MIKE MALSCH,

FBI SPECIAL AGENT, LEGAL ATTACHÉ WARSAW, POLAND

Mike Malsch talks about new cyberthreats and challenges related to new technologies. He also describes the role of other US institutions and agencies responsible for cybersecurity, FBI priorities and international cooperation.

Kasia Sokół: It is a rare opportunity to be able to talk to the FBI Agent stationed in Warsaw, Poland. Can you, please tell us about your carrier in the FBI?

Mike Malsch: I joined the FBI in 2004. I did not grow up dreaming of becoming an FBI Agent. I am a computer scientist by education and worked professionally as a software developer/ computer programmer for 11 years.

When the horrific events of September 11, 2001 occurred, it caused me to reexamine my career choice. I had never served my country in the military or any other form of public service, so started looking for ways to contribute my skills to the service of my country. After a year of searching and praying, I applied to the FBI. It took nearly 2 years from submitting my application to receiving an appointment to the FBI Training Academy in Quantico, Virginia. I graduated as a Special Agent and began my new career.

Today we face quite a significant deficit of specialist in this area. As an expert in cybersecurity, do you have any suggestion as to what can we do to encourage young people to choose a career in cybersecurity? What would be your message to them?

You are correct – there is a massive need for this type of expertise with cybersecurity challenges increasing daily. You also raise a good point regarding providing encouragement to choose cybersecurity as a career path. Cybersecurity is now a fact of life. So much of our daily interactions involve computer-based applications and systems. We store our schedules, our contacts, our messages, our documents, our music and entertainment, and much more on our devices.

Protecting that information is critical to our safety and security. For that reason, I believe the encouragement must start early with educating kids about not only the use of computers, but also the protection of their information. If kids are brought up respecting the value of their information, they will see the importance of protecting it. As a corollary to this, as a Law Enforcement officer, there is also a certain satisfaction in investigating and bringing to justice those who choose to take information that doesn't belong to them.

Beyond education, there are other incentives to pursuing cybersecurity careers – good salary, job security, constant challenge in solving new problems, and satisfaction in knowing you contribute to the safety and security of others.

You have been in Poland for over two years dealing with all kinds of crimes which ties to the US or just supporting Polish partners.

During my time in Poland, my office has provided support to the Polish Services with regard to cybercrimes and relied on my Polish partners for information to assist with US cybercrimes. We have also supported each other in many other areas. As you probably know, cybercriminals do not respect national borders and are indiscriminate in their targets. Having partnerships around the globe is essential to fighting crime these days. We are privileged to have outstanding partnerships here in Poland.

One of NASK main responsibilities is cybersecurity so if you don't mind I would like to focus on that part of your responsibility.

What are FBI priorities nowadays? Few years ago, combating cybercrime was one of the first five.

While protecting the American people from terrorism—both international and domestic—remains the FBI's No. 1 priority, the FBI's enterprise strategy highlights cyber as one of our highest priorities. Nation-state threats are a top concern for us because of their persistence, sophistication, and potential for destructive intent and cyber criminals deploying ransomware are undoubtedly having the most visible direct impact on US critical infrastructure, including hospitals, the energy sector, and emergency services. We are using our nationwide assets—our presence and our people—

to proactively engage systemically important partners. Not just the well-known big companies but also smaller companies that form the bedrock of our critical infrastructure. We are also integrating engagement into the intelligence cycle. We want to share information quickly with our partners, but we also want them to share the right information back with us, which comes from being open and honest about what our information needs are. We want our partners to be a force multiplier for us and for the country's collective security, as we all take on shared responsibility to defend against our cyber adversaries.

We want partners to know that, especially when it comes to cyber threats, we don't have all the information and that much of it lies with the private sector. We need them to know that we're a trustworthy partner who will act when they point us in the right direction and show us the threats that lurk in systems and networks for which they have the best visibility.

What changes have you noticed as far as cybercrime is concerned, over the last years?

Ransomware is increasingly targeted and lucrative. The number of incidents reported to IC3 in **2020 grew by 20 percent**, but the monetary losses from those incidents grew by **225** percent. These statistics do not include the costs associated with business disruption and remediation, which can dwarf the ransom demand itself.

If there is one thing the FBI understands, it's taking down criminal organizations, and when it comes to ransomware, we are working with an unprecedented number of government and private sector organizations to do just that. Our strategy for countering ransomware, like other complex cybercriminal schemes, is focused on disrupting 1) the actors: identifying key criminals, 2) their infrastructure. 3)their money to make crime less profitable.

Each of these elements is crucial to the fight against ransomware. But we have the most durable impact when we disrupt all three together and when we combine the capabilities and authorities of our partnerships.

Cyber, and cyber incident response is the ultimate team sport. Effective presentation and response effort require an all hands-on-deck approach, and that team much include foreign partnership, the private sector, and even the general public.

For a few reasons, the FBI strongly discourages victims from paying a ransom to criminal actors: 1) paying one is no guarantee that the cybercriminal will decrypt your files or make good on their promise not to do anything with the data they stole, 2) the scale of the ransomware problem flows from the money acting like gas on a fire. We aren't going to get the problem under control until there's at least less gas feeding the flames, 3) also, it's worth noting that when it comes to data theft, we often see actors re-victimizing the same companies again.

That said, we understand to pay or not to pay is a difficult decision. I've spent a lot of time in the private sector helping companies weigh tough decisions—I know how it feels to be pulled in multiple directions, or even sometimes like there isn't any choice but to pay.

What are the main challenges regarding cybersecurity and cyber threats today? What are your predictions for the future?

Nation-state threats are a top concern for us because of their persistence, sophistication, and potential for destructive intent and cyber criminals deploying ransomware are undoubtedly having the most visible direct impact on US critical infrastructure, including hospitals, the energy sector, and emergency services. For years, our adversaries and strategic competitors have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk.

They are now becoming more adept at using social media to alter how we think, behave, and decide. As we connect and integrate billions of new digital devices into our lives and business processes, malicious actors almost certainly will gain greater insight into and access to our protected information.

The recent state of high profile, broadly impactful cyber intrusions like SolarWinds, Hafnium, Pulse Secure, and Colonial Pipeline highlight the investments in time, money, and talent that our adversaries are making to harm us—both nation-states and cyber criminals.

The number and scale of these major incidents is evolving every day and it is challenging our collective ability to respond. Importantly, we don't see criminal vs. nation states as an "either/or." Something that distinguishes the FBI is that we have the authority to investigate and collect intelligence on both criminal and nation-state threats. And what we see through that work is a blended threat, where there is often no bright line where cybercriminal activity ends, and nation-state activity begins. t's probably better to think of malicious cyber activity on a continuum, where you have some cyber criminals contracting for or selling services to nation-states; some nation-state actors using their access and skills to make money on the side; and nation-states using tools and techniques typically used by cyber criminals to obfuscate their activity.

No agency can address as big and difficult a problem as the cyber threat on its own. We sit in the middle of the ecosystem defending the country, with resources ranging from deep private sector connections to the tools of an intelligence service. We're using that broad footprint to investigate adversaries and how to stop them, develop the intelligence we and our partners need to take action, and then move as a community in a joint, sequenced way—hitting actors with everything from arrests, to government and private sector infrastructure takedowns, sanctions, diplomatic pressure, and more for maximum combined effect. Because none of our government's tools function without an identified target to aim at and enough evidence to justify action. We're working against cyber threats in two different ways: 1) Relentless focus on prevention and disruption, 2) and setting aside thoughts about credit and feeding information to the partner best positioned to hit the adversary hardest.

The biggest difference between cyber and other programs are how central a partner the private sector is. We provide companies and academia with a few different kinds of important intelligence—from strategic warning about adversary intentions, to tactical, specific information about indicators net defenders need to protect themselves, to individualized warnings that actors are targeting or actively compromising them. We also rely heavily on what the private sector can tell us about what it's seeing on networks it controls—and which contain nearly all of the critical infrastructure, PII, and intellectual property the FBI works to defend.

How does the FBI contribute to fostering international cooperation and building partnerships in the area of cybersecurity and fighting cybercrime?

Most of our adversaries, and their infrastructure, are abroad, so our global partnerships are vital.

The FBI works closely with other U.S. agencies and foreign partners to successfully leverage resources to target cyberterrorist actors, particularly to prevent any advancement of their capabilities, as well as cyber-facilitated physical attacks against U.S. entities. Through these partnerships, the FBI has successfully disrupted multiple computer network operations campaigns. We take what we learn and share it, as well as our capabilities, with partners, so we can jointly bring all our tools into sequenced operations against the adversary.

As far as international reach is concerned, since cyber has no boarders, the FBI must have a global reach. Cyber Assistant Legal Attaches (ALATs) stationed in embassies around the world have helped build coalitions of like-minded countries to stand with the U.S. against our adversaries. Our ALATs work closely with international counterparts to share information, coordinate action, and seek justice for victims of cybercrime. This program embeds cyber agents with our international counterparts in strategic locations and helps to build trust with key partners around the world.

The FBI can also leverage the assistance of international law enforcement partners to locate stolen data or identify the perpetrator of a cyber incident. For example, we coordinated a global operation to disrupt a go-to service for cyber criminals, the Emotet botnet, which criminals used to gain access to more than a million computers worldwide and sell that access to others, including ransomware groups. By taking coordinated global action, we made it that much harder for the criminals to reconstitute.

Ransomware-specific. We are building new and deeper international cooperation to disrupt the ransomware ecosystem, including by establishing an international counter-ransomware initiative with partner governments to disrupt the financial infrastructure upon which these criminals relay and by engaging face-to-face diplomacy to address safe harbors for ransomware criminals.

Is FBI the only intel/law enforcement agency dealing with cybercrime in the US? Or do you have a threshold or division of competences?

The FBI is the lead federal agency for threat response which means our role is to disrupt and bring pain to our adversaries.

Our investigations focus on developing evidence to discover who the hackers are, where and how they operate, who supports them, and the types of actions that will be most impactful against them. So when we advise or work with the private sector, we're using our knowledge of the threats to look at how a company might be targeted, how their systems may be interconnected, and the best way to guard against the threats they are likely to face. For example, information about the attack vector—or where they think the vulnerable point was that allowed cyber actors to breach the system.

We are fortunate to have two domestic agencies, CISA and FBI, with very different authorities and insights, whose roles complement one another and who, working together, strengthen our defense of cyberspace in ways that could not happen if they were in competition or isolation.

CISA's strength is addressing vulnerabilities within cyberspace, assessing risk, and strengthening the resilience and defense of the .gov and critical infrastructure.

The FBI contributes information it uniquely collects through a combination of criminal and national security authorities that are the envy of many partners overseas, as well as its physical presence across the US that enables their close engagement with entities before something bad occurs and with victims when unfortunately it does.

Once revealed, that information gives CISA the opportunity to identify other networks vulnerable to the same technique; it may give the FBI, CYBER COMMAND, or NSA a piece of the actor's infrastructure to disrupt or exploit; and it helps the National Security Agency know where to focus all the instruments of power the government might bring to bear against those responsible.

No matter where information comes into the government, it's important that CISA and FBI have equal ability to see it and act on it for their respective parts of the mission.

Nothing in the way we organize ourselves will change the FBI's responsibility to investigate computer intrusions and obtain justice for victims by finding who's responsible and holding them accountable.

What is the role of the FBI Internet Crime Complaint Center (IC3)? How can its work and responsibilities have impact on the European cybersecurity ecosystem e.g. in Poland and generally in the EU?

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyberattacks and major criminal threats, and to provide or many partners with services, support, training, and leadership.

The IC3 serves those needs as a mechanism to gather intelligence on cyber and internet crime so we can stay ahead of the threat. It was established in May of 2000 to receive complaints of internet related crime and has received over 6.5 million complaints since its inception.

The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected cyber enabled criminal activity, and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and for public awareness.

To promote public awareness, the IC3 aggregates the submitted data and produces an annual report to educate on the trends impacting the public.

The quality of the data is directly attributable to the information ingested via the public interface, www.ic3.gov, and the data categorized based on the information provided in the individual complaints.

The IC3 staff analyzes the data to identify trends in cybercrimes and how those trends may impact the public in the coming year.

What is the role of the National Cyber Investigative Joint Task Force (NCIJTF) in the US? What is the role of the Bureau within this structure?

To address this evolving cyber challenge, the National Cyber Investigative Joint Task Force (NCIJTF) was officially established in 2008. The NCIJTF is comprised of over 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization's mission from a whole-of-government perspective.

As a unique multi-agency cyber center, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation

The NCIJTF also synchronizes joint efforts that focus on identifying, pursuing, and defeating the actual terrorists, spies, and criminals who seek to exploit our nation's systems.

There are a lot of joint initiatives/bodies in the US with the purpose to share and exchange of information. It seems that you have learnt your lesson after 9.11 but also it proved to be working effective tool. We have mentioned IC3 and NCIJTF.

Can you, please tell us about the National Cyber-Forensic and Training Alliance (NCFTA)?

The National Cyber-Forensic and Training Alliance (NCFTA) was established in 2002 as a nonprofit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cybercrime. The NCFTA focuses on results. By establishing an environment where participants trust each other and freely share information, the NCFTA has been able to prevent nearly $2 billion in potential losses while also helping to identify critical threats to private industry.

The NCFTA also supports global law enforcement efforts by helping to identify current threats, which are most impactful to private industry. The three main areas of focus at the NCFTA are Brand and Consumer Protection, Financial Threats, and Malware and Cyber Threats. The NCFTA endeavors to be a global model for public-private partnership, collaboration, mutual support, and trust without regard to borders or sectors. They intend to continue to meet the needs of private sector, law enforcement, academic, and international partners by expanding relationships, constantly enhancing their operational capabilities, and improving their technical infrastructure.

In your opinion, is it more effective: centralize or decentralize capabilities to combat cybercrime (state vs. federal, and in Poland: regional/voivodship vs. national)?

This is difficult to answer due to the differences in our structure and our legal systems. What I can say is that expertise will develop in a decentralized manner as cybercrime investigators encounter different scenarios in the cases they work. And threats will manifest in a decentralized manner as cybercriminals operate without regard to the structure of law enforcement capabilities. Regardless of the formal structure, flexibility and adaptability remain as the key competencies to combating cybercrime.

How would you define what the greatest risks associated with offenders' exploitation of new technologies? Which of the technologies you think has contributed the most to facilitating crime?

Cybercriminal actors' adoption of new technologies could limit law enforcement's ability to detect, identify, and mitigate against the new TTPs. Cybercriminal actors could see unmitigated success for some time as law enforcement collection and mitigation efforts evolve. Victim reporting may not be able to articulate language defining the new technologies or how they were victimized.

When I think cybecrime and cybersecurity I also think of fake news, misinformation. Does FBI addresses those issues. If so, how?

We are concerned about the future of malicious cyber and foreign influence operations.

The rapid pace of the development of emerging artificial intelligence and machine-learning technologies used to generate synthetic content—images, audio, video, or text—likely will outpace the development of detection and attribution capabilities. Synthetic content may be used in a newly defined cyberattack vector referred to as Business Identity Compromise.

BIC represents an evolution in Business Email Compromise tradecraft by leveraging advanced techniques and new tools. It involves the use of content generation and manipulation tools to develop synthetic corporate personas or to create a sophisticated emulation of an existing employee.

Synthetic content could also be used to target and victimize vulnerable individuals or groups, such as children. This emerging attack vector can have a significant financial and reputational impact on victim businesses and organizations. We have been working with our interagency partners and the private sector to get ahead of this issue.

Several factors have decreased the resources, time, and effort required to create or use convincing synthetic content. This means that methods once limited to those with the necessary computing power and expertise can now be employed by a broader customer base via user-friendly applications. One consequence of this trend is that synthetic content creation has been essentially commoditized and scaled beyond once-limited-use cases. Visual distortions and warping or inconsistencies in images and video may be indicators of synthetic images, particularly in social media profile avatars.

Third-party research and forensic organizations, as well as some reputable cyber security companies, can help identify and evaluate suspected synthetic content.

Familiarity with media resiliency frameworks can help mitigate the impact of malicious cyber and influence operations.

Individuals and organizations can lower the risk of becoming victim to malicious actors using synthetic content by adopting good cyber hygiene and other security measures.

Be aware of the potential for cyber or foreign influence activities using synthetic content; Be alert when consuming information online, particularly when topics are especially divisive or inflammatory; Seek multiple, independent sources of information; Seek media literacy or media resiliency resources, as well as training to harden individuals and corporate interests from the potential effects of influence campaigns. Such resources are often available through public libraries, universities, and nonprofit organizations. Use multi-factor authentication on all systems, especially on shared corporate social media accounts; Train users to identify and report attempts at social engineering and spearphishing, which may compromise personal and corporate accounts; Establish and exercise communications continuity plans in the event social media accounts are compromised and used to spread synthetic content; Do not open attachments or click links within emails received from unrecognized senders.

Do not provide personal information, including usernames, passwords, birth dates, Social Security numbers, financial data, or other information in response to unsolicited inquiries; Be cautious when providing sensitive personal or corporate information electronically or over the phone, particularly if unsolicited or anomalous; Confirm, if possible, requests for sensitive information through secondary channels; Always verify the web address of legitimate websites and manually type them into a browser.

The FBI strongly encourages individuals and organizations who suspect they may have been the victim of a criminal cyber act, or have information about suspicious or criminal cyber activity, to contact their local FBI field office or file a detailed complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov.

We cannot ignore war in Ukraine. I know we cannot talk about details but do you have more work since the war broke out?

Unfortunately, I cannot comment on that. I can only share the following FBI official approved statements related to Ukraine/Russia:

- (*Assistance to Ukraine*) "The FBI is dedicated to investigating and combatting any malicious cyber incidents impacting Ukraine's critical infrastructure. We are working with our partners, domestically and internationally, to identify, disrupt, and deter these targeted cyber threats. Our Legal Attaches in Europe and around the world are playing a key role in supporting and sharing information with our Ukrainian and international partners."

- (*Domestic Threat*) "The FBI, along with our federal partners, remains committed to investigating and combatting any malicious cyber activity targeting the United States. The FBI has consistently disseminated public threat advisories warning about these activities conducted by Russian cyber actors. We continue to proactively share information with our private sector partners to identify targeting and prevent incidents. We encourage the public to report any suspicious cyber activity to www.ic3.gov.

What are the main challenges regarding your job in Poland?

I find the main challenges in this job in Poland to be like the challenges found in any law enforcement job in most other countries, including the U.S.

When working investigations with our partners – we often get bogged down with administrative burdens, outdated policies, and legal restrictions that haven't kept pace with the technological developments in the cyber arena. I am not talking about those things guaranteed by our respective Constitutions – freedom of speech, religion, assembly, press; protection from unreasonable searches and seizures; due process in court; etc. I am talking about burdens with paperwork requirements, policies that apply to older technology but miss aspects of newer technology, and laws which do not provide adequate punishment for criminal offenders. Synchronizing investigative techniques with prosecutorial process and aligning both with judicial outcomes is necessary to succeed in the cybersecurity realm.

Thank you.