with some state collaboration at the beginning, I believe. What's the role of actually—sort of creating an environment where we can create more defense tech, cyber defense tech, that seems to be a strategic place where it's not a kind of either or, but both 'and' — is there other stuff which our governments can do to sort of foster innovation around this area. Because, you know, in terms of separating signal from noise, obviously that's what you do. If we need more of that, then it seems like we should be sort of spurring innovation in this area.

Jill Popelka 31:39

It is so important that we all work together, that it is an ecosystem effort here. And yes, so Darktrace was founded in 2013 and founded by mathematicians and intelligence officials. And so they really worked together to understand —how do we come together to really protect companies right from what's going on externally? And they really were visionary in how they saw the future and saw that there was going to be an ever evolving threat landscape that we needed to protect from. And so to try to keep up with the landscape actually didn't make as much sense as protecting the company by understanding that normal—what is the volume of normal within the network, within people, within data. And so we can protect those things by knowing what's normal. And then, you know, elaborating on what's not and evaluating that versus models. Today we work with governments, we work with even our competitors, in order to ensure that the fabric of cyber security all sits together. So, as an example, we recently found that one of our competitors had a vulnerability in their solution and we didn't call the media. We called them directly and we said we recommend that you take a look at this. And we have basically ombudsmen that do that amongst our companies so that we can create that fabric that protects the world. It works with governments as well. I think, right now, governments are looking at AI in a broader way, you know, the proliferation of AI and everyone using it now, everybody's looking at, how do we use this most impactfully? And there is a way to use AI across all of our cybersecurity ecosystem in order to ensure that we're protecting and understanding. Just like Bellingcat is doing—how do we protect right from those things happening in the future?

Simon Radford 31:39

I think that maybe this is the first time in a Milken Conference. How many years has it been—20? However many years—that you've advocated calling a competitor to tell them how to improve their product. So that's a—

Jill Popelka 33:28

It's counter cultural but if you think about the importance of it, it's important that we all have that kind of integrity so that we can, you know, protect ourselves against the bad guys.

Darrell Blocker 33:38

And it's what the enemy is doing. It's what the nation states are doing because they control the companies and it's expected, in fact, it's demanded that if they want that information, they'll give it. So if corporations stateside or globally don't, you're making yourself at a disadvantage. So, smart for Darktrace to do that. Good business.

Simon Radford 34:04

We've got a great question here saying Africa has come up a few times today with aid being pulled removing it as a source of soft power and the main source of influence in Africa for the US, I would say also for the UK which has cut its aid budget. What do you think will replace the kind of soft power in terms of influencing western ideals in Africa and what role can intelligence play in terms of winning hearts and minds? Because I think obviously in terms of the dollar following the flag, you know, there's an element where having influence with some of these governments can help to create markets, create economies where taking money out of the country doesn't necessarily need to be the way that people are successful. Do you have a view on what role aid has played? Can play? Was it being well directed? Cutting it—presumably not a good idea? What would you like to see in terms of complementing?

Katherine Mulhern 34:56

Well it's an interesting question. Well, I was told to say that if it was a difficult question.

Simon Radford 35:04

We can ask someone else if you'd like?

Katherine Mulhern 35:06

No! We, from our perspective, we see the issues as being sort of multi-fold. So cuts will cut into some of the very basic services that Africa needs. So medical care, for example, USAID has been responsible in Western Africa for 70 percent of the medical care that communities receive. So it's done through civil society. But for us, in a sense, what we've seen as well is there's potentially an opportunity to start again talking a little bit about stranded assets, historical assets, corruption and corrupt networks. So Africa would be a net creditor if illicit financial flows were reversed. So that includes everything from trade, mispricing of trade, through to non-payment of licenses, through to tax dodges. So fixing that, and I've sat with a couple of very senior ministers of finance who are saying, actually, for us, there's some very interesting opportunities here in terms of trade but also looking at historical assets, stranded assets, and returning them, because if you're able to bring the billions back, then potentially, you can start funding your own health-care initiatives. So I think part of it is not great at all, but part of it, potentially, there are some opportunities as well.

Simon Radford 36:32

Well I did ask you first. I think there's probably a few people who have got some interesting things to say here. You both served in Africa

Darrell Blocker 36:39

So I spent probably 12 years in five different countries, west, north and east Africa, the AID portion of it—the development portion of the soft power that we had is—I don't know how we regain that after we close these programs. Personally, I was not a huge fan of how AID administered some of the things, there's things that can be fixed, but overall they do so much more good with the local population that what we're creating by pulling out is more enemies. And we don't need more enemies in the world. We need either move them into the frenemy camp or into the into the friendly camp. It's going to hurt us for a long time. I just got back from Nairobi and I was talking to someone from the embassy. What has been the impact of all these executive orders and everybody is—they're frightened. People are afraid. So now they're creating insider threats of people who are going to get back at the government by reporting to someone else or not feeding—children are going to start dying because, again, 70 percent of the aid that goes into some of these places, and I ran all of Africa division for the agency, and it breaks my heart personally, but I think it's making us a target, and it's going to be a much dangerous in ways that I don't think the unintended consequences have quite yet been discussed. But there are good signs. There are things that shouldn't have been going on that are no longer going on. And maybe there can, you know, they can meet in the middle and figure out a way forward. There are a lot of good businesses in the United States that are still there. Maybe filling the gaps of what AID was unable to do. Civil society in lots of Africa can rise up. And, quite frankly, I think AID should have been one of those things where you're creating the capacity for the countries there to do it themselves and they've been doing it since the early 60s. So maybe some of those programs in the long run will be—it'll be a betterment. But for the foreseeable future I see nothing but a lot of confusion. Governments who might have been on the fence or might have been on the United States side are going to go fully into the China camp or fully into the Wagner or Russia camp, and that's not going to be good for us in the long run.

Simon Radford 39:16

Tony, did you want to add to that?

Anthony Camerino 39:18

I mean, it's more just confirming what Daryl said, which is that — I've also been involved in training in Africa, and it's about bringing up their capabilities to counter I mean—you look at the southern Sahel, for example, and what's happening there and how rapidly things are progressing and they really need the capability to conduct things like counter-terrorism, counter-insurgency, effective policing, policing, with regard to the rule of law and ramping up those capabilities is beneficial to us too. Because, I mean, you look at the number of terrorist attacks that have originated in Africa targeting the United States or through Europe and those capabilities benefit us. So to pull back from that and to leave them on their own to try to learn those capabilities and to implement them and you're talking about enormous training requirements across those countries just because of population and size. And to pull back from that is really, I think, like Daryl said, it's really, we're going to see the effects of that in the long run.

Simon Radford 40:18

With a much larger population projected over the years. So there's a lot more people, or more hearts and minds to be won if we pull back now. And Christo, is Russia stepping into the gap?

Christo Grozev 40:28

Totally and with the understanding that the playing field is being emptied for them. And what is interesting is that they had the Wagner initiatives seven years ago, eight years ago, and that was a combination of providing sort of military assistance to local governments, together with some political technology, as they call it, sort of advice on how to win elections and so on and so forth. But that was just then. What is happening now is every intelligence agency in Russia has its own Africa initiative. One of them is called the 'Africa Initiative' coincidentally—a new one that was started after it became clear that the United States is going to pull out from from aid. It has a little known name, Department E, it actually mass recruits agents of influence on the African continent, across every country, and it's hidden under the [inaudible] of military intelligence. That tells you the intention, right? It's not a benign, soft power intention. It's much harder than that. They're planning to get every country that was on the fence to the Russian side and they're competing with China in that in several markets. So they're doing this through mass recruitment. Bringing people to study in Russia for six months to two years and then sending them back already pre trained in the dark arts of both influencing political process, but also, worse than that, sabotage operations. And yes, there was the role for continuing private initiatives by the United States in the absence of American government support but it's much more difficult now when the government has given up on Africa. I'll give you an example of the Bill and Melinda Gates Foundation were providing all of this vaccines to the African continent and those vaccinations were subject of a very concerted Russian campaign of defamation saying that all of this is sort of a plan by the CIA to control the minds of like, physically, the minds of Africans and citizens of African countries. And then the United States did a pretty good campaign a couple of years ago in last year, through the Global Engagement Center, of traveling through Africa and showing that this campaign is based on false premises and on disinformation coming from Russia. And that was, in a way, a counter to that disinformation project. But now the Global Engagement Center has been canceled, has been disintegrated, together with the AID, so even the private initiatives will be faced with lack of support from—the only place where they could have gotten the support is from government initiatives such as the Global Engagement Center. So I'm very, very pessimistic of the next four years in and I think we'll see many more countries in Africa taking the bait of Russia and the offer of money. And while we're talking about Africa, this is also true for LATAM, the Global South, more generally. I mean, even looking at elections in eastern and central Europe, I think in terms of information and disinformation, there are maybe lessons to be learned from this example, which we're talking about in Africa.

Katherine Mulhern 43:34

Yeah, the one I think you've mentioned China, and so we do quite a bit of work in Africa as well. China was very active a couple of years ago. But the issue I think, and African countries are starting to tweak to this is that if you do a deal with China, often that deal will be a debt deal. Well, you end up giving up your assets. You end up giving up ports. This happened in Sri Lanka. I think, particularly with China and Russia, African countries are looking at them and saying, yes, you may have something to offer, but we need to understand more as to what that offering is, because with the Belt and Road Initiative, quite a few African countries got burned by that. So I think for us it's interesting to watch. There is definitely a play between the US, China and Russia, but I also don't think the

Russians have the money to be able to give to—replace what the US has given. So it's a question of influence peddling, as opposed to, here's the cash this will replace what the US gave you.

Simon Radford 44:37

Now it's an abiding source of regret that I went to Cambridge University, speak Russian, even went to Russia, and no one's ever asked me to spy on anyone. Despite the fact that I am incredibly good at keeping secrets. But we've talked, we've talked about, you know, sort of cyber security, open source—I wanted to come to the human element here. Now, you know, I was interrogated over several days to get a job at the Milken Institute. You were actually an interrogator. You must have learned a bit about when someone's lying to you when they're not. Certainly there's been some potential failures in terms of relying on human sources in terms of the Iraq War. So maybe great successes in terms of predicting what Russia was going to do in Ukraine. What are the lessons, I suppose, both in terms of what we've learned from a state and geopolitical angle. But what can people here learn about betting on their instincts in terms of, you know, relying on humans and working out how to trust and when to trust?

Anthony Camerino 45:37

It's a great question. We learned a lot of lessons, hard lessons, some lessons we're relearning that we had learned in Vietnam. Obviously — I think the biggest lesson I learned, I did, you know, I conducted or supervised over 1300 interrogations. I physically interrogated the number two and three guys in ISIS when they later went on when they were in Al Qaeda in Iraq, and I also interrogated a lot of very young recruits in Al Qaeda. People who had been for six months to build a website or to wire a bomb. And I think one of the things I learned is that we need to get better at asking questions and not just making assumptions. And we made a lot of assumptions in going into that war, not just about, I'm not talking about the big ones like weapons of mass destruction—like what factors and influences are on an individual to join a terrorist organization. Because we put so much effort into countering terrorism from the perspective of stopping a bomb from going off and so little effort into stopping from people from becoming a terrorist in the first place. And that, you know, the policies that we had in Iraq at the at the beginning, with de-Baathification, disbanding of the army, allowing Shia militias to run free, to infrastructure, you know, made that decision for people and made them incredibly vulnerable to recruitment and then wondered why are all these people joining Al Qaeda and also not understanding the tribal politics of Iraq and how influential they are on people's decision on what side they fight on. And it took us years to learn those lessons and I really think it was a result of us not being able to ask ourselves questions and be able to question our own assumptions and the effects of our own policies. And so I think one of the things we really need to get better at is understanding the micro. I mean, the biggest recruiting tool for Al Qaeda during that entire war was Abu Ghraib. Continues to be. You know, understanding that if somebody is facing social factors, socio-economic factors, that make them vulnerable to recruitment, but then they see pictures of Abu Ghraib and they realize, now, this is a calling. This is something beyond my socio-economic status. This is something I feel very deeply internal which is not that different from the way we feel when we join up. Understanding those very individual motivations, I think is really important.

Simon Radford 48:15

Christopher, we had a question here about how the former Soviet Union tried to sort of demoralize Western cultures. And speaking of Cambridge, I mean, half of them wound up spying for Russia. We saw the troll farms in the election. Is there anything which we should be thinking about or doing from a national security perspective in terms of the culture war aspects of things? In terms of trying to sort of safeguard our elections, for example? Apart from me starting my own troll farm startup to attack them, is there something?

Christo Grozev 48:48

Which is very much doable these days and that is the problem, because, as I said at the beginning, the privatization and the market nature of offensive intelligence operation by Russia will now make it exponentially more effective because whereas seven years ago, the troll farms run by Prigozhin had to run a competition of essays provided by the wannabe troll operators through trollers, trolls, where they had to describe a day in the life of a typical American in order for them to qualify as a troll, right? And we were reading those in real time. And some of these are hilarious. I mean, one of them, I even published it on Twitter, was somebody wrote essentially, My day—imagine my day—as a typical American—and you could see that most of the knowledge about the day of a typical American was taken from Jon Bon Jovi songs, which was great. But now you don't need that. Now you can use AI to really, really replicate the life of a typical American. So that is a problem. You can do that as well, but there's no incentive for you to do it other than, apparently, your pursuit of fun and some social responsibility. Russia is creating these incentives for everybody with the money to do that and get game papers from government. So that is a big problem. I don't know how to counter that, because, again, the problem is that for that most vulnerable part of the population that will be susceptible to influencing—the quality of fakes created by AI will be sufficient for them to be convinced this a real human on the other side. So that's the problem. It's this balanced. It's not going to work on the informed people. It's going to work on the uninformed people which can be swayed to to a particular group and help them win elections. I don't know how you find that other than through education but it will take a generation for that to be fixed. So I don't have any optimistic answer

Simon Radford 50:50

It was a long shot question.

Christo Grozev 50:55

If I can just say please going after the money is the only way to do that. Yes, equating any funding of such troll farms to essentially a crime, a transnational crime, so that you can deter these mini-oligarchs, oligarchs, businesses, infrastructure providers, even AI providers, to anything that results in such malign operation. Equating it to a crime, to terrorism, to information terrorism, that's the only thing that you can deter. You can't fight the symptoms. You can fight the sort of the funds that fund this operation.

Simon Radford 51:29

So I think we need a sovereign wealth fund for you Katherine for the public good. I think that sounds like a good thing to do. Speaking about interfering in elections, you know, I think actually, the West been quite good interfering in each other's right? You know, we've had Elon Musk saying he was going to give lots of money to the British populist party. We've had JD Vance coming to Munich Security Conference. There's been some people saying that the Five Eyes system, which has obviously been a tremendous strength in terms of cooperation on intelligence for the West, might be under threat. What do you think about that? Is that something which is a hyperbole? Something real? If you were Sir Keir Starmer would you be sending over all your high grade intelligence for people who can't use a Signal app encrypted chat?

Darrell Blocker 52:11

I would say that the threat to the Five Eyes alliance, which was formed after World War One, is as close to being permanently damaged as any time in my 38 years in the intelligence world. I can't think of an operation that I ran that didn't involve at some point MI6 or at some point ASIS, which is the Australians, or at some point CSIS, all of our partners we tap into each other and we share training, we share common history, we share everything on the counter proliferation on the counter-terrorist side of the intelligence. When trust is lost, then it is really, really hard to regain, and trust is absolutely the currency of intelligence. It's the currency of every relationship you have in your in your life, personal, professional, intimate, and otherwise. It all begins and ends with trust. And when your partners start to distrust one another, then you start to hold back, which you know I'm certain that four other partners are going to continue, but they are going to think twice about sharing their most sensitive information that could result in, you know, the death of whoever was behind it, or identifying, you know, how we tapped into their critical infrastructure. I would imagine it's already started having been, you know, I've been out for seven years now, so don't know for sure, but I know these partners, and I'm still in touch with a lot of folks who are now retired like me and it is having a trickle down impact on the Five Eyes. Most definitely.

Simon Radford 53:57

Does anyone else want to jump in on that question?

Christo Grozev 53:58

From my little observational experience I can say that this is happening. There's a reluctance to share even with other members of the five eyes because no, no country knows whether they will share with the United States. So at least for a while there's a withholding of data. The only upside of that is that they are now inward looking to establish certain sourcing that didn't exist before because there was an over-reliance on American intelligence through NSA sources, for example, provided to the Five Eyes. The Five Eyes are no longer five eyes, I mean, we call it five eyes, but it's like 12 eyes, so 12 pairs of eyes. So there's an attempt to rebuild their own open source intelligence to replace, to supplement some of the missing data. But even that is kept closely to the chest because they're not sure if, for example, if the Swedes share with the Dutch. They're not sure if the Dutch will not share data with an Elon Musk infiltrated America intelligence operators. I think this will improve but, for now, that is a fact.

Simon Radford 54:01

Jill, we can't have a conference without, you know, discussing the future of AI and all the rest of it too. I was at a dinner yesterday with some European folk worried about the transatlantic relationship. Some saying, will there be a move to sovereign AI, or, you know, an EU cloud, or whatever it might be. I'm not going to put you on the spot with that because that seems unfair. But in terms of the West winning the AI race, which seems so integral to a lot of what we're talking about, just both in terms of company safety and but also in terms of for use by our governments and others. Are there—is there a sort of a three point list, or a wish list, or something you'd like to see our governments doing in terms of helping to accelerate our race for kind of the AI dominance, I suppose, you know,

Jill Popelka 55:48

I'd love to see them work together. I mean, I think that would be the first thing that I'd like to see. And, of course, Darktrace is a British founded company, right? And there's incredible intelligence happening in the AI space, incredible creativity and innovation. And I just think working together is going to be the best option for us across the ocean. Especially when it comes to AI and these large language models. I mean, the more that we try to create our own regional models, the less power they'll have and the less balance and the more bias. And so that's not going to be great for the world. So, I mean, it might be an unfair question but my perspective is that we need to continue to work together as a global entity because that's when you know—that's when AI is going to be the most powerful for us combating all the things that we're working on.

Simon Radford 56:32

Katherine, maybe the same question on illicit financial flows, is there a wish list, something, one or two things that, if you'd like to see heads of state come together that could make a real difference in terms of combating those financial flows?

Katherine Mulhern 56:44

Yeah, it's an interesting question. In a sense, it's the same answer, which is, the more cooperation, the better. So particularly for countries who are that—essentially the source of illicit financial flows and those who are receiving the illicit financial flows. So—and there's another piece to this which I find fascinating, which is the personal piece, which is, there are super connectors. So if you are sitting in Afghanistan and you have a poppy field, you're not going to be able to figure out how to get heroin to the UK. There are connectors who connect you to the global network. So focusing and targeting those connectors and sort of disclosing who they are, using AI to go after them, and also looking at other ways to foil that, could be a very interesting perspective. So more cooperation, more use of these open source information, and really looking for these super connectors.

Simon Radford 56:45

Well, we're almost out of time. Tony's a screenwriter too and has brought a lot of this for our entertainment [on] stage and screen. So that's going to be the inspiration for this final question, which is, who is your favorite not real life spy and why? Which is a key takeaway for you all. Get your pen and paper ready. Jill, why don't we start with you? Do you have a favorite spy?

Jill Popelka 57:57

I'm a girl of the '80s and grew up with Tom Cruise, and so the Ethan Hunt story is fabulous, and I think he's taking on AI soon so it's going to be a great one coming out. So I'll go with Ethan Hunt.

Katherine Mulhern 58:09

Weird one, but Ben Affleck and 'The Accountant.' Yeah, I work with a lot of forensic accountants, and the second part of this movie is coming out and they're so excited.

Simon Radford 58:22

That is the most Milken answer—your favorite spy is an accountant. I love it. Christo—favorite spy?

Christo Grozev 58:29

Well, because I live and investigate this work I have to say that—I would say the one that is closer to reality, not the ones that are most beautiful to watch on screen and that must be the characters from 'Burn After Reading,' as opposed to any of these guys because that's really the average quality of spies.

Anthony Camerino 58:48

[To Anthony] are you allowed to name your own characters? I don't know. That's what I was going to do. Well, of course, personally invested in John Reese who was in 'Person of Interest,' the TV show which I worked on for five years, and we poured a lot of information from personal experiences into that character to humanize them, to understand the cost that happens to spies, not in the field, but also when they come home.

Darrell Blocker 59:12

My—when I was the deputy director of counter-terrorism I met the cast and crew of 'Homeland' before the beginning of season three. So Saul is my man.

Simon Radford 59:33

Yeah!

Darrell Blocker 59:33

And I remember the creators of the show asked me what they were doing right, and we were told you can't say anything bad about this script. You can't say anything about her having mental health. And I said, you're not getting much right, but you don't want to get it right because it makes us less safe as a nation. Your goal should be entertainment, which it is, so I would I'd say '24' and 'Homeland' would probably be the ones that I enjoy. And 'The Americans' which my classmate at the agency created that show

Simon Radford 1:00:08

In terms of 'Homeland,' one of the best stories I heard about this is Damian Lewis. When he went to the White House to meet Obama, he gave him a copy of season one of 'Homeland', saying, from one secret Muslim to another. I'm going to give a shout out to 'Our man in Havana' and Graham Greene, but this has been an absolute riot to moderate and so much fun and so interesting. We learned a huge amount too. I'd love to have a warm round of applause for our panel. Thank you.

Announcer 1:01:11

We thank our 2025 Global Conference underwriter for their support of this event.

Disclaimer: This transcript was generated by AI and has been reviewed by individuals for accuracy. However, it may still contain errors or omissions. Please verify any critical information independently.