7.17.24

9:55 — 10:30 AM

Phishing, Fakes, and Fraud: Tackling Transnational Crime and Enhancing Global Security
Brian Nelson, Under Secretary of the Treasury for Terrorism and Financial Intelligence, U.S.
Department of the Treasury

<u>Matthew Noyes</u>, Cyber Policy and Strategy Director, Office of Investigations, United States Secret Service

Jürgen Stock, Secretary General, INTERPOL

Moderator: <u>Nick Schifrin</u>, Foreign Affairs and Defense Correspondent, PBS NewsHour YouTube recording: <u>https://www.youtube.com/watch?v=Nyx_TXhnl_s</u>

Nick Schifrin:

Thank you so much, Niamh. Thank you everyone. If you guys could just take your seats, those of you who are staying in the room, and I'll open this by admitting that when we plan this panel, we plan to talk about organized crime, financial crimes, cyber crimes, and the geopolitical impact they can have, as well as more personal financial attacks like elder fraud and pig butchering, which is not at all what it sounds like. That's when scammers fatten up their victims like pigs and then lead them to the financial slaughter. And I am going to cover quite a bit of that as much as I can, as much as possible in the time. But given the events of the last few days, you'll forgive me for shifting for a few questions at least. Matt Noise from the Secret Service. Let me state for the audience upfront. Matt is not in any way part of the Secret Service package of personal protection provided to former President Trump or to any other officials, nor are you involved in the investigation or even cyber threats against the people who the Secret Service protects. But I'm hoping that you could for this audience, give a little insight into a few of the following questions. How has the Secret Service shifted its resources or frankly had to shift its resources since the failed assassination attempt to former President Trump?

Matthew Noyes:

Yeah, thank you and good to be here. Clearly there's several reviews ongoing as there should be, and so I think it's important to let those reviews get the accurate facts. At the Secret Service, we're charged with two important missions on behalf of the nation, safeguarding the financial systems and also ensuring the security of our protectees. The protection is always urgent and so we obviously have to shift resources to address that. Neither manpower or budget is as elastic as you would hope when you're responding to events, but that is part of the design of the Secret Service is that we have a depth so we can shift resources as needed to meet increased requirements, which is the case.

Nick Schifrin:

Now you describe a Depth, but over the years some Secret Service agents have gone public and said that you guys feel spread too thin. And I'm wondering if you could talk about if there's been any internal discussion about whether you are spread too thin.

Matthew Noyes:

Yeah, I think that's long been the case. The Budget Control Act essentially put a harsh limit on civilian agencies, non-defense, non intelligence community components in terms of hard budget caps that limited hiring for a number of years When you're an organization like the Secret Service, just shy of 8,000 people to not hire for several years in a row has a long tail impact across the careers of those individuals. That was reversed in recent years and we've been hiring as fast as we can hire, but we have to maintain high standards. Our job requires an incredible workforce that have the commitment and dedication to do it, and so we are limited on how quickly we can grow in any given year. And so that's why that continued growth is essential. And unfortunately there was a gap in that and some of that has returned with the Fiscal Responsibility Act, again, returning just hard caps. And when you're dealing with hard fiscal caps, it really constrains the room for strategic planning and thoughtful consideration of how to best allocate resources to meet threats.

Nick Schifrin:

Do you believe that limits your ability to provide protection?

Matthew Noyes:

Obviously we are constrained by the resources we have. We do the best we can with the resources we have, but we have been constrained for well over a decade now in terms of resourcing and hiring, and that has a long impact in terms of increasing the staffing to do both of our incredibly important tasks.

Nick Schifrin:

And as I introduced you, you're part of the Secret Services transnational crime division. Is there any indication whatsoever of what you do on a daily basis has anything to do with what we saw in Pennsylvania last weekend?

Matthew Noyes:

Again, there's many journalists in the audience. I appreciate the need to make news, but we're just not well served with any kind of speculation at this point. There's ongoing reviews, they're going to be comprehensive in nature, and so let's let those play out, make sure we have an accurate understanding of every element involved here. Before we do a disservice of speculating on this

Nick Schifrin:

Juergen stock, let me expand the conversation here, whether about Trump, whether about Robert Feso in Slovakia, er, Bolsonaro, he was stabbed. I did a whole story about how many Mexican candidates have been attacked. Shinzo, Abe of course. Do you believe that violence against politicians is expanding and what is the threat there? What are you hearing in terms of that threat, whether it's individuals, lone wolves, terrorists or organized crime?

Jürgen Stock:

Yeah, thank you very much and good morning everyone. Great to be here and represent global law enforcement. Interpol with 196 member countries. I have not been talking to a single police chief around

the world who would've said, I'm sufficiently staffed. I have the resources I need to address all the challenges we are facing. And since I took over office in 2014 at the home of Interpol, the situation definitely has been changing globally in terms of criminal crime, primarily international terrorism, organized crime in all this manifestations, cybercrime, increasingly complex, increasingly international. And that is a challenge also in regards to resource. Of course, understanding that any government, any political leader has competing interests and you will never get it perfect, but at least a shortage of staff. Also, lack of training, lack of necessary capacity is a topic in almost all jurisdictions. First remark, sanctuary mark regarding violence.

I don't have any statistics here, but you have been mentioning prominent examples where political leaders have been targeted in many of these incidents. Investigations are still ongoing where we clearly see statistics going up and there is obviously a rise in violence against political leaders is at the very local level, rural level. It concerns political leaders, it concerns police officer, it concerns members of the fire brigades. It concerns medical teams who are increasingly being attacked while helping protecting our communities. So there is obviously an element that is worth looking into it also from a scientific point of view, what is going on in our communities? And that is a phenomena in many of our societies that violence is increasingly be directed against those who are serving our communities and political leaders 0.1. So there is at the national level, definitely, and we have statistics for that in many Interpol member countries, clearly an increase.

And that obviously also concerns attacks against political leaders. By the way, we also know that organized crime in many parts of the world increasingly is also targeting political leaders. I've been recently visiting Ecuador. We have some examples in South America regarding drug trafficking. We have lots of examples. Interpol is based in Lyon in Europe, the example Sweden, the Belgium, the Netherlands in my home country, Germany. In all these states and beyond, we see two types of crime. First of all, organized crime that tries to maneuver under the radar of law enforcement being silent and infiltrating our societies. That is extremely dangerous. And the second element is violence, open violence against political leaders. So we had the case of the attempted kidnapping of the Belgian Prime Minister, one of the prominent examples, and we can clearly see that also the violence of those who are at the end of the drug supply chain, for instance, are increasingly fighting each other.

So for territory and very often, yeah, this is shooting, this is bombings explosions where we see increasingly a number of victims not only amongst those groups, but also members of the public who suddenly find themselves in such a fight between two gangs. So the clear answer is all the indications we have, it's increasingly a problem. It might also have something to do with increased polarization in our societies, but again, that is something we're also Interpol, is working with the academia trying to find out what we can do in supporting our countries to prevent these incidents from happening. So what are the early warning indicators that maybe give us room to maneuver and working against something that obviously is a trend in many countries around the world. So a concern,

Nick Schifrin:

And Brian Nelson, if that's the trends, can you let us know if there is anything unique about the threat environment because it is 2024 because it is the US election perhaps before what we saw last weekend or maybe enhanced because of it.

Brian Nelson:

I don't know that there's anything particularly unique about 2024 from our perspective, but I do think sort of the trends that we're seeing in the context of so much disruption globally, the fact that obviously we're still actively trying to support Ukraine in the context of a hot war, the fact that there is this ongoing conflict in Israel and Gaza that we see sort of the rise of cyber enabled criminal activity across the globe and sort of the work that we're doing at Treasury is to both think about how we can use our limited resources and authorities to manage as best we can and support our national security and the management of these global crises. But also being pretty hardnosed about the way we prioritize the use of our sanctions authorities, prioritize how we try to identify those financial trends that are going to be most relevant in the context of these crises and help identify for law enforcement, some of the actors and networks and financial flows that support so much, particularly in the context of organized crime, their capacity to engage in violent activity, engage in the type of trafficking of drugs and people and guns that I think we rightly worry so much about here.

And the fact that a lot of this criminal opportunity, frankly is cyber enabled and that is increasingly the case I think has to give us all a lot of pause and concern about the ways in which we can further, as you noted, those networks that are going to be most impactful to our disruptive tools.

Nick Schifrin:

And part of what you just described is what colloquially I would call follow the money. And again, I know you won't be able to engage with anything specific about what happened in Pennsylvania, but in general, are there follow the money questions being asked right now? And again in general, what are the challenges of following the money, so to speak when it comes to apparently a lone wolf?

Brian Nelson:

Yeah, no, look, lone wolfs are very difficult and would largely defer to my FBI colleagues. But oftentimes the transactions that are associated with loan wolf activities are not ones that would necessarily create a suspicious activity report that financial institutions file with our financial crimes enforcement network. They're often low dollar transactions and again, would look like a regular transaction. So of course in this case, we're working very closely with the FBI on their investigation and we'll continue to do so. But this is an area where frankly we have really struggled to send clear guidance to financial institutions about how to look for suspicious activity.

Nick Schifrin: Why is that?

Brian Nelson:

Again, it's just because the types of transactions, low dollar transactions, so not going to trigger using sort of our currency transaction reports. You have transactions purchases that could be used in a way that involves violent activity but wouldn't necessarily be obvious on the front end. And of course suspicious activity actually has to be suspicious in order to generate a report and of buying the types of

materials that a person could use again for attacks is not necessarily going to trigger those types of reports.

Nick Schifrin:

Juergen stock, the title of this panel is essentially a call for us to look around the world and to acknowledge that organized crime not only is about drugs or crime itself, but it is about political stability. Haiti for example, it seems to me brought down in government when it comes to organized crime and as Brian was just talking about, crime is fueled or accelerated by cyber capabilities. So how are organized crime groups, in fact undermining societies?

Jürgen Stock:

That's the \$1 million question. A complex issue as I indicated earlier, because all these crime developments on an international level, at least they are linked to what we very often discussed in the context of the so-called mega trends, migration, food security, climate change, and of course not to forget technology, which perhaps is the most impactful game changer in the international criminal landscape. We could clearly see that during the pandemic where the criminals very quickly shifted to new business models. And that also has been stimulating what we are now discussing in the context of these activities. Fishing, scamming, which is let's say of course, international by nature and the kind of industrial scale commitment of crime, which I have never seen in my long career, that you can, of course you can sit back home wherever you are around the globe and maybe preferably in those areas where you might have weak law enforcement, where you have political instability, where you have a high level of corruption where for instance, these scam centers are settling an interesting combination, interesting, of course not in a positive way but in a negative way, interesting combination between human trafficking to get victims into lower victims into these scam centers.

They're very often again operating in weak areas after the pandemic in casinos and hotels that had to close somewhere in Southeast Asia, but not only in Southeast Asia, but meanwhile all around the globe. And we see victims from Asia showing up in scam centers in South America or from Africa in Southeast Asia. So it's really a global issue. And of course any investigation has a global dimension that makes it difficult because we are still operating based on national jurisdictions and more than ever the threats for our communities are coming from outside our own jurisdictions. We know that the fragmented legal framework and in many of our member countries, there is not a kind of law at all to deal with cyber criminality. It's not a criminal offense in many of our jurisdictions or some of our jurisdictions and discussions are now going on at the UN level to find a kind of basic agreement and to make the fight against this crime more effective.

And in the future, what we are expecting in the discussion this morning on artificial intelligence, synthetic media, I think in the future we might not need, or the criminals might not need these scam centers with maybe 5,000 victims of human trafficking any longer because all these messages are generated automatically with a more efficient business email compromise. So many representatives from the private sector are here, they know what that means. Ransomware attacks more sophisticated from a technology point of view. So this is what we are expecting and it's time again to reconsider our classical approach, whether this is enough. And of course we have to build any, spoke about the need for

collaboration and partnerships this morning to intensify definitely our partnership approach, our preferably global response against these gangs who, despite all the efforts you might see from the news in the media, drugs, 50 tons seized here, 100 tons there.

There is no impact at the front lines of policing. And you see these criminal groups becoming more dangerous, more impactful, more powerful, more influential in all parts of the world. We are currently last remark conducting a study. We try to identify the 10, 15 most dangerous criminal groups in the world. And they are growing because of technology. The new technologies that are now available, they have the resources to invest in these technologies and they properly monitor where the weak spots in international corporation are and place the activities in these areas. So we have to reconsider our strategic approach. And again, partnership is key for that. So we need to build bridges instead of walls between our agencies with the private sector, with the academia. And that also makes such an event like here in Aspen. So important

Nick Schifrin:

Matt, no add what the journalists would call color to this and make it a little more personal. Talk about sextortion, talk about pig butchering, talk about elder fraud. What are those things, especially pig butchering and why is the secret service so focused on it and then make the point of course about how it does go well beyond the shores of the US and so that gets to the challenges that interpols.

Matthew Noyes:

Yeah, first I'd emphasize everything Oregon said. It is a transnational criminal problem. I would say taking a brief step back, a big picture, finance is not just the sin news of war, it's the sin news of the economy of organized criminal activity following the money goes back to the Roman Empire in terms of an investigative strategy to whom the benefit that is where you can have the greatest impact is who is benefiting from the activity and denying their ability to benefit and enjoy that benefit. And that's where criminal law enforcement's role come in, not just in arrest, but also asset seizures as to the criminal cases themselves, they're brutal crimes. They're devastating, they're causing victims of these fraud schemes to commit suicide. We are seeing particularly retired individuals be defrauded, lose their entire life savings. The pig butchering the term comes from the criminals themselves.

That is how they describe their scheme and typically involves a romance element. They're providing a investment tip oftentimes involving crypto. Whether or not there's any crypto actually purchased is a separate question. And they entice the victim that they're getting inside information on a market opportunity. They get them to put in more money, take out loans to invest more money. And to the extent these victims are deceived is heartbreaking, they believe they're in a romantic relationship, they believe they're profiting from these investments. It gets to the point where they will go to their banks, their bank will tell 'em, we think you're a victim of a fraud scheme, don't do this. And sometimes they ultimately allow 'em to conduct the transaction because it's the customer's money and they are concerned about the civil liability. When law enforcement, even our own agents talk to 'em, they're still convinced that they are in a legitimate investment and in a legitimate relationship.

And when they finally realize it, they very much need help. Otherwise, we see these tragic suicides on this extortion multiple elements to it, whether it's enticing young people to send nude photographs to

'em or just other photographs that then digitally altered, put pressure on 'em. We'll share this with your social network unless you pay us again, isolating that victim from that extortion scheme, from their family, from their loved ones to have that impact. And so just from the victim level impact, it's extremely important for us to focus on how we focus on it. We can have the most impact going after the financial streams, which has wide ranging implications. Drug traffickers are using the same money laundering networks. These are poly criminality things. And I would mention on the cyber crime piece, they're increasingly sophisticated, right? Cyber crime in the US is a fraud violation computer fraud and abuse act. It is in most other countries that are signatories to the Budapest Cybercrime Convention. It is a fraud scheme. The interplay of technology and use of the internet in these schemes, deep fakes to make these fraud schemes more convincing is continued to increase. And it really is imperative for cooperation amongst communications companies, both traditional telecoms, social media, but also financial institutions, payment companies to protect their customers from these fraud schemes and that conduct to reduce that activity.

Jürgen Stock:

Can I just support that? Because we recently got access to an interview that was made with one of these victims of such a scam center in Malaysia, and we could see how brutally, I mean you have double victimization. I mean you have those who are tricked into these scam centers thinking about, oh, a nice job opportunity somewhere in another country and they find themselves in circumstances that can only be described as modern slavery. So they are in a kind of jail, they get their passports being removed, they get electroshock, they get been punished and treated in that way. They've been provided with 15 or 20 sim cards and mobile phones, and they have through 20 hours a day they have to do these. And I mean this is industrial scale criminality where obviously the criminals based on language skills, they are scanning country by country, let's say German speaking, English speaking, Spanish speaking, and so on. So industrial scale criminality, which is really a new dimension. And again, that should be considered a national security priority to go against it. And not just domestic crime where, yeah, my grandma is maybe losing 100,000 euro to these scam centers. No, this is organized crime at is worst. And it's destabilizing the trust into those, I mean elements, the internet applications that are very often used, the stating apps, as you said, the WhatsApp and all these channels are being used by the criminals and it's step-by-step eroding trust in the infrastructure that we need. And on the other hand is so beneficial to all of us.

Nick Schifrin:

And Matt Noy, you were briefly referring to this, but why is the solution that Secret Service has found less about arrests and more about stopping the fraudulent financial movements?

Matthew Noyes:

Yeah, so it's two pieces. One, it's the right thing to do to make the victims of these fraud schemes hold. So we prevented over 2 billion of fraud loss last year. We returned over 400 million to victims of fraud through asset recovery. So it's the right thing to do for them, alleviate the impact on 'em. Second, it's a financially motivated crime. Go after the money laundering networks, go after the profitability of it.

That's what drives the scale. That's what allows 'em to invest in the infrastructure. For example, U-N-O-D-C and both US Institute of Peace just published reports this year on the scam call centers in Southeast Asia, Miami, Marley House and Cambodia in particular. That's what allows them to scale these and build them into 3000 person operations and compounds. And so tackling those elements, you can have outsized impact. And we do see the interplay in terms of particularly Chinese organized crime money laundering networks where they're facilitating asset flight from China, also fentanyl, trafficking, fraud, revenue tracking. They are multi elements and it's importantly, this is an area of shared interest. Chinese speaking communities get impacted by these scams. English speaking communities get impacted. And one of the challenging pieces is technology is allowing a broader transnational targeting effectively because they can automate the translation and using deepfake technology to swap faces and video so they can continue these schemes regardless of what culture or language their victim is.

Nick Schifrin:

And Brian Nelson, again, zoom out for us and remind us, drug cartels, international terrorism, these are criminal enterprises. Why are they not only causing the of drugs or guns or violence, but actually increasing regional destabilization?

Brian Nelson:

Yeah, no, I mean I think exactly going back to my initial point about prioritization, really what we've tried to do and President Biden has really directed us to do is think about how corruption drives so much of this criminal activity. And we need to prioritize that as a national security priority here in the United States, and particularly in the context of the illicit finance flows that support all of this activity, recognizing that these bad actors are relying on their opportunity to access those gaps in the US financial system. So doing the work of both closing those gaps, but using our financial institutions to send the trends and typologies and the things that we're seeing in order to hopefully both prevent the victimization and the horrible consequences for those victims, but also to provide meaningful information to law enforcement so that we can actively get after this in a way that relies on partners in a way that ansif, to your point, the partnerships that we have internally.

We have a strike force on fentanyl. We see how these drug trafficking organizations are heavily relying on new forms of fraudulent schemes. Like timeshare fraud is a big problem. We just on Monday sanctioned a number of individuals, did a joint notice to financial institutions with the FBI in our office of Foreign Assets Control because we see that these criminal organizations are really generating quite a lot of financial revenue in support of their trafficking of fentanyl through these schemes. So we have to approach this problem holistically, do the work of closing our own gaps, preventing bad actors from setting up shell companies, for example. And we also have to work with our partners internationally because it's just not the work that we do domestically through information sharing and events like these

Nick Schifrin: Very quickly.

Jürgen Stock:

I like the sentence, I mean, we are internationally in law enforcement. We are cooperating with the speed of law. The criminals are operating with the speed of the internet. So international cooperation, real time exchange of information is key. There are some interesting projects nationally, anti scam centers where people from law enforcement regulators, banking sector are sitting desk by desk 24 7. That is a model that we also have to do, would have to do at a global level going after the money. One remark, the UN is saying 1.7 trillion US roundabout are channeled illicit proceeds of crime are channeled through the global financial sector. Every year the optimists are saying two to 3% are track traced and ceased by law enforcement. Maybe the realists might say less than 1%, less than that. So we get an idea how rich the most dangerous criminal groups in the world are.

Nick Schifrin:

Let me, I only have about five or six minutes Jurgen stock, and I want to ask you something about what a lot of European officials are talking about. There have been public reports about plots to murder a German defense industry executive. There have been attacks on European defense facilities. Now to help the audience here, you are constitutionally forbidden from talking about any or taking any actions in response to the actions of a state. But as we know, as we've been talking about, there is a lot of organized crime aspects to the attacks that I just mentioned. There's a long history of the use of organized crime networks by a certain actor that presumably has been targeting these people and these facilities across Europe. So have threats to European defense industry increased and what can we do about it?

Jürgen Stock:

Thank you for already answering an important part of your question, Interpol was built 100 years ago exactly with a purpose, stay away from politically motivated crime at that time, including terrorism, by the way, which we have changed focus on what is called ordinary law crime. So people who are abusing children, who are trafficking drugs, who are trafficking human beings. That is what we try to do. Of course, not always easy, I think you say a blurred line, but the success of Interpol that we still have all the 196 member countries at the table, that we still bring them into operations where we collect 60, 70, 80 countries to join in for certain operations is because we are handing that very strictly staying away from politics. There are other agencies and organizations who can deal with this. Interpol is focusing on ordinary law, crime, nothing else to say on

Nick Schifrin:

No increased risk to defense industry that you can even discuss.

Jürgen Stock:

I mean, we have been discussing the increasing risks at the beginning of this conversation. There is no doubt that the risks are increasing, but again, it's for our communities regarding organized crime and particularly cyber crime where we have to reconsider our business model also in Interpol in law enforcement away from the classical, just bilateral work or cooperation of the like-minded states. This is not enough to address these threats.

Nick Schifrin:

And then here's another question that you really won't want to answer if you don't want to answer that one. Major technology executives including Elon Musk, who course runs x Peter Thiel, who's still on the board of directors of Facebook, there are others have come out in the last few days as supporting Trump and Vance. Are you concerned that technology companies who seem to be heading toward the Republican ticket today will provide less assistance if that Republican ticket is elected in November?

Jürgen Stock:

I mean, we are in general concerned about technology. Again, those two sides of the coin, let's say that of course always we know how beneficial all these technologies are for development and fighting poverty and so on and so on. But it's, the question is how do you use technology? And we see that criminals are increasingly using that. I really believe that AI will be a huge game changer and we have to be prepared, particularly in terms of prevention because international cooperation with this fragmented system will remain to be difficult. And I'm very grateful that, for instance, the United States have been setting up, and this for me is a role model, global coalition at that time to defeat against isil, a real, I mean 87 states international organizations, nato, Interpol, European Union, the Arab League under one umbrella fighting isil, the counter ransomware initiative that was set up. This is the way we need to go. Truly, almost global solution and technology. We are concerned about encryption. That is something where we are very concerned that we are getting, we are no longer in a position to monitor. What I've been doing throughout my career when I was still investigating is monitoring conversation between criminals if they increasingly use end to end encryption and we have no chance to legally to intercept. We are having a big problem concern. But

Nick Schifrin:

We've been talking about partnerships. You just mentioned the United States being a leader. Are you worried, are you concerned about whether the United States will provide that partnership depending on the outcome of the election?

Jürgen Stock:

Again, I am in this office now for 10 years as Secretary General of Interpol. We always had fantastic support from the United States. We have seconded detailed officer who working in Interpol from the F-B-I-D-H-S and so on. They are supporting many of our projects, capacity building training activities in different parts of the world. And I think together we have been able, that's our mission, making the world a little bit a safer place. For instance, very particularly on mobility of foreign terrorist fighter and so on. And that is the spirit in which we also have to cooperate to mitigate the increasingly relevant cyber risks.

Nick Schifrin:

Fair enough. Brian Nelson, we have 30 seconds. I will let you take us home. Phishing, fakes and fraud tackling transnational crime and enhancing global security. How can this audience, how can the people here enhance global security from your perspective?

Brian Nelson:

Look, you all are leaders, global leaders in thinking about how we can better enhance our partnerships. We are investing in internationalizing a lot of the work that we do. Our financial crime enforcement network starting to send liaisons out into the world. We're trying to move faster. We have a rapid response program to try to get money back to victims with international partners. So we recognize that truly forms like this, help us get the word out to the stakeholders who are best positioned to be able to take meaningful disruptive action in this space.

Nick Schifrin: That one was easy. See, it was,

Brian Nelson: I appreciate it.

Nick Schifrin: Brian Nelson, Juergen stock. Matt Noyes. Thank you very much.