INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

Case Study Assignment: The Hushpuppi Investigation A Comprehensive Analysis of International Cybercrime Cooperation

Course Code: ACI202 Assignment

Type: Case Study Analysis Case

Subject: Ramon Abbas (Hushpuppi) Cybercrime Investigation

REG. NUMBER: 2025/ACI/9958
NAME : Ambreena Munir
Date: August 18, 2025
Batch: Batch B2025

Task 1: Comprehensive Case Analysis

1.1 Introduction

Ramon Olorunwa Abbas (born 11 October 1982), commonly known as **Hushpuppi**, **Hush,** or **Ray Hushpuppi** is a Dubai-based Nigerian Instagram influencer, very successful person, fraudster and cybercriminal. He came from modest roots reportedly working as a used-clothing vendor in Lagos, with his father a taxi driver and his mother a bread seller . From a young age, he was involved in cyber scams with the "Yahoo boys" . Dr. Adedeji Oyenuga, a cybercrime expert, explained that these scammers typically used stolen identities to launch romance scams. Abbas followed this path, getting involved in on.

Abbas's operations were built on precision, patience, and trust within his criminal circle. In Business Email Compromise schemes, his team would first compromise a company's email account through phishing or hacking. Once inside, they would monitor real email conversations for weeks or months, waiting for a high-value transaction to be discussed. At the right moment, they would send a fake but convincing payment instruction to the victim, directing the funds to accounts they controlled. In romance scams, the process was slower but same as fake online persons were crafted to appear caring and loving, eventually persuading victims to send money for fake emergencies. The funds were then send through money mules, offshore accounts, and cryptocurrency wallets to make tracing difficult. By using these types of technical hacking skills, social engineering, and money laundering investigators made his network highly effective.

His most commonly used method was Business Email Compromise (BEC), where he and his partners compromise companies into sending money to fake accounts. Victims included a U.S. law firm defrauded of $40 million, a Maltese bank hit for $14.7 million, and even an attempted $124 million scam on an English Premier League football club. In June 2020, Dubai police started a "Operation Fox Hunt 2," and arrested him. During operation they found about 40$ million in cash, 13 luxury cars, and data of over 1.9 million victim email addresses. In 2022 , he was sentenced in the U.S. to 11 years in prison and ordered to repay 1.7$ million.

Ramon Abbas lifestyle became his own downfall. He posted photographs of himself wearing luxury brands, staying in five star hotels, and driving branded cars on instagram. This behavior attracted millions of followers and the attention of investigator. In today's connected world, such displays not only inspire others but also provide investigators with valuable clues about a criminal activities and movements. The case is significant in cybercrime history because it shows how using a social media can expose criminals activities, how international investigators can work together to catch them, and deal with these types of cyber crimes.

1.2 Criminal Enterprise Structure

Ramon Abbas coordinated activities through trusted **associates** and **intermediaries** who managed specific fraud schemes The criminal network operated under a **central leadership model** with Ramon Abbas ("Hushpuppi") at the top..Major scams managed by Ramon Abbas like

- **Money Mules:** Received money from victim and then send into personal or shell accounts, then transferred them to offshore destinations.
- **Hackers:** Breach defenses to gain unauthorized access to computers,phones and IOT devices etc. Hacker also take advantage of weaknesses in networksecurity to gain access . Weakness can be technical and social in nature
- **Co-Conspirators:** Collaborates with two or more individuals in carrying out a conspiracy , sharing the intent and purpose of commetting the illegal act. Carried out phishing campaigns, impersonation, and fraudulent communications.

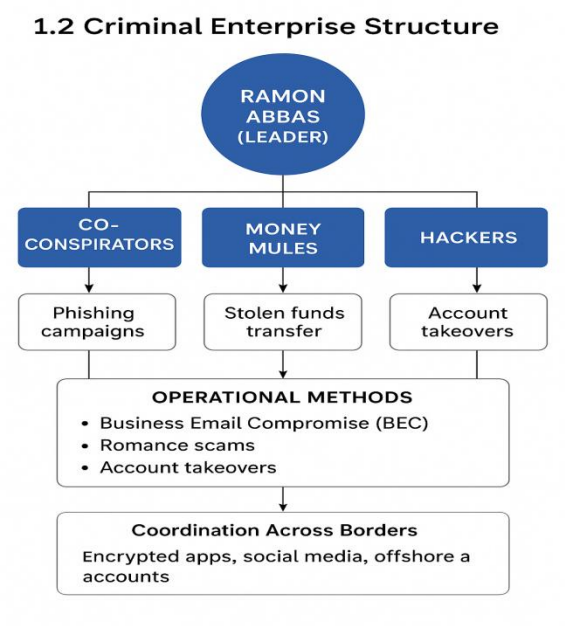
Hushpuppy main operational methods that they used are **Business Email Compromise (BEC):** Impersonating legitimate business contacts to trick companies into wiring funds to fraudulent accounts. **Romance Scams:** Establishing fake romantic relationships online to gain victims' trust and request money. **Account Takeovers:** Gaining unauthorized access to email, banking, and social media accounts for fraud or resale.

Abbas's group worked like a proper organized gang, but instead of controlling streets, they controlled online spaces and tricked people's trust. Even if one person got caught, the others could still keep the scams going. Sometimes they didn't even hack accounts themselves they bought stolen login details from others online. Money mules were often people who didn't

even know they were helping in a crime, as they were told it was just an online job sending payments. Everyone had their own role some handled the hacking, some created fake stories, and some moved the stolen money around.

Abbas personally managed the biggest deals but left smaller scams to other members. His image of being rich and generous kept his team loyal to him.They also broke large money transfers into smaller ones so banks wouldn't get suspicious. Many times, they used cryptocurrency to hide the money trail.

Abbas leveraged his connections in multiple countries, allowing the group to operate across North America, Europe, Asia, and Africa without a fixed base of operations.Investigators though that he was working for North Korea Hackers.The network used encrypted messaging apps (such as WhatsApp and Telegram) and social media platforms for real-time coordination. Stolen funds were moved through offshore bank accounts and cryptocurrency wallets to conceal origins and evade detection.



1.3 Investigation Timeline

Law enforcement agencies first noticed suspicious patterns linked to Ramon Abbas through large-scale **Business Email Compromise (BEC)** fraud reports and unusual money flows involving international bank accounts.The FBI, Dubai Police, Interpol, and other agencies

coordinated intelligence, pooling data from multiple ongoing fraud cases tied to Abbas's network.

Financial monitoring flagged multi-million-dollar transactions linked to shell companies and accounts connected to Abbas's network.Authorities began tracking Abbas's online activities, especially his public Instagram posts showing extreme wealth inconsistent with any declared legitimate income. Search warrants were issued for email accounts, social media profiles, and communication logs. Evidence from victims' reports was linked to Abbass.

Digital experts also checked the background of his Instagram photos and found location tags that proved he was in Dubai. Even small details like reflections in windows were used to confirm where he was staying. Undercover officers joined online chats where his group discussed deals, pretending to be part of the team.

The case against Abbas was built slowly over years. Banks had already reported strange transactions to financial crime units, showing money moving through accounts in different countries before being used to buy expensive items like watches and cars.

Dubai Police conducted **Operation Fox Hunt 2**, raiding Abbas's penthouse at the Palazzo Versace in June 2020. In July 2021, Abbas pleaded guilty to conspiracy to engage in money laundering. They seized **$40 million cash**, luxury cars, and digital devices containing data from over **1.9 million potential victims**. UAE police sent Abbas to US. In **November 2022**, a U.S. federal court sentenced him to **135 months (11 years, 3 months)** in prison and ordered him to repay **$1.7 million** to identified victims.

1.4 Legal Framework

Abbas was sent from the UAE to the United States under a legal agreement between the two countries. This agreement allows them to hand over people accused of major financial crimes, especially when the victims or banks affected are in the country requesting the extradition.

Applicable U.S. Federal Laws:

- **Money Laundering Control Act (18 U.S.C. §§ 1956–1957):** Prohibits individual from engaging in a financial transcation with proceeds that were generated from certain specific crimes known as specified unlawfull activities.
- **Wire Fraud Statute (18 U.S.C. § 1343):**To convict on wire fraud charges , the government must prove beyond a reasonable doubt that the accused person intentionally used some kind of electronic communication, such as phone or email for the purpose of committing fraud.

- **Computer Fraud and Abuse Act (CFAA):** The unauthorized access to computers and systems used in Business Email Compromise (BEC) and account takeovers.Gaining unauthorized access to the system criminal should be punished according to law.

  The U.S. prosecutors first filed charges against Abbas for BEC, wire fraud, and money laundering. . In November 2022, the court in California gave him 11 years and 3 months in prison and told him to pay back $1.7 million. He went to court, was told his rights, and in July 2021, he admitted he was guilty.He is now in a U.S. federal prison and is expected to be released in 2029.

  The UAE is not part of it, but the U.S. is. Even so, its ideas like working across borders, sharing digital evidence, and doing joint investigations were used when U.S. authorities worked with Dubai Police, Interpol, and other agencies in this case.The Budapest Convention on Cybercrime (2001) is an agreement that helps countries work together on cybercrime cases.

Prosecutors used several laws together. The **Wire Fraud Law** allowed them to charge him even if the crime happened outside the U.S., as long as messages or payments went through U.S. systems. The **Money Laundering Law** helped them take away his assets, no matter where in the world they were. This made the case stronger and harder for him to escape.

This case showed how hard it can be to handle cybercrime that happens across countries. The U.S. was able to bring Abbas over from Dubai because most victims and banks affected were in America. Special legal agreements allowed the U.S. and UAE to share electronic proof quickly.

Some experts say this case could be used in the future to go after influencers who show off illegal wealth or help promote scams online.

1.6 Outcomes & Impact

He apologised to his family members for bringing them shame while commending the FBI for doing a thorough job while bringing him to justice.In a final appeal to Judge Otis Wright ahead of his scheduled sentencing on 19 September 2022, Hushpuppi wrote a personal letter to the court narrating his source of wealth, criminal adventure and regrets.

Authorities found around $40 million in cash, 13 luxury cars, branded watches, designer clothes, and digital devices full of evidence.Abbas was sentenced to 11 years and 3 months in a U.S. federal prison and ordered to pay back $1.7 million to his victims. His arrest sent a strong warning to other cybercriminals that even if they operate in different countries, they can still be traced and caught.

In the short term

- the case grabbed global attention

- made cybercriminals more cautious about showing off their wealth online, and showed that social media can be used as evidence.

In the long term

- it encouraged stronger cooperation between countries
- improved intelligence sharing, and inspired new strategies for tackling Business Email Compromise (BEC) and large-scale online fraud.
- It also proved that even high-profile figures with international networks are not beyond the reach of the law.

The case had a big effect on both people and law enforcement. Many young fans saw Abbas as someone who got rich fast, but his arrest made them think twice about that lifestyle. People started talking online about how showing off wealth without saying where it comes from can be a red flag.

For police, it was proof that even criminals who hide in other countries and use technology can still be caught.Companies began using this case in training to show how scams like Business Email Compromise (BEC) work. Some experts even suggested making a worldwide system to track suspicious online money movements in real time.

Banks and companies also became more careful with big payments transcation. Many started asking for people to check and approve any large money transfer.

The Hushpuppi case highlights key lessons for law enforcement, businesses, and individuals in the fight against cybercrime. The Hushpuppi case showed countries that they need to improve cybercrime laws andmore ways to work with other countries.The case shows that cybercrime is not just belong to one country instead it requiring international cooperation between police, intelligence agencies, and private sectors. It proves that no matter how difficult a criminal may seem but cooperation in investigation and global partnerships can bring them to justice. Oversharing personal information on social media can make both criminals and victims vulnerable, as digital footprints often reveal locations , time and related metadat. Business Email Compromise is one of the most financially damaging cybercrimes today, and it can often be prevented with strong email security, two-factor authentication, and staff training to spot suspicious payment requests.

References:

https://en.wikipedia.org/wiki/Hushpuppi

https://www.aljazeera.com/news/2022/11/8/hushpuppi-gets-prison-term-for-money-laundering-conspiracy?

Task 2: International Cooperation Evaluation

The case of Ramon Olorunwa Abbas, also known as “Hushpuppi,” shows how important cross-border cooperation is in fighting cybercrime. Abbas was a Nigerian citizen living in Dubai and running large-scale business email compromise, romantic scams and money laundering schemes. He targeted the victims in the United States, Europe, Malaysia and other regions, using digital networks, banks, and accounts spread across many countries.

Because of this, no single country could investigate, arrest, and prosecute him alone. The FBI in Los Angeles worked with Dubai Police in the UAE, who carried out “Operation Fox Hunt 2” to arrest Abbas and seize evidence in Dubai. Devices, bank records,files and other materials collected in the UAE were shared with U.S. authorities to support the case.

Abbas was sent to the United States through **administrative expulsion**, which was much faster than a formal extradition process. International cooperation also allowed investigators to trace the criminal activities across multiple countries and accounts.

Without this close coordination between the UAE and the U.S., it difficult to reach out the Abbas , he may destroyed important evidence, or continued his crimes. This case proves that cybercrime is truly borderless, and only strong international cooperation can stop it.

Key reasons why cross-border cooperation was important in this case:

- **Jurisdictional Reach** – The FBI in Los Angeles could not go to Dubai and arrest Abbas themselves. Dubai Police in the UAE carried out "Operation Fox Hunt 2," where they did the surveillance, raids, and arrests to catch Abbas and collect evidence in Dubai.
- **Evidence Collection and Preservation** – Dubai Police seized phones, computers, bank records, and expensive items. This evidence was shared with U.S. investigators. Without cooperation between UAE and U.S. law enforcement, most of this evidence would have been hard or impossible to get.
- **Defendant Transfer** – The UAE sent Abbas to the U.S. through administrative expulsion, which was much faster than a normal extradition process. This meant he was in a U.S. court in California only weeks after his arrest.

2.2 Cooperation Mechanisms

In the Abbas case, different cooperation methods were used between the United States and the United Arab Emirates to make sure that the abbas will arrested without removing any evidence. These included formal legal processes, faster administrative actions, and direct law enforcement communication.

Mutual Legal Assistance Treaties (MLATs)

When Abbas's arrest in 2020, the U.S. and UAE did not yet have a formal MLAT , but they still used similar legal methods to share important evidence. Official MLAT was signed between US and UAE in 2022, which will make the process faster and easier in future cases. These legal channels help make sure evidence is properly authenticated and meets the rules for admissibility in court. Through these processes, Dubai Police sent certified copies of bank transaction records, digital evidence and other documents to the U.S. so they could be used in court.

Extradition Agreements

Generally, when someone is in another country, extradition agreements are used to send them to face allegations. In this case, instead of undergoing a long and complex extradition process, the United Arab Emirates chose to remove ABBAS using administrative removal. This meant that he considered him as someone who could no longer live in the country and directly handed him over to the US authorities. This was much faster than the formal extradition and allowed Abbas to remain in American custody within the weeks of his arrest, allowing the delay that could give him time to challenge or block the process. write same as it is

Informal Intelligence Sharing

Before and after the arrest, Dubai Police and the FBI exchanged information directly through law enforcement channels. This included surveillance details, lists of email accounts used in scams, bank account numbers, and data from seized devices. This kind of informal cooperation is faster than formal legal requests because it allows both sides to act immediately. In this case,

it helped Dubai Police plan the raids and also gave the FBI enough information to prepare the criminal charges.

These three cooperation mechanisms worked together to make the case successful—informal sharing allowed quick action, the expulsion got Abbas into U.S. custody quickly, and legal assistance ensured the evidence was strong enough for use in court.

2.3 Multi-Agency Coordination

Following coordinations we discussed bellow

FBI (Federal Bureau of Investigation)

In United State investigation was led by FBIs Los Angeles Field Office. The FBI also prepared the criminal complaint and coordinated with U.S. prosecutors to make sure all the legal requirements were met. Investigators collected evidence from victims in the United States, discovered the money through international accounts, and worked with partners abroad to connect the crimes to Abbas.

U.S. Department of Justice (DOJ)

The DOJ, through the U.S. Attorney's Office for the Central District of California, handled the legal side of the case in the U.S. This included filing charges, presenting evidence in court, and managing the legal process after Abbas was brought to the U.S. The DOJ also worked through its Office of International Affairs to make sure evidence from Dubai could be used in court.

Dubai Police

Dubai Police carried out the actual surveillance, raids, and arrests inside the UAE. In "Operation Fox Hunt 2," they searched Abbas's residence, seized digital devices, luxury goods, and bank records, and detained him. They were also responsible for preserving the chain of custody for the evidence before it was shared with U.S. authorities.

Interpol

Interpol acted as a global link for sharing alerts and intelligence between countries. While Dubai Police and the FBI worked directly together, Interpol channels helped with verifying information, flagging international travel movements, and checking for other linked suspects in different countries.

Joint Operations Planning

The agencies collaborated closely on the operation to ensure everything unfolded perfectly. For instance, Dubai Police had to be clear on the specific evidence the FBI was after, while the FBI needed to have the arrest warrant ready so that Abbas could be handed over without any

holdups. This teamwork in planning helped prevent any slip-ups and ensured that no chance to catch him slipped through their fingers

Secure Communication Channels for Information Exchange

During investigation, agencies used protected communication systems to share sensitive information. This included encrypted emails, secure databases, and direct law enforcement channels to exchange evidence files, bank records, and intelligence reports. Using these secure methods were important to protect the investigation from leaks and to keep the information admissible in court. By working together in this way, each agency is focusing on its strength and maintains continuously, was able to quickly move to arrest from safe communication conduct investigation and then for prosecution without significant delay.

2.4 Diplomatic & Political Factors

The Abbas case was not only about law enforcement - it also included important diplomatic and political views between the United States and the United Arab Emirates. These factors impressed how the case was handled by arrest to prosecution.

US–UAE Diplomatic Relations

The United States and UAE have strong diplomatic and security relations, which smooth

cooperation in the matter. The UAE was ready to help quickly because the U.S. Working with helps strengthen their partnership in fighting international crime. This good relationship made it possible for the Dubai Police to work fast, share evidence and arrange to send Abbas to America without long delay.

Media Influence on Case Handling

The case attracted the attention of heavy media worldwide as Abbas was famous on social media to show luxury cars, expensive clothes and wealth. The news report and video of "Operation Fox Hunt 2" was widely shared by Dubai Police. The public attention put pressure on both UAE and US authorities and to show that they were serious about stopping cybercrime. Media coverage also helped send a message to the public that such crimes would not be ignored.
Media coverage fulfilled two objectives:

1. Public awareness - showing that cyber criminal can be caught even after working from abroad.
2. Reputation Management - Presenting Dubai as a place that actively fights cyber crime instead of sheltering it.

At the same time, meditation meant very little space for mistakes, because any delay or exercise would have been seen quickly by the public and criticized.

Sensitivities Around Public Image of Dubai

Dubai is known as a global business and tourism hub, so its government is careful about its international reputation. Having a high-profile cybercriminal living there could damage this image. By arresting Abbas and cooperating with U.S. authorities, Dubai showed the world that it does not tolerate criminals using its territory for illegal activities. This was important for protecting Dubai’s reputation as a safe and trusted place for business.

Overall, these diplomatic and political factors worked alongside the law enforcement efforts to make sure the case was handled quickly and effectively, while also protecting the public image of both countries.

Political Will and Soft Power

Beyond the law enforcement, the UAE's quick action was also a form of "soft power" - to make the matter international respect and influence. By collaborating with the US, the UAE deployed itself as a responsible partner in the prevention of global crime. This helped the UAE to combat any criticism that its banking or residency system can be used for funds.

2.5 Recommendations for Improvement

While the ABBAS case was successfully handled, the ways of international cooperation in cyber crime investigation are faster and more effective. The following recommendations can help improve future cases:

Evidence Request Processing

In many international investigations, valuable time is lost in waiting for the formal evidence requests to be approved through legal channels. Even if the UAE and the U.S. Hurriedly worked in the matter, but other countries may still take weeks or months to respond. Rapid review and approval processes - especially for immediate cases related to digital evidence - may help the suspects to remove data or prevent money from transferring money before law enforcement.

Standardized Data-Sharing Formats

Different countries and agencies often store and share evidence in different formats, which can slow down analysis. For example, bank transaction records, phone logs or digital forensic data may need to be changed before using. If all agencies agree on general file formats and evidence-reporting templates, information can be shared and analyzed more quickly, without wasting time on technical adjustment.

More Joint Cybercrime Training Programs

Cybercrime technology changes very quickly, and investigators in different countries may have separate skill levels or equipment. Regular joint training programs between countries - especially for cyber crime units - will help all agencies updated on the latest investigation methods, digital forensic equipment and safe communication practices. Simultaneous training also creates confidence between agencies, making cooperation smooth during real matters.

Additional Recommendations

- Use of real -time safe communication platforms for quick coordination during operation.
- Precious-nominated emergency cooperation agreement that allows to share temporary evidence without waiting for full legal paperwork in immediate cases.
- Regular reviews of cooperation successes and failures after major cases, so the lesson can be implemented immediately to investigate the future.

By improving these areas, future cross-border cybercrime investigations can be completed faster, with fewer delays, and with stronger results in court.

Refrences:

https://www.justice.gov/usao-cdca/press-release/file/1292056/dl

https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions

https://www.secretservice.gov/newsroom/releases/2020/07/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds

https://en.wikipedia.org/wiki/Hushpuppi

Task 3: Ethical Analysis and Professional Conduct

3.1 Introduction – Ethical Considerations in International Cybercrime Cases

When it comes to international cyber crime cases, morality becomes even more important because various countries, laws and cultures are included. Investigators and prosecutors are working not only with technical evidence, but also with sensitive issues that affect people's rights on boundaries.The significant challenge in these cases is finding the right balance between catching cyber criminals and protecting personal rights such as privacy and freedom. Any action that are legal in one country can be it possible that it illegal in another country which make ethical thinking at every step.

Although cybercrime often affects multiple victims in various countries, investigators need to work quickly, but still respect professional standards, legal processes and moral values. If they fail to do so, it can damage the trust between nations, damage innocent people, and weaken the fairness of the case.

In short, moral views in cases of international cyber crime are about ensuring justice by respecting laws, rights and cultural differences.

3.2 Ethical Framework Application

When looking at ethical frameworks in international cybercrime cases, three main principles stand out: **proportionality, respect for privacy rights, and professional integrity with impartiality.** These guide investigators and prosecutors so they can do their work fairly and responsibly.

Proportionality Principle

Proportional theory means that the strength of the search methods should match the seriousness of the crime. Investigators should not go beyond what is necessary. For example:

• If a suspect is involved in a small financial scam, it will not be moral to keep them under 24/7 continuously monitoring or monitor all your family equipment.

• On the other hand, if the suspect is associated with a serious crime like a large -scale hacking attack that threatens national security, then strong discovered methods (such as international cooperation, comprehensive digital monitoring, or seizing several equipment) can be justified.

This theory helps to ensure that investigators do not misuse their power. This avoids conditions where someone's entire personal life is exposed to a small crime. Instead, it encourages impartiality only by applying the level of probe which is really necessary

Respect for Privacy Rights

Privacy is one of the most important rights that must be protected in cyber crime cases. Because digital examination often involves individual equipment, accounts and communication records, investigators have access to very sensitive information. Honoring privacy means:

• Collecting only data that is directly related to crime.

• Before reaching individual accounts, using appropriate legal steps like warrant.

• Avoiding contact with personal or family information which is unrelated to investigation.

Honoring privacy also protects innocent people who may be associated with suspects (such as family members, friends, or colleagues), but are not part of the crime. This ensures that the investigation remains appropriate and does not suffer unnecessary damage. Reading through all private conversations or sharing personal photos will be a privacy invasion and will be morally wrong

For example if investigators are looking at Abbas's email, they should only focus on messages associated with alleged cyber crime.

Professional Integrity and Impartiality

Professional integrity means that investigators and prosecutors should always act honestly, carefully and within the law. They should never manipulate, hide or exaggerate to strengthen the case. Whatever they do should be transparent and be able to stand in court.

Fairness means staying neutral and not giving individual feelings or pressure out pressure affecting the probe. For example:

• Investigators should not assume that Abbas is guilty just because of his background or personal beliefs.

• Prosecutors should not only insist for heavy allegations wrongly to win the case.

Instead, their job is to focus on facts and truth. Acting with professional integrity creates public belief in the justice system and ensures that the suspect is treated properly. Even if the offense is serious, investigators should follow respectable, fair and law.

3.3 Privacy & Rights Considerations

In cases of cybercrime, privacy and rights play a huge role as investigation often involves collecting digital data such as email, social media messages, browsing history and stored files. Warrants to focus on two major areas and balance public safety with fixed process and personal freedom. Such information is very personal, so investigators should be extremely careful to respect personal rights while protecting public safety.

Warrants and Due Process in Digital Data Collection

The fixed process means that investigators cannot take or see digital data without following legal procedures. They need to receive a proper authority such as a warrant, before reaching private accounts or equipment. This is important for three main reasons:

1. Protecting privacy: A warrant ensures that only the investigation related data is accessed. For example, if investigators discover Abbas's computer, the warrant should clearly explain what kind of files they are allowed to see, rather than giving them unlimited access.

2. Preventing the misuse of power: If investigators can access someone's data independently, it can cause misuse or unfair targeting. Warrant stops it by making clear rules and limits.

3. Maintaining fairness in court: Evidence collected without a fixed process can be considered invalid in the court. By following appropriate legal steps, investigators ensure that the case remains strong and fair.

In short, warrant and fixed procedure protect individuals from unnecessary infiltration and keep the investigation professional and valid.

Balancing Public Safety with Individual Freedoms

Cybercrime can affect community and sometimes national security, so it is the duty of investigators to protect the public. At the same time, individuals also have rights such as privacy, freedom of expression and protection from unfair treatment. The challenge is getting a balance between these two.

• If too much attention is on public safety: Governments can correct public monitoring or strict monitoring, which can harm the privacy and freedom of innocent people.

• If too much attention is on personal freedom: Investigators may not have enough equipment to prevent severe cyber crimes, such as mass fraud, identity theft, or cyber attacks.

Abbas case is a good example of this balance. Investigators needed to work to protect the society from potential cyber crime, but they also had to ensure that Abbas's rights were not ignored. Ethical practice means using the least intrusion methods that can still achieve the goal of public safety. For example, instead of tracking every aspect of your personal life, monitoring the online activity of the suspect involved in alleged crime.

3.4 Professional Conduct Assessment

The way investigators and prosecutors behave during a cyber crime case are as important as they do technical work. Professional conduct means that they should follow laws, respect moral rules, and should do a lot of work towards everyone involved. In the Abbas case, we can see both examples of good professional behavior and possible areas where mistakes or controversial action can occur.

Examples of Exemplary Investigator Conduct

1. Proper handling of digital evidence

Investigators are expected to maintain a clear series of custody for all digital evidences. This means that when and how evidence was collected, collected, stored, and transferred. If Abbas's equipment and data were handed over with full documentation, hashing and safe storage, it shows very professional conduct.

2. Respected treatment of suspect

Professional investigators treat suspects with fairness and dignity. For example, if Abbas was informed about his rights, was given legal representation, and a respectable question without intimidation, it reflects exemplary behavior.

3. Use of legal procedures (warrant and court order)

Following appropriate legal steps, such as obtaining warrant before collecting Abbas data, is a strong sign of professionalism. This shows that investigators have worked within the law instead of taking shortcuts.

4. Fair and purposeful approach

Good conduct also means avoiding prejudice. If investigators did not give personal opinion, politics, or external pressure does not affect their decision, and prosecutors only brought further allegations supported by evidence, showing integrity and fairness.

These examples highlight the professional side of the investigation, where investigators worked responsibly and morally.

Any Possible Missteps or Controversial Actions

While there are many positive aspects, some actions in the investigation can raise questions or even wrongly seen:

1. Removal of confidential limits

If investigators have accessed the personal data of ABBAS that was not associated with the case (for example, unrelated private messages or family files), it can be seen as a violation of privacy. Even if not intentional, such action can create controversy about whether the investigation was very infiltrated.

2. Excessive use of monitoring

Cybercrime cases sometimes enticing investigators to use extensive monitoring devices. If the monitoring on Abbas was proportional to the suspected crime, the critics could see it as an overache and a moral misunderstanding.

3. Prosecution pressure

Prosecutors can sometimes be very aggressive in demanding confidence, which can be controversial. For example, if the prosecutors exaggerated the severity of Abbas's alleged crimes or used heavy legal dangers to pressurize him to confess to crime, it would not match professional integrity.

4. Issues of transparency

If the evidence was not completely shared with Abbas's defense team or if some investigative steps were kept secret without proper justification, it could increase concerns about fairness. Investigations are often criticized for lack of transparency in moral reviews

3.5 Ethical Dilemmas

Usually cybercrime cases often create situations where investigators and prosecutors face ethical dilemmas moments where there is no simple right or wrong answer and they must carefully choose the most fair and balanced option. In the Abbas case, two main dilemmas stand out: handling evidence from foreign jurisdictions with different privacy laws and deciding between public disclosure and operational secrecy.

Handling Evidence from Foreign Jurisdictions with Different Privacy Laws

International cybercrime cases usually include data that are stored in different countries. Each country has its own privacy laws, and sometimes these laws struggle.

• Dilemma: If investigators collect evidence from another country that allows comprehensive access to personal data, should they use it, even if they have strict privacy security in their own country?

• Example: Suppose Abbas's emails were stored on a foreign server, where local law allows authorities to hand over all the account data without warrant. In the home country of Abbas, however, investigators will require a normal detailed warrant to access such data.

This creates a moral question: Should all data provided to investigators be used, or would they have been allowed themselves under their own legal and moral standards?

A fair and moral approach must honor the strict privacy rules, even if it means collecting less evidence. It prevents investigators from "purchasing" for weak privacy security abroad and shows respect for universal human rights.

Decisions on Public Disclosure vs. Operational Secrecy

Another dilemma comes from deciding how much information should be shared with the public.

• Dilemma: Investigators and prosecutors want to maintain transparency so that the public rely on the justice system. At the same time, a lot of information about the ongoing cyber crime investigation can warn the suspects, highlight sensitive techniques, or even damage innocent people.

• Example: If Abbas was accused of running an online fraud scheme, should the investigators announce the details to warn the potential victims in public, or should they keep them calm until the matter is complete so that Abbas and any partner do not destroy the evidence?

This is a difficult balance.

• If too much privacy is used, the public may feel that investigation lacks transparency and accountability.

• If too much disclosure is done, it can compromise the investigation, reputation of damage, or even puts individuals at risk.

The moral solution is usually a middle path: only required for public safety (such as warning or confirming the victims that an inquiry continues), but keep sensitive technical details or strategies confidential until the case resolves.

References:

https://amigocyber.com/ethical-considerations-in-digital-forensics

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

https://www.indiancybersecurity.com/Understanding-the-legal-and-ethical-considerations-in-cybercrime-investigation.php

https://skillfloor.medium.com/the-ethical-dilemmas-of-cybersecurity-balancing-privacy-and-security-318adcf949a3

https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime

https://en.wikipedia.org/wiki/International_Principles_on_the_Application_of_Human_Rights_to_Communications_Surveillance

Task 4: Technical Investigation Analysis

4.1 Introduction

In the Hushpuppi case, digital forensic was very important because most crimes were made online. He used email, social media and financial platforms to cheat, so investigators had to rely on digital evidence to prove their activities. Digital forensic helped collect data from their phones, laptops and online accounts, so that it could be used in court. Without these methods, it would be very difficult to connect him with crimes, as he used the Internet and digital tools to hide his actions.

4.2 Digital Evidence Collection

In the Hushpuppi case, investigators had to collect several types of digital evidence as most frauds were done online. This included email, financial records and social media activity. Each type of evidence requires a separate method of collection to ensure that it was accurate, reliable, and can be used in court.

Email Tracing (Headers and Server Logs)

Email played a big role in fraud schemes. Investigators discovered the email header, showing details like the sender's IP addresses, used servers and time tickets. This helped them to link email directly to Hushpuppi and their colleagues. The server log was also investigated to confirm where the emails came from and whether fake accounts were used. One of the challenges here was that cyber criminals often use VPN or fake domains to hide their actual

space. To solve this, investigators compared several email headers, saw the pattern, and requested data directly to email providers through legal channels.

Financial Data Extraction (Bank and SWIFT Records)

Since crime belonged to financial fraud and money laundering, bank records were major evidence. Investigators collected Swift transfer details, bank account details and transactions history. It shows how stolen money was taken to various accounts and countries. This data was difficult to collect as it included collaboration with many banks in various courts. To overcome this, investigators used mutual legal aid treaties (MLAT) and worked with international agencies to achieve official access to financial data. Once received, the forensic accountant analyzed the flow of money and added it back to the luxury purchase of Hashupppi.

Social Media Evidence Preservation

Social media was another important source of evidence, as Hushpuppi often posted pictures of his expensive lifestyle, luxury cars and designer clothes. These posts were used to show that their property does not match any valid income source. To preserve this evidence properly, investigators used forensic tools to capture positions, metadata and timstamps without changing anything. The screenshots alone were not enough, so official data requests were sent to platforms such as Instagram and Snapchat to collect account records. A challenge here was that criminals sometimes remove positions, but investigators preserved them quickly using forensic capture tools and provider backup.

4.3 Forensic Methodology

While working on a cyber crime case such as Hashupppi, investigators must follow strict forensic methods to ensure that evidence is valid in court. If the process is not followed properly, defense can challenge evidence as incredible. In this case, the main focus was on a series of custody, hashing and verification, and handling of across the border.

Chain of Custody

The series of custody is the record that shows the evidence at every step. In the case of Hushpuppi, digital evidence such as laptops, phones and online records was carefully documented. Every time an investigator collected or transferred evidence, his name, date and reason had to be written. This stopped the claims that evidence changed or tampered with. Without a proper range of custody, even strong evidence could be rejected in court, so this step was important.

Hashing and Verification of Evidence

To prove that digital evidence was not changed, investigators used hashing techniques. A ish value is like a digital fingerprint for a file. For example, when he created a forensic copy of Hushpuppi's phone, he created a hash for the original and copy. If the value matches, it meant

that the copy was accurate and there was no change. This method assured the court that the data shown (email, chat, or financial records) was real and was collected during investigation.

Cross-Border Evidence Admissibility

One of the biggest challenges was that Hushpuppi's crimes and data were spread in many countries. His email, bank accounts and social media were hosted in various courts. To accept this evidence in court, investigators had to follow international agreements such as Budapest Convention on Cyber Crime and use official requests such as mutual legal aid treaties (MLAs).By working with international partners and respecting local privacy laws, prosecutors ensured that evidence could legally be presented in the US court. If evidence was collected without a proper authority from a country, it can be consider illegal.

4.4 Technical Challenges

The Hushpuppi investigation faced many technical problems because the crimes were complex and spread across different platforms. Investigators had to deal with issues like data being stored in multiple countries, encrypted communications, and cloud-based evidence. Each of these created unique hurdles that needed careful solutions.

Data in Multiple Jurisdictions

A big challenge was that Hushpuppi's data spread to many countries. His email account, bank transactions and social media data were hosted on servers in various fields. Each country has its own privacy and data-sharing laws, which slowed down and difficult to reach the record. To solve this, investigators used mutual legal aid treaties (MLATS) and international cooperation structure to achieve legal access. This process was about to take time, but ensured that evidences were collected methodically and it could be used in court..

Encrypted Communications

Hushpuppi and his colleagues sometimes used encrypted apps and communication devices to hide their messages. Encrypted chat is difficult to intercept because they are designed to protect privacy. Investigators faced the difficulty of finding other ways to crack the encryption or get interaction. To address this, they used device forensic (extracting data directly from seized phones and laptops), as well as metadata analysis to track when communication occurred. Even if the entire content of encrypted chat is not always good, the pattern in communication helped create the case.

Cloud Storage Evidencet

Another major challenge was that some data were stored in the cloud, such as files, records and backups associated with Hashupappi's accounts. Cloud data is difficult because it is not bound to a physical device and can move between different servers around the world. This raised questions about jurisdiction, privacy and data integrity. Investigators sent an official request to the cloud service providers to control it, who supplied verified copies of data along with metadata and timestamps. He also used forensic protection equipment to ensure that evidence was captured without changes.

4.5 Technology and Tools

In the Hushpuppi case, investigators used many different techniques and equipment to collect, analyze and verify digital evidence.While these devices were very effective, they also had some limitations. Each tool had a special role, from collecting open-sources intelligence to deep forensic analysis.

OSINT Tools (Maltego, Whois)

Open-source intelligence (Osint) was important to map the online appearance of Hushpuppi. Tools such as Maltego helped investigators connect domains associated with email addresses, phone numbers and fraud activities. Open Source Intelligence (OSINT) is the collection and analysis of data gathered from open sources to produce actionable intelligence. Open source data is any information that is readily available to the public, such as information on social media, news articles, and government reports.
Maltego is a graphical link analysis tool that lets you visualize connections within complex data sets, displaying interconnected links. It can be used to identify relationships that might otherwise not be obvious, making it a valuable tool for investigative purposes by journalists, government agencies, and cybercrime units

Digital Forensic Software (EnCase, Cellebrite)

To properly analyze Hushpuppi's devices, forensic software was necessary. Encase was used for disk imaging and file recovery, ensuring that no evidence was missed by the laptop or hard drive. Cellebrite was particularly useful for extracting data from HushPupPi's smartphone, including removed messages, contacts and app data. These devices made it possible to recover hidden or erased files. A range, however, is that some modern apps use advanced encryption, which these tools cannot always break without cooperation from the provider.

Blockchain Analysis Tools

When seeking a blockchain analysis solution, it's important to choose one with substantial depth, breadth, and quality of coverage along with connections to real-world entities — if the data is wrong, it doesn't matter what other functionality the tool possesses.

Since some money laundering included cryptocurrency, blockchain analysis equipment was also used. These devices helped detect suspected cryptocurrency transactions and followed the flow of funds in the wallet. They can identify the transfer pattern and link the wallet for the exchange where the criminals tried to cash. While blockchain analysis is powerful, the limit is that criminals can use privacy coins or mix services to make the trace hard. Nevertheless, a combination of blockchain analysis with traditional financial records gave strong evidence to investigators.

Refernces:

https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions

https://www.justice.gov/usao-cdca/press-release/file/1292056/dl

https://en.wikipedia.org/wiki/Digital_forensics

https://en.wikipedia.org/wiki/Digital_evidence

https://en.wikipedia.org/wiki/Digital_forensic_process

Task 5: Lessons Learned & Future Implications

5.1 Introduction

Hushpuppi (ABBAS) case matters a lot for the future of cyber crime investigation because it shows how online crimes are not limited to a country today, but are spread all over the world. The case also proved that digital evidence is now the most important part of modern investigation. From Instagram post to financial records, evidence of almost every proof was collected online. This shows that the future investigation will depend even more on advanced digital forensic, blockchain tracing and international cooperation. Abbas used social media, email and international banks to fraud millions of dollars. It worked together in various countries to prove that cybercrime could not be solved alone by an agency.

Another reason is that this case is important that it exposed the balance between catching criminals and protecting people's privacy. The case also reminded the investigators that cyber criminals often live luxurious lifestyle that can attract attention. By showing money online, criminals inadvertently make digital trails.The methods used here gave lessons about how investigators can be professional, moral and fair, while still effective.

It is also shown that cybercrime rely on not only companies but also on digital systems. The victims included business, individual and even football clubs, proving that no area is safe.

5.2 Key Lessons Learned

Importance of multi-agency cooperation

Activity conducted through the internet and other networked digital systems represents an increasingly important front for national and international security and crime-fighting. One of the most problematic issues in cyber security is the lack of cooperation and coordination amongst organisations to monitor, detect and react to attacks. Recently, cybercrime has become a primary security challenge . Most cyber offenders target the private entities, and the police are only able to track such individuals after obtaining a report from the victims . Furthermore, the investigating officers rely on the information provided by the victims to apprehend the criminal .

The Hushpappi case revealed that no country or agency can fight cyber crime alone. Abbas committed fraud in the US and Europe while living in Dubai, which made the case very complicated. The FBI, Interpol and Dubai Police all worked together to track it. This proves that teamwork among agencies is one of the strongest equipment against global cybercrime. Such cooperation also helps in sharing skills and technology. For example, the Dubai Police had advanced monitoring tools, while the FBI specialized in financial offenses, and the two strengthened the case simultaneously.

Value of OSINT and social media monitoring

In today's modern age driven by digital innovations, the widespread adoption of technology has transformed criminal activities, leading to the emergence of cybercrime as a significant challenge for law enforcement agencies globally. Cybercrime acts have left a considerable dent on criminal activities and nowadays that we are halfway into the subsequent technological era stands as one of the most crucial issues for law enforcement agencies all around the globe. The aim of this work is to discuss the relationship between cybercrime and organized crime and the importance of OSINT within criminal investigations in supporting law enforcement itself.

Another big lesson is how useful can be OSINT. Abbas himself shared a lot on Instagram, where he posted pictures of luxury cars, designer clothes and expensive hotels. Osint is cheaper and effective than expensive undercover operations. This proves that sometimes criminals highlight themselves more than expected.This simple but powerful monitoring helped law enforcement their identity and help them to add their money to fraud Investigators used these positions to confirm their lifestyle and track their movements. For example, her Instagram stories often gave clues about her exact location in Dubai. . It shows that social media is not only for communication, but also a rich source of evidence on carefully monitoring. .

Speed of asset freezing

The case also highlighted the need to freeze the stolen money quickly. Abbas and his colleagues transferred money through banks and fake companies at high speed.Osint is cheaper and effective than expensive undercover operations. This proves that sometimes criminals highlight themselves more than expected. In a plot, he tried to steal $ 100 million from a Premier League Football Club. If investigators had not worked rapidly to freeze bank accounts and detect transfer, most of the money would have disappeared in different countries or converted into cryptocurrency.With the property of the cold, criminals can easily change money to crypto or transfer it to countries with weak laws, making the recovery almost impossible. This example suggests that financial coordination and early assets are important to reduce the cold deficit and protect the victims. 

5.3 Best Practices

Early international engagement

Publics in 24 countries around the world are generally more inclined to believe their country should pay more attention to problems at home rather than focus on international concerns. A median of 55% across these nations say their country should pay less attention to problems in other countries and concentrate on problems domestically, while 43% say it is best for the future of their country to be active in world affairs.
Cybercrime does not stop at borders, and criminals like Abbas work in many countries at the same time. By attaching international partners such as Dubai Police, FBI and Interpol, investigators made the operation smooth and rapidly.One of the strongest lessons from the Hushpuppi case is the importance of involving international partners at the beginning of an inquiry.In his case, he was living in Dubai, cheating against people and companies in the United States and Europe, and carrying money throughout Africa and Asia. If only the investigators of one country tried to handle it alone, the matter would have failed. Late starting often gives criminals enough time to avoid or destroy evidence. Initial teamwork avoids such risks.

Continuous training for investigators

Those involved in investigations should have a baseline understanding of how to approach an investigation. Generally, internal investigations will concentrate on fact finding and establishing the facts and circumstances, and avoid reaching conclusions on the firm's or individual's culpability or legal liability. Those managing an investigations' team, or teams, need to have the skills and knowledge to exercise critical oversight in order to adequately direct and challenge investigations.

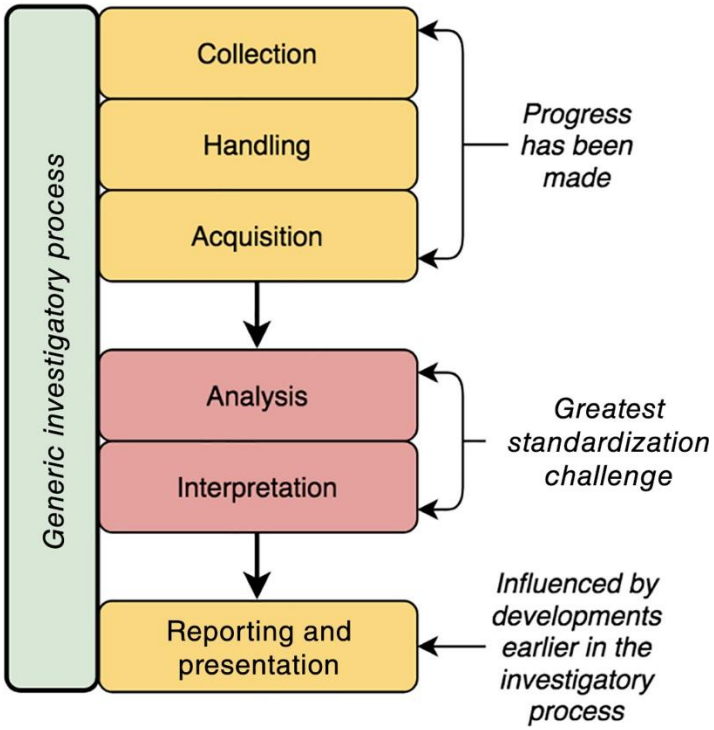
Similarly, financial investigation training helped find out the movement of funds across the boundaries. Training should include not only technology but also cultural knowledge as criminals work in areas and use language tricks to fool the victims.Regular training helps investigators understand new techniques, learning updated equipment and identify new patterns of fraud.This proves that continuous training is not optional, but is necessary, if investigators want to be ahead of global cyber criminals. For example, in this case, training under social media supervision allowed investigators to use Abbas's own Instagram post as evidence.

Adoption of standardized forensic protocols

The need for the standardization of operational practices in digital forensics has seen much discussion. There are clear benefits for digital forensics if its procedures can be harmonized including increasing the reliability of the work produced by its practitioners, consistency of practice, and the potential for greater quality control, however, attaining standardization is a difficult task, and further work in this field is required.

This case shows why standardized forensic protocols in countries are very important. If each country follows the same process to collect and preserve evidence, it becomes easy to share

and accept it in court. For example, a phone data has been seized in Dubai and then the U.S. By verifying the same hash, it was proved that the evidence was unchanged. It is suggested that whilst all efforts to support standardization are valued, focus could be turned towards attempts to standardize parts of the investigative process in more detail. Whilst there are many proposed frameworks which outline a standardized investigatory process, the field requires further work which concentrates on standardizing those actions which occur within each stage.



.5.4 Future Implications & Trends

Growth of BEC scams

According to the FBI's 2022 Congressional Report on BEC and Real Estate Wire Fraud, BEC is "one of the fastest growing, most financially damaging internet-enabled crimes." In 2021, claimed losses exceeded $2.4 billion, a 566% increase since 2016, according to the Internet Crime Complaint Center (IC3). Cases of BEC are expected to rise given the increase in remote work and, by extension, the ubiquity of digital communication channels like email.

The Hushpuppi case showed how powerful trade email agreement (BEC) scams could be. Abbas and his group cheated companies for sending fake emails to companies to send millions of dollars. BEC attacks rely on a human-to-human connection, as opposed to digital tools like malware or viruses. As a result, BEC are difficult to detect or prevent with traditional security tools, such as antivirus solutions or endpoint detection and response (EDR).

Increased use of crypto in laundering

Cryptocurrencies are anonymous at their point of creation therefore the placement stage of the money laundering process is often absent. It only takes a few seconds to create an account ("address") and this is free of cost. It is only possible to use each account twice: to receive money and then transfer it elsewhere. It is possible to create a large money laundering scheme with thousands of transfers at a low cost and to execute it using a computer script.Due to rapid increases in exchange rates, with some cryptocurrencies showing 10,000% growth, it is very easy to justify unexpected wealth through cryptocurrencies.

Another tendency that will continue to grow is to use cryptocurrency to loot money. In the past, Abbas and his colleagues transferred money through fake companies and traditional banks, but many new cyber criminals prefer to use bitcoin or other digital currencies. The reason is simple: cryptocurrency is sharp, works beyond the boundaries, and can sometimes hide the identity of the sender and the receiver.

Greater reliance on AI in investigations

The rapid advancement of artificial intelligence (AI) technologies has implications for every sector of society, including the criminal justice system. As AI tools for investigation, adjudication, prioritization, analysis, and decision-making proliferate and evolve, understanding their potential benefits and risks becomes increasingly important.In June 2024, the Council on Criminal Justice (CCJ) convened a group of experts and stakeholders to discuss the implications of AI for the U.S. criminal justice system. The meeting brought together a diverse group of three dozen leading stakeholders from across ideologies, disciplines, and sectors of the system—policymakers, practitioners, researchers, technologists, and advocates—for two days of discussion and the examination of three use cases.

In the future, cases such as Hushupppi can be rapidly examined as AI can automatically add social media posts, financial records and communication patterns. However, AI also brings challenges. Criminals can start using AI for their own scams, such as making fake sounds or videos (deepfec) to trick people. This means that investigators will have to use AI not only to detect crimes but also to protect against AI-operated scams.

5.5 Policy & Regulatory Recommendations

Stronger cross-border cybercrime treaties

The international community concluded its final negotiations at the United Nations over an international cybercrime treaty. The treaty—now set to go to a vote before the UN General Assembly—is intended to align the cybercrime laws and investigatory police powers of its state

parties. The negotiation process revealed deep fault lines within the global community about the role of human rights in the digital age.

The Hushpappi case proved that cyber crime cannot be resolved by a country alone. Abbas operated from Dubai, targeting victims in American and Europe, and transferred money through banks in Africa and Asia. Without international cooperation, the matter never succeeds.

For example, cooperation between Dubai Police and FBI was successful in the matter, but such a team work should become a standard exercise globally. New agreements should also include modern issues such as cloud data, cryptocurrency and social media evidence, so that no safe area for cyber criminal is present.

Mandatory KYC (Know Your Customer) for financial platforms

Compliance with KYC regulations are required to establish the legitimacy of a customer's identity and identify their risk factors. KYC, which means "Know Your Customer", is the process of verifying customer identity and assessing risk. While individual organizations design their own programs, banks, credit unions, and other financial institutions must meet strict regulatory standards to stay compliant.

One of the biggest problems in cybercrime is how criminals carry forward the money without found. Abbas and his group used bank accounts, shell companies and other tricks to rob millions of dollars. Today, with the rise of cryptocurrency exchanges and online payment platforms, it is even easier for criminals to hide its identity if proper checks are not done.KYC regulations affect nearly any business, platform, or organization that opens accounts or processes transactions through a financial institution. These rules were designed to prevent financial crimes like money laundering, terrorism financing, and fraud, many of which rely on anonymous or poorly verified accounts.

Improved global cybercrime reporting systems

Right now, reporting systems are different in every country, and not all victims know where or how to report cybercrime. A global platform supported by agencies like Interpol may allow companies and individuals to report immediately fraud, no matter where they are. This system can then consume banks, payment platforms and investigators worldwide to prevent investigators from transferring stolen money.

Another lesson from the case is that the victims often report crimes, or in the wrong place, which causes delays. In BEC scams, as long as a company finds out that money has been stolen, criminals have already transferred it to several accounts. If there was a fast and global cyber crime reporting system, authorities can work more quickly to freeze accounts and recover

money.Such a platform will not only accelerate the investigation, but will also create strong global awareness about the dangers of cybercrime. The report should be centralized so that the victims do not waste time in contacting the wrong authority. A single portal can save millions in stolen funds.

Refernces:

https://www.businessinsider.com/fbi-used-hushpuppis-instagram-to-charge-him-with-money-laundering-2020-7

https://www.theguardian.com/law/2022/nov/08/influencer-ray-hushpuppi-jailed-money-laundering-ramon-abbas-fbi

https://www.justice.gov/usao-cdca/press-release/file/1292056/dl