Houston Area Model United Nations
Specialized Committee

INTERPOL



Chair | Manizah Ahmad
Topic A: Combating International Ransomware Networks
Houston Area Model United Nations 52
February 4 & 5, 2027

Atilgan Ozdil/Anadolu Ag

Chair Letter

Hello Delegates,

Welcome to HAMUN 52 (and in my opinion the coolest committee), INTERPOL! My name is Manizah Ahmad, and I am thrilled to be your chair for this year's conference!

I'm currently a sophomore pre-med student at the University of Houston majoring in Business (yes I'm somehow balancing accounting spreadsheets and organic chemistry because why not?!!). This will be my second time staffing for HAMUN and the INTERPOL committee. My journey with Model UN began in high school, and it became an activity that essentially pushed me outside of my comfort zone. Through MUN, I've learned the importance of and how much goes into understanding an issue from perspectives different from your own; a skill that has served me well beyond individual conferences.

I chose to chair INTERPOL because it provides a unique opportunity to explore international issues at the intersection of law enforcement and transnational crime. As delegates, I hope you challenge yourselves to look beyond obvious solutions and consider what can actually be implemented by governments, law enforcement agencies and international organizations.

A few words of advice: Come prepared, but be willing to think on your feet. Don't be afraid to speak up and approach delegates you disagree with, because some of the best ideas come from finding common ground. Most importantly, enjoy the conference! Whether you have been doing MUN for years or this is your first time, I hope INTERPOL gives you the opportunity to learn something new, meet great people, and leave with memories you'll want to talk about long after our time together ends. If you ever have any questions please do not hesitate to reach out!

I'm looking forward to meeting all of you and seeing what you bring to the committee. Best of luck, and I'll see you at conference!

Manizah Ahmad
Chair of INTERPOL
mahmad36@cougarnet.uh.edu



Background Information

History:

The International Criminal Police Organization (INTERPOL) was set up in order to strengthen cooperation among police forces worldwide and to fight transnational crime. Originally, the International Criminal Police Commission was founded in 1923 in Vienna, Austria as a result of talks concerning international police cooperation, criminal identification and extradition. In 1956, the organization adopted its present Constitution and transitioned to the current name. Since it is the largest international policing body, INTERPOL links law enforcement agencies in almost every country by means of secure communication, the sharing of intelligence, and coordinated operations. It helps its member states deal with offences that go beyond national frontiers, such as terrorism, cybercrime, human trafficking, financial crimes, drug trafficking, environmental crime and organized criminal networks. Even though INTERPOL has no authority to make arrests, it plays an important role in helping with international investigations, publishing wanted person notices and assisting with cross-border law enforcement activities. As transnational crime continues to develop, INTERPOL is committed to promoting international cooperation, improving public safety and helping its member states to deal with new global security threats.

Mandate: To promote the widest possible international police cooperation between all member countries, strictly within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights.

Topic A Context

Ransomware is a type of malicious software that renders people or organizations unable to access their files, data, networks or computer systems until a ransom is paid. In recent times, the malware has been used to steal data and threaten to expose or sell it if the ransom is not paid. This new form of extortion is referred to as double extortion, and the consequences of an attack can extend far beyond financial gains. Businesses that fall victim to such extortion could be forced to shut down due to a loss of goodwill and the inability to continue operating. The entities involved in cyber extortion could be located in different jurisdictions, for instance, the perpetrators, the servers hosting the ransomware, the business attacked, and the financial systems that facilitate the ransom payment. This jurisdictional complexity can impede investigations, particularly when it comes to collecting digital evidence and identifying anonymous perpetrators. One of the emerging trends that make ransomware attacks even more challenging is the recent proliferation of ransomware as a service. Under this business model, ransomware developers sell their expertise and infrastructure to perpetrators, thus, evading responsibility for their actions and creating opportunities for anonymity. As a result, states and private entities must invest significantly in tracing perpetrators, particularly those evading responsibility for creating and distributing the malware.

The ransomware crisis requires a concerted effort that goes beyond cybersecurity measures and involves police investigations, financial regulations, private sector partnerships, and critical infrastructure protection. INTERPOL can play a critical role in facilitating international cooperation and coordination between law enforcement agencies, financial regulators, and private entities by supporting information sharing and intelligence analysis. However, the responsibility for investigating and prosecuting ransomware-related crimes rests with individual states.

Topic A Case Examples:

WannaCry Ransomware Attack

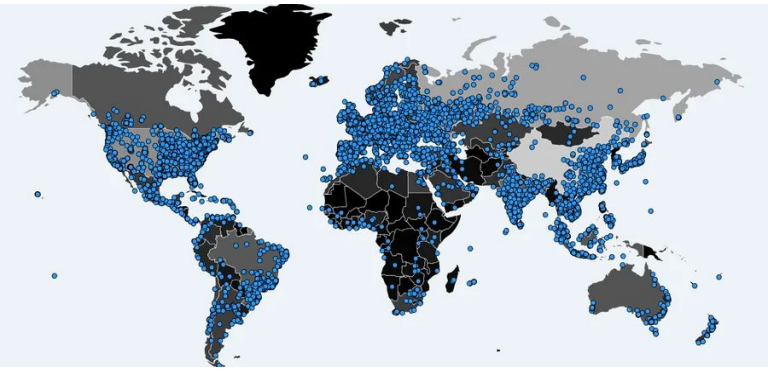
In May 2017, WannaCry, a type of 'ransomware' which works by encrypting files and requiring ransom payment for its removal, began infecting and encrypting files stored on computers worldwide. Using vulnerability in Microsoft windows, WannaCry ransomware would self-propagate within an organization's computer network. Within a short period of time, the attack affected over 200,000 computers across 150+ countries.

In the UK, approximately 80 of the 236 NHS (National Health Service) hospital trusts suffered disruption either due to being infected or having to close systems as a precaution. The NHS estimated that almost 20,000 appointments and operations had been cancelled, while 5 emergency departments moved some patients to other hospitals. Businesses, manufacturers and public institutions were similarly affected, although it should be noted that the attack was not directed against the NHS.

Microsoft had released a security patch to address the specific vulnerability that WannaCry exploited, but many companies failed to apply this critical software update. Ultimately, a cybersecurity researcher discovered a 'kill switch' that could halt further spread of the malware, and the European Cybercrime Center at Europol, working alongside the various national cybercrime units and private sector partners, coordinated an effective international response. But there has never been a new international treaty addressing these events. Instead, we saw a demonstration of existing cybersecurity practices, including national-level response procedures, and how global actors, particularly law enforcement and tech companies, work together internationally on such issues. The consequences of the attack went beyond financial losses, as patients had to wait for their care, healthcare workers were forced to use alternative methods, and the organizations incurred costs related to restoring their systems and enhancing their cybersecurity. The affair also brought to light a difficult policy issue since even when security updates are available, institutions may lack the funding, staffing, or operational flexibility needed to install them promptly.

While a strict requirement to update systems may have a positive effect on security, carrying out the implementation can be difficult for organizations that use older technology or systems which cannot be easily taken offline.

WannaCry shows that preventing ransomware attacks relies on being prepared beforehand. Delegates should think about the ways in which states can promote timely security updates, backup systems, and incident-response planning while also helping organizations with limited resources to meet these requirements. They should likewise consider how INTERPOL can aid in the sharing of information and the conducting of investigations across borders while at the same time ensuring that national agencies and private organizations remain responsible for protecting their own systems.

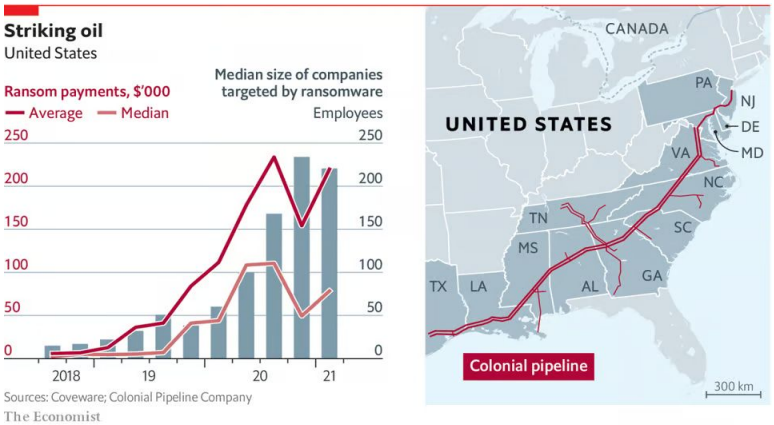


[6] Worldwide computers infected by WannaCrypt ransomware.

Colonial Pipeline Cyber Attack

On May 7, 2021, Colonial Pipeline disclosed that it had been the subject of a ransomware attack by the DarkSide cybercrime group. Colonial Pipeline runs a major fuel transport system in the United States and had to put part of its infrastructure out of action due to the attack, which lead to concerns about the fuel supply and to disruptions throughout the eastern United States. The FBI stated that the DarkSide ransomware was what had caused the breach. As a result, Colonial Pipeline paid a ransom of about 75 bitcoins. A month later, the U.S. Department of Justice announced that it had seized 63.7 bitcoins, the value of which at that time was approximately $2.3 million, and said that this amount consisted of funds traceable to the ransom payment.

The response was the product of coordination between the company affected and various U.S. government agencies, including the FBI and the Department of Justice. The FBI looked into the network breach while the Justice Department dealt with the cryptocurrency connected to the ransom payment. The seizure showed that it was possible to use financial tracing and legal powers to recover some of the ransom money; it did not, however, mean that the whole of the payment had been recovered or that the wider ransomware network had been broken up. The incident also led to increased attention being paid to ransomware-as-a-service, whereby developers provide malicious software to affiliates who carry out the attacks and divide up the proceeds. The pipeline operator, the consumers of fuel, and businesses that rely on transportation were all affected. The situation also posed a difficult question to organizations under urgent operational pressure. Although paying a ransom may seem to provide a way of getting access back, such payments can help fund criminal networks and do not ensure that recovery will take place. On the other hand, policies which discourage payment may lead to further difficulties for the victims whose services are urgently needed by the public. The example of the Colonial Pipeline demonstrates the need for coordination between private operators, law enforcement, and government emergency response agencies when it comes to the cybersecurity of critical infrastructure. Delegates should think about the ways in which governments can assist victims, investigate ransom payments, and cut down on criminal profits without either discouraging people from reporting incidents or failing to put in place a recovery plan for essential services.



[8] Regions affected by colonial pipeline and graph showing similar attacks by size of company.

INTERPOL Operation Synergia II

Operation Synergia II was an international operation against cybercrime that took place in 2024 from April 1- August 31 and brought together law-enforcement agencies from 95 of the INTERPOL member countries as well as private-sector cybersecurity partners. The goal of the operation was to combat phishing, ransomware, and information-stealing malware. During the mission, investigators located about 30,000 suspicious IP addresses and over 22,000 malicious IP addresses or servers, 76% of which were shut down. The authorities seized 59 servers and 43 electronic devices, arrested 41 people, and identified 65 further individuals who became subjects of investigations. The success of the operation was the result of coordinated investigative efforts carried out by the national police agencies, INTERPOL, and private-sector partners who provided technical information on the malicious infrastructure. It led to the ultimate disruption of that infrastructure which had been used in cybercrime. However, dismantling servers does not always mean that the people involved, the financial networks, or the technical services behind a criminal operation are eliminated, since some of the infrastructure might be replaced and digital evidence collected in one country may still have to go through the necessary legal procedures before it can be used in prosecutions in another country. The operation also shows the importance of private-sector involvement, although it raises questions as to how intelligence should be verified and shared responsibly. Measurable enforcement outcomes can be achieved through operations of this kind, but it is essential for the delegates to tell the difference between causing only short-term disruption and actually bringing about the long-term dismantling of criminal networks. Care should be taken to address the root cause of these systems, with an emphasis on prevention rather than responding after an incident has occurred.



[10] The estimated rising costs of cybercrime.

TOPIC A: QUESTIONS TO CONSIDER

How can INTERPOL improve information-sharing between countries when ransomware investigations involve multiple jurisdictions?

What forms of technical training or investigative support would help countries with fewer cybersecurity resources participate in international investigations?

How can countries coordinate the collection and preservation of digital evidence while respecting differences in national laws and privacy protections?

What role should private-sector cybersecurity companies play in sharing threat intelligence with national authorities and INTERPOL?

How can international cooperation protect critical infrastructure while minimizing disruptions to essential public services?

What approaches could help identify and disrupt the financial networks associated with ransomware operations?

What safeguards should be included in international cybercrime cooperation to protect human rights, privacy, and due process?

UN PAST ACTIONS

UNODC Global Programme on Cybercrime (2013): Provides capacity building and technical assistance to help Member States combat cybercrime. Its creation was authorized by General Assembly resolution 65/230 (2011) alongside resolutions 22/7 and 22/8 of the Commission on Crime Prevention and Criminal Justice.

UN General Assembly Resolution 74/173 (2019): Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing.

UN Convention against Cybercrime (2024): First global, binding legal agreement explicitly designed to tackle borderless digital threats like ransomware and online fraud. It established a unified legal rulebook allowing countries to share electronic evidence across borders to track down and prosecute ransomware groups.

Operation Shadow Storm (2026): Focuses on using global intelligence networks to dismantle industrial-scale online scam compounds, unmask the criminal leaders hiding behind shell companies, freeze stolen digital assets, and break the ties between financial fraud and human trafficking.

TOPIC A APPENDIX & SOURCES

Borghard, Erica D., and Shawn W. Lonergan. "The Colonial Pipeline Incident Shows the Need for Broader Thinking about Cyber Resilience." Council on Foreign Relations, 20 May 2021, https://www.cfr.org/articles/colonial-pipeline-incident-shows-need-broader-thinking-about-cyber-resilience.

Bitdefender. "Fake Interpol Investigation Emails Target Small Businesses with Ransomware." Bitdefender, 1 July 2026, https://www.bitdefender.com/en-us/blog/hotforsecurity/fake-interpol-emails-serve-ransomware.

European Union Agency for Cybersecurity. "WannaCry Ransomware: First Ever Case of Cyber Cooperation at EU Level." ENISA, 15 May 2017, https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level.

Federal Bureau of Investigation. "Cryptocurrency Investment Fraud." FBI, https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud.

TOPIC A APPENDIX & SOURCES

Global Coalition. “Global Programme on Cybercrime” Global Coalition, https://www.globalcoalition.us/node/228.

“INTERPOL Emails Spread Custom Ransomware with Decryption Key Left Inside.” SC Media, https://www.scworld.com/news/interpol-emails-spread-custom-ransomware-with-decryption-key-left-inside.

INTERPOL. “INTERPOL Cyber Operation Takes Down 22,000 Malicious IP Addresses.” INTERPOL, 5 Nov. 2024, https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses.

INTERPOL. “INTERPOL Report Warns of Increasingly Sophisticated Global Financial Fraud Threat.” INTERPOL, 16 Mar. 2026, https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat.

TOPIC A APPENDIX & SOURCES

National Public Radio. “WannaCry Ransomware: What We Know Monday.” NPR, 15 May 2017, https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

SQ Magazine. “Cybersecurity Statistics 2026: Rising AI Threats & Global Impact” SQ Magazine, https://sqmagazine.co.uk/cybercrime-statistics/.

“The Colonial Pipeline Incident Shows the Need for Broader Thinking about Cyber Resilience.” The Economist, 10 May 2021, https://www.economist.com/graphic-detail/2021/05/10/ransomware-attacks-like-the-one-that-hit-colonial-pipeline-are-increasingly-common.

United Nations Office on Drugs and Crime. “Cybercrime Day.” UNODC, https://www.unodc.org/unodc/en/cybercrime/day.html.

World Health Organization. “WHO Director-General Briefs the UN Security Council on Ransomware Attacks on Healthcare.” WHO, 26 Nov. 2024, https://www.who.int/news/item/26-11-2024-who-director-general-briefs-the-un-security-council-on-ransomware-attacks-on-healthcare.

Copyright Notice

The contents of this document and any supplementary material are the sole intellectual property of Houston Area Model United Nations.

It may not be reproduced, republished, or used without the express written permission of Houston Area Model United Nations. Please email staff@houstonareamun.org with any questions.