

**Table of Contents**

[**1. Welcoming letter 3**](#_1j12nqtzny4x)

[**2. Introduction to the committee 4**](#_p9vsxbk551s9)

[2.1 Historical Background 4](#_y2gaoekjfk1d)

[2.2. Functions and Powers. 5](#_w73fgo1twrr)

[**4. Topic A: Financial fraud assessment: LockBit cybercriminal group 10**](#_p7u1obk8jca3)

[4.1 Introduction to the topic 10](#_no9fswtrtm6t)

[4.2 Historical context 11](#_qf61qidut2u1)

[4.3 Current situation 13](#_ukc1y6o9p6to)

[4.4. Previous resolutions 14](#_nahxy149emin)

[4.5. Guiding questions 15](#_j3hgoc6sx1yb)

[4.6. Recommendations to the delegate 16](#_3k3x71f9e5re)

[4.7. Support links 16](#_bkmw0bc66oyh)

[4.8. Glossary 17](#_rtrj0jxdnygw)

[**5. List of Delegations 19**](#_g5u9hhg9ap4q)

[**6. References 20**](#_vqwaubssg615)

# 1. Welcoming letter

Dear Delegates,

Allow us, Juliana Bedoya and Maximiliano Montoya, the privilege of extending our warmest greetings as your presidents for the Interpol Committee, Version XV.

To say that we are merely delighted to lead you in this commission would be an understatement. The depth of our enthusiasm exceeds mere words. We recognize that this committee presents a unique challenge, with its own distinctive protocols and operational methods. However, it is precisely these attributes that make it an unparalleled opportunity for each of you to showcase your true potential as delegates.

Within these UN models, between the vibrant exchanges of ideas and perspectives, lies the stage for you to excel. This is where your arguments can ascend to new heights, where you can distinguish yourselves amidst a heightened level of complexity within the UN models and with the best of delegates. Therefore, we encourage each of you to push beyond your limits, to strive for excellence in every discourse, and to emerge from this experience with a profound sense of accomplishment.

UN Models serve as a platform for future leaders, a nexus where the world's changemakers converge. As your presidents, it is our aspiration to nurture and guide you along this transformative journey. Our aim is to facilitate an environment wherein you not only offer the best versions of yourselves but also acquire invaluable skills that will serve you well beyond these halls.

With that said, we invite you to embrace this challenge wholeheartedly. Let us together endeavor to make every moment count, to leave no stone unturned in our pursuit of excellence. For in doing so, we not only elevate ourselves but also contribute to the collective advancement of our global community.

Welcome to the Interpol Committee, Version XV. Let us embark on this journey together, resolute in our commitment to making a difference.

Warm regards,

Juliana Bedoya Maximiliano Montoya

316 7505787 316 5867074

President President

# 2. Introduction to the committee

## 2.1 Historical Background

Our full name is the International Criminal Police Organization and we are an intergovernmental organization. We have 196 member countries, and we help police in all of these countries working together to make the world a safer place.

To do this, we enable nations to share and access data on crimes and criminals, and we offer a range of technical and operational support.

The INTERPOL was created in 1914 when police and lawyers from 24 countries first got together in Monaco at the first International Criminal Police Congress (14 to 18 April 1914), to discuss identification techniques and catching fugitives. For more than 100 years, police across the globe have been cooperating to prevent and fight crime.

After the First World War, the idea of an international police body was revived by Johannes Schober, President of the Vienna Police. The International Criminal Police Commission was established in September 1923, with headquarters in Vienna. The 4th General Assembly in Amsterdam adopted a Resolution that each member country should establish a central point of contact within its police structure; this was the forerunner

of today's National Central Bureau. These specialized departments were established to deal with criminal records, currency counterfeiting and passport forgery. In 1932, new statutes were established creating the role of Secretary General. The first Secretary General was the Austrian Police Commissioner Oskar Dressler.

Belgium led the rebuilding of the Organization after the Second World War with a democratic process to elect the Executive Committee. The Headquarters moved to Paris, France. In 1947, the system of color-coded notices was created, and it expanded over the years to cover other alerts. Nowadays, the Red Notice for wanted persons remains a key tool for international security.

While some of the basic crimes remain unchanged over the years (Eg. murder, robbery), other crimes have followed technological, economic and sociological developments in our world (such as cybercrime and people smuggling).

Additionally, the very first initiatives to discuss extradition procedures, identification techniques and record keeping are still at the heart of the role of the international police up until today. Locating fugitives remains a core activity, biometrics have replaced paper fingerprints, and databases contain millions of global records of criminal data.

The committee began as the International Criminal Police Commission, created in 1923, and became the International Criminal Police Organization-INTERPOL in 1956.

## 2.2. Functions and Powers.

Interpol empowers law enforcement agencies to make a long-term difference to their national security. It also provides police with the knowledge, skills, and sustainable tools needed to meet today’s challenges. Interpol offers investigative support, such as forensics and assistance in locating fugitives around the world, as well as coordination support for on-the-ground operations.

Interpol has a broad area of intervention helping countries to fights the following crimes:

● Corruption

● Counterfeit Currency And Documents

● Crimes Against Children

● Cultural Heritage Crime

● Cybercrime

● Drug Trafficking

● Environmental Crime

● Financial Crime

● Firearms Trafficking

● Human Trafficking

● Illicit Goods

● Maritime Crime

● Organized Crime

● People Smuggling

● Terrorism

● Vehicle Crime

● War Crimes

The Interpol works to achieve Seven Global Policing Goals as uprising security challenges increasingly threaten sustainable development. These Goals were created to address a range of issues related to crime and security. The Interpol Global Policing goals are expected to be achieved by 2030, jointly with the United Nations Sustainable Development Goals due to their capabilities and the power they hold. Not only that but the UNSDG it's the oldest international law enforcement police organization in the world. The Seven Interpol Global Policing goals consist of:

● Counter the threat of terrorism

● Promote border integrity worldwide

● Protect vulnerable communities

● Secure cyberspace for people and businesses

● Promote global integrity

● Curb illicit markets

● Support environmental security and sustainability

The International Criminal Police Organization does not work like common law-enforcement agencies and state forces. The International Criminal Police Organization works as an administrator and source to member countries giving database assistance. INTERPOL’s analysis systems are a tool to fight international crimes. The Interpol works under each member’s existing laws, and in the spirit of the “Universal Declaration of Human Rights”- as stated in its constitution. Therefore, under the Interpol’s Constitution article 3 declares that “it is strictly forbidden to undertake any intervention or activities of a political, military, religious or racial character.” (ICPO-INTERPOL, 1956, p. 3) Therefore, the Interpol must remain politically neutral.

The databases of the Interpol are a network that offers to member countries information about all the areas of intervention of the organization’s working 24/7/365. These databases hold information about organized crime networks, firearms trafficking, stolen property (art, vehicles, vessels), travel and official documents (counterfeit and documents), forensics, and individuals. The main database and the most important in the organization is The Notices system.

The Notices work under the colored notice system of the Interpol, that are alerts of

fugitives, allowing members to share crime-related information. In most cases the notices are private, but in some cases they are published to request help from the public. The color notifications are:

Red Notice:

To seek the location and arrest of a person wanted by a legal jurisdiction or an international tribunal seeking his/her extradition. 

Yellow Notice:

To help locate missing persons, often minors, or to help identify people who are unable to identify themselves.



Blue Notice:

To collect additional information about a person’s identity, location or activities in relation to a crime.



Black Notice:

To seek information on unidentified bodies.



Green Notice:

To provide warning about a person’s criminal activities, where the person is considered to be 

a possible threat to public safety.

Orange Notice:

To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.



Purple Notice:

To seek or provide information on modus operandi, objects, devices and concealment 

methods used by criminals.

INTERPOL–United Nations Security Council Special Notice: Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees. (INTERPOL, 2022)

# 

# 4. Topic A: Financial fraud assessment: LockBit cybercriminal group

## 4.1 Introduction to the topic

Transnational financial crime has grown exponentially in recent years, undermining global financial systems, impeding economic growth and causing huge losses to businesses and individuals worldwide. Corruption adds to the complexity of the problems, creating a fertile ground for organized criminal activities. This is where financial fraud assessment for countries comes into play. Financial fraud assessment its a critical tool for governments to identify and address weaknesses in their financial systems, safeguarding national wealth and promoting economic well-being. It is a national financial checkup, proactively seeking out vulnerabilities before they can be exploited. This type of crime has been boosted by the use of technology, which has been exploited by criminals to reach more people. Also technology boosted the facilities that make the process of cybercrime faster and in a more anonymous way. The use of Artificial Intelligence (AI), large language models and cryptocurrencies combined with phishing- and ransomware-as-a-service business models have resulted in more sophisticated and professional fraud campaigns without the need for advanced technical skills, and at relatively little cost. LockBit is a highly dangerous ransomware group that has become a major cyber threat worldwide. Operating as a Ransomware-as-a-Service (RaaS), LockBit develops and distributes malicious software that encrypts victims' data, rendering it inaccessible. Known for its aggressive tactics and global reach, LockBit poses a significant risk to individuals, governments and organizations alike. LockBit employs a range of attack methods, including phishing, exploiting vulnerabilities, and brute-forcing passwords to gain access to systems. Once inside, Lockbit encrypts critical files, demanding a ransom for decryption. To maximize pressure, they often steal data before encryption, threatening to leak it publicly if the ransom isn't paid.

## 4.2 Historical context

In the Mid- 2000s there was a significant rise in online banking and the adoption of digital payment methods. Consumers embraced the convenience of these new technologies, unknowingly creating vulnerabilities in the financial landscape. Traditional banks, accustomed to physical security measures, were challenged to adapt their cybersecurity protocols to this evolving digital environment. When late 2000´s online banking gained traction, there was a general increase in cyberattacks targeting financial institutions. These early attacks often relied on brute-force methods, attempting to directly breach security systems through hacking attempts. While the exact origin of LockBit remains shrouded in mystery, it's generally accepted that the group emerged in late 2019. The initial version of the ransomware was relatively basic, focusing on file encryption and ransom demands. Early attacks primarily targeted smaller businesses and individuals, with ransom amounts typically in the thousands of dollars. The release of LockBit 2.0 in early 2020 marked a crucial turning point. This release was a significant improvement in the ransomware's capabilities, making it much more powerful and difficult to remove. Some of LockBit 2.0's primary features were:

* Improved encryption: Making files unrecoverable by using increasingly complex encryption techniques. As a supplementary form of extortion, data exfiltration involves stealing confidential information prior to encryption.
* Sites that publish stolen data: when the victims are unable to pay the ransom.
* Better infrastructure for command and control: Making it more difficult to sabotage the group's activities.

These developments in LocBit’s software, make them go from being a small but dangerous threat to a significant international cybercrime organization.

In 2022, more specifically in September, a LockBit attack targeted Rio Tinto, a major global mining company, causing disruptions to its operations. Then, in October, LockBit claimed responsibility for an attack on Siemens Energy, a German multinational conglomerate, disrupting its operations and leading to significant financial losses.

In 2023, the first months of the year were tough. LockBit didn't seem to take a break.

January: The Royal Mail, the UK's national postal service, fell victim to a LockBit attack, causing widespread disruptions to mail delivery and online services.

February: A massive wave of ransomware attacks targeting VMware ESXi servers worldwide was attributed to LockBit, affecting thousands of organizations.

April: Perdue Farms, a major U.S. poultry producer, suffered a LockBit attack that disrupted its operations and led to product shortages.

## 4.3 Current situation

In recent months, LockBit has experienced severe condemnations. The operations of the cybercriminal group are being significantly disrupted by law enforcement agencies across the globe (FBI, Europol, and NCA). The infrastructure was seized, important individuals were arrested, and the ransomware belligerent group has been severely damaged.

Law enforcement has dealt significant attacks to LockBit. The arrest and indictment of alleged leader Mikhail Astamirov in February 2024 marked a major victory. International cooperation has been crucial in dismantling the group's infrastructure and hindering its operations. Additionally, financial sanctions have limited LockBit's resources, making it more difficult to sustain its criminal activities.

Nevertheless, LockBit is still strong, and it continues to threaten the security of any type of organization with lack of cyber protection. Organizations must remain vigilant and maintain harsh cybersecurity defenses to protect against LockBit and other ransomware threats.

Interpol's collaboration with other law enforcement agencies and cybersecurity organizations has been vital in disrupting LockBit's operations and mitigating its impact.

International organizations are uniting to stop the spread of cyberattacks made by these hackers and it has seemed to reduce them. The group's agility and the constantly changing cyber threat landscape makes it difficult to stop them, but not impossible. Governments and businesses around the world must maintain constant awareness and implement proactive defense plans that may be resolved in this committee.

## 4.4. Previous resolutions

There is not a specific resolution for this type of financial fraud cyber crimes caused by LockBit. Still there are some international organizations that have made initiatives in order to fight against this problem. These initiatives are:

* The United Nations Convention on Cybercrime: It establishes a legal framework for cross-border collaboration in cybercrime investigation and prosecution.
* Budapest Convention on Cybercrime The objectives are to increase international collaboration and criminalize particular types of cybercrime.
* Global Cyber Security Forum: An international forum for talking about problems with cyber security and working together to find solutions.
* Programs for Building Cybersecurity Capabilities: The United Nations, the Organization for Security and Cooperation in Europe (OSCE), and the European Union are just a few of the organizations that provide assistance to nations looking to strengthen their cybersecurity capacities.

These frameworks and initiatives to fight against cyber financial fraud, are a strong foundation to combat this problem. The international community has to look up for new solutions, plans, and agreements that are updated to the new threats.

The INTERPOL has been a crucial actor in the combat against cyber criminal gangs like LockBit, providing operational support to member countries, such as assistance with investigations, arrests, and asset seizures related to ransomware groups. The Interpol raises awareness about the threat of ransomware and provides guidance to individuals and organizations on how to protect themselves.

## 4.5. Guiding questions

1. Has your country been affected by cyber financial fraud? How?
2. Has your country had a similar cyber threat to its national security? If so, how was it resolved?
3. Has your country helped with any of the investigations or prosecutions related to the fight against LockBit? How effective has that help to other countries proven?
4. Does your country have any enterprises / companies that have been attacked by LockBit?
5. Has your country contributed to the interpol or any other organization by sharing information to facilitate the pursue and elimination of LockBit and other cybercriminal groups?
6. Has your country suffered or been affected indirectly by any of the attacks done by LockBit?
7. How does your country protect its national databases to prevent ransomware?
8. Are there any specific cases of enterprises that have been attacked by LockBit in your country?Which ones are they, and to what extent were they affected?

## 4.6. Recommendations to the delegate

Even though this topic is centered around LockBit attacks and its ransomware abilities, we expect you to find new ways to combat cybercriminal groups (not only LockBit). This is a problem that concerns national security, threatening the databases, finances and government files. Governments should also put some effort, so that big companies in their countries do not suffer any of these kinds of attacks affecting their citizens. If your country has been directly affected by financial fraud, more specifically LockBit, we recommend you look up the cases and study them ,so you share first hand in committee what has been done in your country to prevent and stop these cybercrime activities.

If your country or any company in it hasn't experienced ransomware attacks, we recommend you to center your research on how your country protects its government from these attacks and how it has contributed to the international community and the Interpol to find solutions. An example could be an Interpol notice to pursueLockBit and other cybercriminal groups. Also, we recommend that you look up how your countries protect the companies in it.

## 4.7. Support links

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a#:~:text=LockBit%20ransomware%20operation%20functions%20as,conduct%20ransomware%20attacks%20using%20LockBit>

<https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation#:~:text=In%20a%20significant%20breakthrough%20in,damaging%20their%20capability%20and%20credibility>.

<https://stonefly.com/blog/lockbit-ransomware-inside-the-cyberthreat-and-defense-strategies/#:~:text=into%20the%20attack.-,Conclusion,has%20enabled%20it%20to%20proliferate>

<https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group#:~:text=LockBit%20ransomware%20attacks%20targeted%20thousands,pounds%2C%20dollars%20and%20euros%2C%20both>

<https://www.justice.gov/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group#:~:text=In%20the%20period%20between%20January,ransomware%20group%20in%20the%20world>

## 4.8. Glossary

1. Ransomware-as-a-Service (RaaS): Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.
2. Phishing: Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
3. Cryptocurrencies: Cryptocurrencies are digital tokens. They are a type of digital currency that allows people to make payments directly to each other through an online system. Cryptocurrencies have no legislated or intrinsic value; they are simply worth what people are willing to pay for them in the market.
4. Cybersecurity: Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.
5. Database: A database is an organized collection of data stored in a computer system and usually controlled by a database management system (DBMS). The data in common databases is modeled in tables, making querying and processing efficient.
6. Data exfiltration: Data exfiltration—also known as data extrusion or data exportation—is data theft: the intentional, unauthorized, covert transfer of data from a computer or other device. Data exfiltration can be conducted manually, or automated using malware.
7. Cybercrime: Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.
8. Decryption: Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system.
9. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.
10. NCA: The National Crime Agency, also known as the NCA, is a crime-fighting law enforcement agency responsible for leading the UK's fight to cut serious and organized crime.
11. Legal framework: The rules, rights and obligations of companies, governments, and citizens are set forth in a system of legal documents called a legal framework.
12. File encryption: File encryption is a way of encoding files, including the sensitive data they contain, in order to send them securely. The encoding prevents unauthorized access and tampering by malicious actors. It keeps a file from being read by anyone except the person or people for whom it was intended.

# 5. List of Delegations

* United Kingdom of Great Britain and Northern Ireland
* United States of America
* Russian Federation
* People's Republic of China
* French Republic
* Federal Republic of Germany
* Republic of Italy
* Canada
* Commonwealth Australia
* The Republic of Singapore
* Republic of the Philippines
* State of Japan
* The Republic of Korea
* The Republic of Iraq
* Syrian Arab Republic
* Hashemite Kingdom of Jordan
* United Mexican States
* Kingdom of Spain

# 6. References

**References**

Ababakr, A. (2022, September 5). (PDF) The Reasons Behind the Rise of ISIS: An Analytical Perspective. ResearchGate. Retrieved September 9, 2024, from <https://www.researchgate.net/publication/363272011_The_Reasons_Behind_the_Rise_of_ISIS_An_Analytical_Perspective>

Alam, M. S. (2023, June 13). Conflict Among Terrorist Groups in South-East Asia - A Case Study of Jemaah Islamiyah and ISIS. التحالف الإسلامي العسكري لمحاربة الإرهاب. Retrieved September 4, 2024, from <https://www.imctc.org/en/eLibrary/Articles/Pages/article13062023.aspx>

Al Qaeda vs. ISIS: Goals and Threats Compared. (n.d.). Brookings Institution. Retrieved September 4, 2024, from <https://www.brookings.edu/articles/comparing-al-qaeda-and-isis-different-goals-different-targets/>

Appendix D – Statement of Reasons – Jemaah Islamiyah (JI). (n.d.). Parliament of Australia. Retrieved September 9, 2024, from <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Completed_Inquiries/pjcis/AQAP_6%20terrorist%20orgs/report/appendixd>

Appendix D – Statement of Reasons – Jemaah Islamiyah (JI). (n.d.). Parliament of Australia. Retrieved September 9, 2024, from <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Completed_Inquiries/pjcis/AQAP_6%20terrorist%20orgs/report/appendixd>

Barton, G. (n.d.). Jemaah Islamiyah: Radical Islamism in Indonesia – NUS Press. NUS Press. Retrieved September 9, 2024, from <https://nuspress.nus.edu.sg/products/jemaah-islamiyah>

CJTF-OIR History. (n.d.). Operation Inherent Resolve. Retrieved September 9, 2024, from <https://www.inherentresolve.mil/WHO-WE-ARE/History/>

Country Reports on Terrorism 2019 - United States Department of State. (n.d.). State Department. Retrieved September 9, 2024, from <https://www.state.gov/reports/country-reports-on-terrorism-2019/>

The COVID-19 pandemic has propelled digital transformation and shown the opportunities that exist for infrastructure to transform developing countries, accelerate their recovery, and increase growth. With these opportunities, there are also serious risks t. (n.d.). World Bank. Retrieved September 4, 2024, from <https://www.worldbank.org/en/programs/kodi/brief/supporting-countries-in-building-cybersecurity-and-resilience-of-critical-infrastructure>

Cybercrime - Crimes. (n.d.). Interpol. Retrieved September 4, 2024, from <https://www.interpol.int/Crimes/Cybercrime>

Digital Currencies | Explainer | Education | RBA. (n.d.). Reserve Bank of Australia. Retrieved September 4, 2024, from <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>

Financial crime – don't become a victim! (n.d.). Interpol. Retrieved September 4, 2024, from <https://www.interpol.int/Crimes/Financial-crime/Financial-crime-don-t-become-a-victim>

guide, s. (n.d.). A guide to ransomware - NCSC.GOV.UK. Retrieved September 4, 2024, from <https://www.ncsc.gov.uk/ransomware/home>

Harmouch, S. (2024, March 28). Moscow terror attack showed growing reach of ISIS-K – could the US be next? The Conversation. Retrieved September 9, 2024, from <https://theconversation.com/moscow-terror-attack-showed-growing-reach-of-isis-k-could-the-us-be-next-226570>

How ISIS recruits its members. Global Affairs. (n.d.). University of Navarra. Retrieved September 9, 2024, from <https://en.unav.edu/web/global-affairs/como-recluta-el-isis-a-sus-miembros>

International investigation disrupts the world's most harmful cyber crime group. (2024, February 20). National Crime Agency. Retrieved September 4, 2024, from <https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group>

Islamic State East Asia. (n.d.). Australian National Security. Retrieved September 4, 2024, from <https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/islamic-state-east-asia>

Jain, S. (2023, November 7). What is Database? GeeksforGeeks. Retrieved September 4, 2024, from <https://www.geeksforgeeks.org/what-is-database/>

Jemaah Islamiyah | Islamic militant organization. (n.d.). Britannica. Retrieved September 9, 2024, from <https://www.britannica.com/topic/Jemaah-Islamiyah>

Jemaah Islamiyah (JI). (n.d.). Counter Extremism Project. Retrieved September 9, 2024, from <https://www.counterextremism.com/threat/jemaah-islamiyah-ji>

Jemaah Islamiyah: Still Southeast Asia's Greatest Terrorist Threat – DASPR. (n.d.). DASPR. Retrieved September 4, 2024, from <https://daspr.org/jemaah-islamiyah-still-southeast-asias-greatest-terrorist-threat/>

Jemaah Islamiyah - Wikipedia. (n.d.). Wikipedia, the free encyclopedia. Retrieved September 9, 2024, from <https://en.wikipedia.org/wiki/Jemaah_Islamiyah>

Kidnapped by ISIS: Failure to Uncover the Fate of Syria's Missing | HRW. (2020, February 11). Human Rights Watch. Retrieved September 9, 2024, from <https://www.hrw.org/report/2020/02/11/kidnapped-isis/failure-uncover-fate-syrias-missing>

Law enforcement disrupt world's biggest ransomware operation | Europol. (2024, February 20). Europol. Retrieved September 4, 2024, from <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>

LAWLESS, J., & CHAN, K. (2024, February 20). Ransomware group LockBit is disrupted by a global police operation that includes 2 arrests. AP News. Retrieved September 4, 2024, from <https://apnews.com/article/lockbit-ransomware-website-police-disrupt-0297653ddfc245fcdf7d9308c6c1e6fe>

Lockbit Ransomware: Inside The Cyberthreat And Defense Strategies. (n.d.). StoneFly Inc. Retrieved September 4, 2024, from <https://stonefly.com/blog/lockbit-ransomware-inside-the-cyberthreat-and-defense-strategies/>

Maizland, L. (n.d.). Jemaah Islamiyah (a.k.a. Jemaah Islamiah). Council on Foreign Relations. Retrieved September 9, 2024, from <https://www.cfr.org/backgrounder/jemaah-islamiyah-aka-jemaah-islamiah>

McCary, I. J. (2024, March 21). The Islamic State Five Years Later: Persistent Threats, U.S. Options - United States Department of State. State Department. Retrieved September 9, 2024, from <https://www.state.gov/the-islamic-state-five-years-later-persistent-threats-u-s-options/>

More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown. (2021, November 26). Interpol. Retrieved September 4, 2024, from <https://www.interpol.int/en/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown>

National Crime Agency. (n.d.). GOV.UK. Retrieved September 4, 2024, from <https://www.gov.uk/government/organisations/national-crime-agency>

Poushter, J., & Manevich, D. (2017, August 1). ISIS and Climate Change Seen as Top Threats Globally. Pew Research Center. Retrieved September 4, 2024, from <https://www.pewresearch.org/global/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/>

Recursos. (n.d.). Cipher. Retrieved September 4, 2024, from <https://www.cipher.com/pt_BR/recursos>

Shahbazov, F., & Slavin, B. (2024, June 6). Is ISIS Reviving in Iraq? • Stimson Center. Stimson Center. Retrieved September 9, 2024, from <https://www.stimson.org/2024/is-isis-reviving-in-iraq/>

Timeline: the Rise, Spread, and Fall of the Islamic State. (n.d.). Wilson Center. Retrieved September 9, 2024, from <https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state>

Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group. (2024, July 19). Department of Justice. Retrieved September 4, 2024, from <https://www.justice.gov/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group>

Understanding Ransomware Threat Actors: LockBit. (2023, June 14). CISA. Retrieved September 4, 2024, from <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>

Watson, M. W. (n.d.). The Conflict with ISIS: Operation INHERENT RESOLVE, June 2014–January 2020. U.S. Army Center of Military History. Retrieved September 9, 2024, from <https://history.army.mil/html/books/078/78-2/index.html>

What is Cybercrime and How to Protect Yourself? (n.d.). Kaspersky. Retrieved September 4, 2024, from <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>

What is Cybersecurity? (2021, February 1). CISA. Retrieved September 4, 2024, from <https://www.cisa.gov/news-events/news/what-cybersecurity>

What is Data Exfiltration? (n.d.). IBM. Retrieved September 4, 2024, from <https://www.ibm.com/topics/data-exfiltration>

What is File Encryption and What Does it Mean? | Box, Inc. (2021, October 28). Box Blog. Retrieved September 4, 2024, from https://blog.box.com/what-is-file-encryption

What Is Phishing? (n.d.). Phishing.org. Retrieved September 4, 2024, from <https://www.phishing.org/what-is-phishing>

Wood, G. (2015, March 15). What ISIS Really Wants. The Atlantic. Retrieved September 4, 2024, from <https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/>

Wouters, P., & Small, H. (n.d.). The History of ISI and the work of Eugene Garfield. Clarivate. Retrieved September 9, 2024, from <https://clarivate.com/the-institute-for-scientific-information/history-of-isi/>

Zelin, A. Y., & Winter, I. (2024, March 20). One Year of the Islamic State Worldwide Activity Map. The Washington Institute. Retrieved September 9, 2024, from <https://www.washingtoninstitute.org/policy-analysis/one-year-islamic-state-worldwide-activity-map>

Legal documents. (n.d.). Interpol. Retrieved May 6, 2024, from <https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents>

What is INTERPOL? (n.d.). Interpol. Retrieved May 6, 2024, from <https://www.interpol.int/Who-we-are/What-is-INTERPOL>