International Criminal Police Organization

(INTERPOL)

Chairs: Shome Chakraborty and Hilary Cheng

Table of Contents

Letter from the Chairs

Welcome to the Herricks Model United Nations Conference 2023! My name is Shome Chakraborty and I am in 10th Grade. This is my 3rd time taking Model UN and I have attended 7 Model UN conferences in my MUN career. This will be my second time chairing an MUN committee. MUN has been an invaluable experience in my life and has taught me about responsibility, researching, speaking, negotiating, and making solutions as is often done in MUN. Outside of MUN, I love doing mathematics and science. Our committee will be simulating the INTERPOL General Assembly. I hope that you will take this committee as a joyful and educational experience. I look forward to reading your position papers and meeting you during the committee session.

Sincerely,
Shome Chakraborty

Welcome to HMUNC 2023! My name is Hilary Cheng and I am in 10th grade. It is my first time taking Model UN and I have attended two conferences so far, and this is my first time chairing! Model UN has become one of my passions and has allowed me to learn about public speaking and debating on the best options. Outside of Model UN, I am on our school's track team and throw shot put. I also play club volleyball, and enjoy reading when I have the time. I hope you will all enjoy our simulation of the INTERPOL committee this year. I am looking forward to meeting all of you and being your chair this year at HMUNC!

Sincerely,
Hilary Cheng

How to Use this Background guide

Dear delegates,

This is the background guide for the INTERPOL General Assembly at HMUNC 2022. As your chairs, we have spent a lot of time writing and gathering research in order to create the best possible guide for you, in hopes that it will aid you in your research and debate. We hope that you take some time to read this, as it'll provide a helpful guideline to the topics you will be discussing in debate as well as the potential solutions you may propose. This background guide should serve as one of the many sources you should utilize in order to conduct your research in preparation for our conference!

This background guide is filled with important statistics and subtopics that you may use in debate, and it provides delegates with a holistic understanding of both topics. In your position paper, you must include why your country thinks that these issues are important , how you have already tried to solve the problems and what possible solutions you may use to make the world a better place, and minimize the problem. This background guide will help you understand the basic ideas of the issues, and it is your job to be creative and figure out different solutions. In order to aid you with your process of writing a position paper and finding solutions, we will have questions to consider at the end of every topic as well as descriptions of your position at the end of the background guide! We look forward to hearing the ideas you bring to the table! Good luck!

Our committee email is: interpol.hmuncxviii@gmail.com

We look forward to meeting you in committee.

How to Write a Position Paper

We ask that you submit at least one position paper on both Topic A (cybercrime) or Topic B (counterfeit currency) to be considered for awards. Position papers should be no longer than one page in length and must have footnotes in MLA format for all sources used.

Each position paper is expected to have 3 paragraphs on each topic as follows:

Paragraph 1:

- Quote important documents and find different statistics regarding cybercrime or counterfeit currency.
- Use the background guide to familiarize yourself with the topics and why the issues are important to INTERPOL.
- Cite documents like the UN Charter or other legal documents that pertain to either topic.
- Explain why this issue is important and should be addressed.

Paragraph 2:

- Research more to find your country's policies and what they have done to address these specific issues.
- Use the position guides listed at the end of the background guide to help you.
- What laws have been passed? What is your country's stance on both topics? What countries has your country worked with in the past and what countries may it be looking to work with in the future?
- You can include quotes from your country's leader, conventions and resolutions your country has ratified, and statistics about your country to justify your position.

Paragraph 3:

- Come up with creative ideas that will help either solve or minimize this issue worldwide. How can we improve cybercrime? How do we improve counterfeit currency? What possible actions can we take?
- Remember to propose solutions relative to your country view and bloc (a bloc is a group of delegates that share similar ideas).
- At the bottom of each topic, we have added in questions to consider to help you find creative and thoughtful ideas.
- Make sure to write about what your country would like to accomplish in this committee.

As such, there should be a total of 6 paragraphs. You can include personal information about your position in the first paragraph for Topic A.

Position Papers are due Friday May, 15th, and must be e-mailed to:

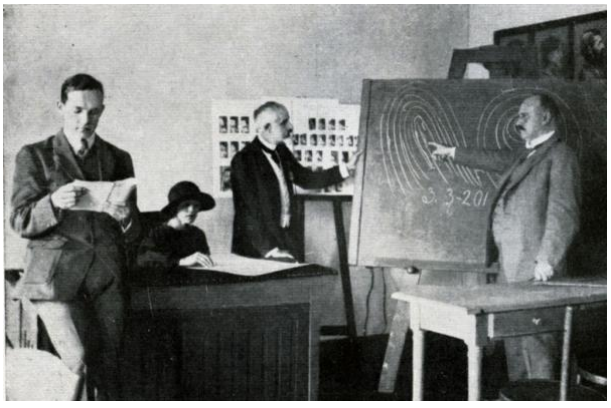
interpol.hmuncxviii@gmail.com

Committee Background

INTERPOL is an intergovernmental organization consisting of 195 member-states[1] with its headquarters in Lyon, France. It facilitates collaboration among law enforcement authorities of different countries through investigative support, intelligence, and secure communication systems to enforce international law (law followed by multiple countries) and combat transnational crime.[2]

International Criminal Police Commission Establishment

The organization's precursor was the International Criminal Police Commission (ICPC), founded by 20 countries in September, 1923, in Vienna, Austria, to respond to the growing crime surge in Europe. The idea behind the organization, proposed in 1914, was for law enforcement authorities to cooperate and share their experiences. After World War I, criminals began to use the new technologies of the time, such as the telegraph, telephones and cars. As a result, they were able to evade law enforcement and flee to other countries outside the jurisdiction of their domestic police force. Organized crime -



[1]"INTERPOL member countries." *Interpol*, https://www.interpol.int/en/Who-we-are/Member-countries. Accessed 4 May 2023.
[2]"INTERPOL Washington | Frequently Asked Questions." *Department of Justice*, 13 January 2023, https://www.justice.gov/interpol-washington/frequently-asked-questions. Accessed 4 May 2023.

criminal activities perpetuated by highly centralized and powerful criminal organizations - was also growing considerably during the same time.[3] During the 1930s, the organization was building better communication systems between countries including an international radio network in 1935.

Rebuilding and Post World War II Journey

During World War 2, much of the ICPC's files were destroyed largely by German activity.[4] So, the organization was reestablished in 1946 by 17 countries, and renamed INTERPOL in 1956.[5] INTERPOL now had to tackle crime in a more fragile world following the mass destruction and displacement of the war.[6] During the following decades, INTERPOL collaborated with other organizations such as the United Nations Division of Narcotic Drugs. INTERPOL shared information and expertise at a regional level, hosting its first regional conference in Liberia in 1969. In the 1990s, INTERPOL also adopted new methods to analyze criminal activity, establishing a criminal intelligence unit at its General Secretariat, which acts as the central body of the organization and enforces decisions made.[7]

Adoption of New Technologies

Since the 2000s, INTERPOL has used new modern technologies such as the automatic fingerprint identification system (AFIS) in 2000, a DNA profile database in 2002,[8] and INTERPOL Face Recognition in 2016.[9] This has allowed the organization to track criminal

[3]Metych, Michele. "Organized crime | Definition, History, Characteristics, & Facts." *Encyclopedia Britannica*, https://www.britannica.com/topic/organized-crime. Accessed 4 May 2023.
[4]Salter, Chuck. "WEB-EXCLUSIVE: The Secret History of Interpol." *Fast Company*, 31 August 2002, https://www.fastcompany.com/65171/web-exclusive-secret-history-interpol. Accessed 4 May 2023.
[5]"Key dates." *Interpol*, https://www.interpol.int/en/Who-we-are/INTERPOL-100/Key-dates. Accessed 4 May 2023.
[6]"History of Europe - The blast of World War II." *Encyclopedia Britannica*, https://www.britannica.com/topic/history-of-Europe/The-blast-of-World-War-II. Accessed 4 May 2023.
[7]"Key dates." *Interpol*, https://www.interpol.int/en/Who-we-are/INTERPOL-100/Key-dates. Accessed 4 May 2023.
[8]"INTERPOL then and now." *Interpol*, https://www.interpol.int/en/Who-we-are/INTERPOL-100/INTERPOL-then-and-now. Accessed 4 May 2023.
[9]"Facial Recognition." *Interpol*, https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition. Accessed 4 May 2023.

activity and process identifying data in a more tech-driven world far more effectively.

Branches

All of INTERPOL's member states meet at the organization's General Assembly. The General Assembly meets once per year attended by senior law enforcement officials such as ministers, chiefs of police, and representatives from the Commission for the Control of INTERPOL's Files (CCF).[10] It makes decisions on the organization's policies, activities, resources, and finances. It also elects the organization's Secretary General and the Executive Committee, which supervises the execution of the actions and decisions of the General Assembly and CCF.[11] [12] The Secretary General runs the organization's administrative headquarters - the General Secretariat - which oversees all administrative and policing ventures of INTERPOL.[13]

The CCF is an independent body which manages the data processed by INTERPOL. It handles requests by individuals to access, fix, or delete data in INTERPOL's information system and ensures that all data processing by INTERPOL conforms to the organization's rules.

INTERPOL's coordination with its member states is made through National Central Bureaus (NCBs). Each member state of INTERPOL maintains a NCB which works with the national law enforcement authorities, other INTERPOL member-states, and the INTERPOL General Secretariat to investigate criminal activity and share criminal data and intelligence.[14]

The INTERPOL Communications and Command Center (CCC) enables collaboration between INTERPOL and various entities.[15] The

[10] "90th INTERPOL General Assembly." *Interpol*, 18 October 2022, https://www.interpol.int/en/News-and-Events/Events/2022/90th-INTERPOL-General-Assembly. Accessed 4 May 2023.
[11] "Executive Committee - Governance." *Interpol*, https://www.interpol.int/en/Who-we-are/Governance/Executive-Committee. Accessed 4 May 2023.
[12] "General Assembly." *Interpol*, https://www.interpol.int/en/Who-we-are/Governance/General-Assembly. Accessed 4 May 2023.
[13] "National Central Bureaus (NCBs)." *Interpol*, https://www.interpol.int/en/Who-we-are/Member-countries/National-Central-Bureaus-NCBs. Accessed 4 May 2023.
[14] "National Central Bureaus (NCBs)." *Interpol*, https://www.interpol.int/en/Who-we-are/Member-countries/National-Central-Bureaus-NCBs. Accessed 4 May 2023.
[15] "Command and Coordination Centre." *Interpol*, https://www.interpol.int/en/How-we-work/Command-and-Coordination-Centre. Accessed 4 May 2023.

CCC controls messages between different police departments and NCBs, and also manages information that goes to the public, offers support in investigation, and aids in both domestic and foreign law.

Functions & Jurisdiction

INTERPOL specifically works against terrorism, cybercrime, and emerging crimes through its network of information and policies that connect its member states.[16] INTERPOL currently has 19 databases holding more than 124 million police records of documents and individuals related to criminal activities such as terrorism, organized crime, trafficking, firearms, and theft. Each day, law enforcement authorities make over 20 million searches from these databases.[17] The I-24/27 is INTERPOL's principle communications system for member-states to securely communicate with each other and access databases.[18]

INTERPOL facilitates the spread of information for public view through warnings and alerts including Red Notices, which act as petitions for people to be found and potentially arrested.[19] The first red notice was made in 1947 against a Russian man wanted for murdering a police officer.[20]

INTERPOL does not have the power to make arrests or to prosecute and investigate particular crimes.[21] It also does not have any law enforcement agents.[22] This is to signify that INTERPOL's activities and intelligence can only be acted upon by the law enforcement authorities of its member states.

[16] "COUNTER-TERRORISM." *Interpol*, https://www.interpol.int/content/download/5266/file/Counter-terrorism.pdf. Accessed 4 May 2023.
[17] "Our 19 databases." *Interpol*, https://www.interpol.int/en/How-we-work/Databases/Our-19-databases. Accessed 4 May 2023.
[18] "What is INTERPOL?" *Interpol*, https://www.interpol.int/Who-we-are/What-is-INTERPOL. Accessed 4 May 2023.
[19] "View Red Notices." *Interpol*, https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices. Accessed 4 May 2023.
[20] "Key dates." *Interpol*, https://www.interpol.int/en/Who-we-are/INTERPOL-100/Key-dates. Accessed 4 May 2023.
[21] "FAQs about INTERPOL." *Fair Trials*, 19 January 2022, https://www.fairtrials.org/articles/information-and-toolkits/faqs-about-interpol/. Accessed 4 May 2023.
[22] "INTERPOL Washington | Frequently Asked Questions." *Department of Justice*, 13 January 2023, https://www.justice.gov/interpol-washington/frequently-asked-questions. Accessed 4 May 2023.

Recent Developments and Programs

Given the significant presence of technology in criminal activity and the subsequent need for member-states to be more technologically adept to respond to crime, INTERPOL has recently created programs for the improvement of technological skills within member countries.

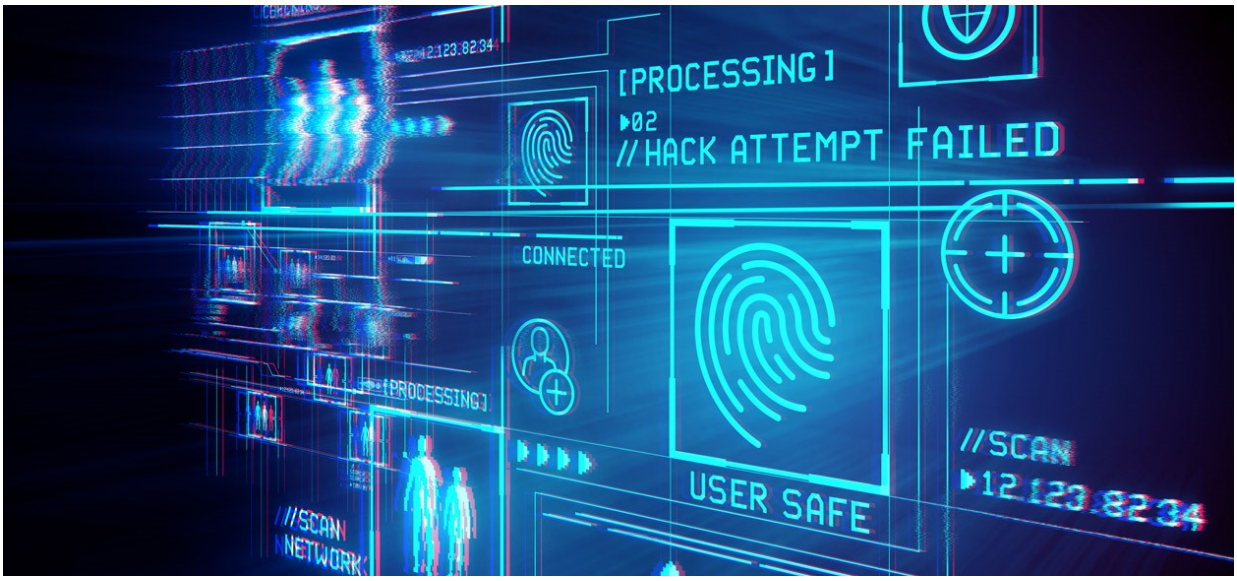
The Digital Security Challenge tested the ability of cyber-investigators from member-countries to solve a complex cybercrime case in a simulated operation.

Regional efforts to improve tech-capabilities among countries include a Canadian-funded initiative to provide technical expertise to cybercrime law enforcement units in Latin America and the Caribbean. An African cybercrime operations desk coordinates with 49 African states to better combat cyber crime.[23]

Furthermore, with the recent surges in financial crime throughout the world, INTERPOL created an organization in early 2022 named the Financial Crime and Anti-Corruption Centre (IFCACC) to help intercept illicit financial activity.[24]

For the purposes of this committee, the committee will be simulating the INTERPOL General Assembly. This committee will also be a SPECIALIZED committee.

[23]"Cyber capabilities development." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development. Accessed 4 May 2023.
[24]Stock, Jürgen. "Financial and cybercrimes top global police concerns, says new INTERPOL report." *Interpol*, 19 October 2022, https://www.interpol.int/en/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report. Accessed 4 May 2023.



Topic A: Cybercrime

What is Cybercrime?

Cybercrime: Criminal activity conducted online.

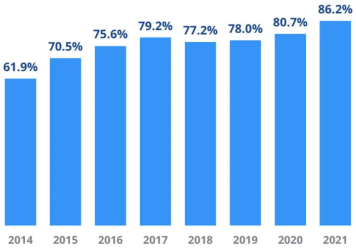


Figure 2: Percentage of organizations compromised by at least one successful attack.

Cybercrime refers to all criminal activity conducted online. As technology has become widespread globally, cybercrime has become an extremely serious problem.[25] Modern cybercrime began in 1962 when an MIT student named Allen Scherr stole password information from MIT computers so he could do more work on his projects as he studied.[26] Scherr continued to steal and use stolen passwords for the entirety of his work in computer science and operation systems, and was only found out when he later confessed.[27]

Three decades later in the 1990s, as technology began to flourish, so did the number of cybercriminals. While communications technologies and global connections increased, security was not a priority for developers, so criminals received a space in which they could commit crimes online. As technology develops, so does criminals' ability to commit crimes digitally.[28] Today, there are about 236.1 million cyber attacks every year.[29]

There are a variety of types of cyber crimes including distributional denial of service attacks (DDoS), identity theft, phishing, ransomware, cryptojacking, and more. This has provided a modern way for criminals to target and extort individuals, businesses, and governments. Whether it is by stealing money or data, compromising devices and machines, and in a more threatening way, blacking out whole communities, and endangering countries. Financially, experts believe that cybercrime will cost individuals and institutions $8

Ransom: cybercriminals take access to a victim's device and data and demand payment to release the information

[25] Powell, O. "The biggest data breaches and leaks of 2022." *Cyber Security Hub*, 13 Dec. 2022, www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022.
[26] "A Brief History of Cybercrime." *Arctic Wolf*, 16 November 2022, https://arcticwolf.com/resources/blog/decade-of-cybercrime/. Accessed 16 April 2023.
[27] "The History of Passwords and the Case of the First Theft — Strategic business consulting news and analysis from BRG | ThinkSet." *BRG ThinkSet*, 4 November 2018, https://thinksetmag.com/issue-6/the-case-of-the-purloined-password. Accessed 16 April 2023.
[28] "A Brief History of Cybercrime." *Arctic Wolf*, 16 November 2022, https://arcticwolf.com/resources/blog/decade-of-cybercrime/. Accessed 16 April 2023.
[29] Griffiths, C. "Aag-it.com | 520: Web server is returning an unknown error." *IT Support Services | AAG – Leaders in Managed IT Solutions*, 6 Apr. 2023, aag-it.com/the-latest-ransomware-statistics/.

trillion by the end of 2023. This would be equivalent to $255,000 every second. This cost is only expected to grow to $10.5 trillion in 2025.[30]

Why Do People Commit Cybercrime?

A significant amount of cybercrimes are committed to make money. Cybercriminals can do this through accessing money with bank account and credit card information of individuals and businesses as well as selling the data they steal from individuals and businesses,[31] [32] and through ransom.[33][34]

Plausible deniability: the ability people have to deny knowledge or responsibility for certain actions

Cybercrime can also be politically motivated. Criminals may attempt to breach information firewalls and attack the technological systems of rival nations, sometimes attacking power grids or military systems of countries.[35] The Chinese and Russian governments have been accused of using cybercriminal groups to target adversary states. Countries often do what China and Russia have been accused of in order to show plausible deniability for directly targeting countries.[36] [37] [38] [39] This represents the growing blurring of lines between cybercriminal entities and governments which needs to be addressed by the committee.

Types of Cybercrime

Malware is software that is used with malicious intent. Malware can be used to steal information such as personal data including people's personal bank

Cyber espionage: the use of online tools to take confidential information

[30]"Cybercrime To Cost The World 8 Trillion Annually In 2023." *Cybercrime Magazine*, 13 October 2022, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/. Accessed 16 April 2023.
[31] Vojinovic, I. "More than 70 cybercrime statistics - A $6 trillion problem." *Dataprot*, 27 Nov. 2019, dataprot.net/statistics/cybercrime-statistics/.
[32] F - Secure. "Why do hackers want your personal information?" www.f-secure.com/us-en/articles/why-do-hackers-want-your-personal-information.
[33] Australian Cyber Security Centre. "What to do if you're held to ransom | Cyber.gov.au." *Australian Cyber Security Centre*, https://www.cyber.gov.au/ransomware/what-to-do. Accessed 30 April 2023.
[34]"Ransom Definition & Meaning." *Merriam-Webster*, https://www.merriam-webster.com/dictionary/ransom. Accessed 5 May 2023.
[35]"Stevenson University." *Stevenson University*, https://www.stevenson.edu/online/about-us/news/cyber-attacks-digital-age/. Accessed 16 April 2023.
[36]Geller, Eric. "Chinese government recruiting criminal hackers to attack Western targets, U.S. and allies say." *Politico*, 19 July 2021, https://www.politico.com/news/2021/07/19/chinese-government-recruiting-criminal-hackers-biden-500091. Accessed 16 April 2023.
[37]"Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." *Department of Defense*, 20 April 2022, https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF. Accessed 16 April 2023.
[38] Handler, S., and L. Rowley. "The 5×5—Cybercrime and National Security." *Atlantic Council*, 7 July 2022, www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/.
[39]"plausible deniability - Political Dictionary." *Political Dictionary* -, https://politicaldictionary.com/words/plausible-deniability/. Accessed 5 May 2023.

account details and social security numbers as well as information and data held by businesses and governments.[40] This is a form of cyber espionage.[41] It can be used to control other peoples' devices and use those devices for malicious means, as is seen in cryptojacking.[42] Cybercriminals can use malware to slow a business' operations by disrupting factories and a company's networks (interconnected computer devices).[43] [44] This can then have very serious economic consequences. Government services and functions can also be targeted by cybercriminals through malware by hacking into government systems.[45]

Most frequently, Cybercrime is done through malware inserted into personal devices in various ways. For example, criminals send malicious links and downloads to people through emails, tricking consumers into downloading malware onto their own devices, otherwise known as phishing.[46]

Phishing: when criminals send emails or messages, impersonating large companies or people the victim knows in order for the victim to give away personal information.

Furthermore, malware is downloaded with illegal movies and shows, or when people click on advertisements that are scams.[47] Often, criminals use **phishing** to compel people to download malware. The main type of phishing is trojan malwares, where criminals act as a legitimate application to download malware onto a victim's device.[48]

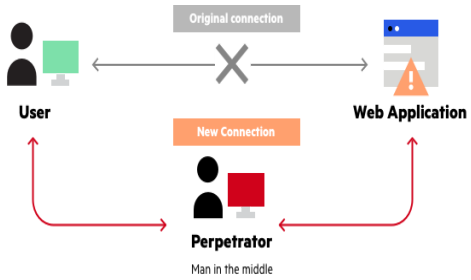
When the criminals take private information from individuals and businesses, they can blackmail the victims for ransom. Criminals can also reach victims through **ransomware**, where they threaten to damage or remove access to files or systems if certain amounts of money are not paid to the criminal.[49] In some cases, data which is stolen can ultimately be permanently destroyed and lost or leaked on the internet.[50]

---

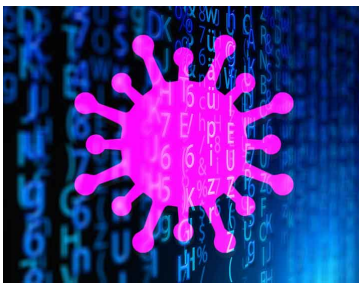
[40] *How To Recognize, Remove, and Avoid Malware*, https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware. Accessed 16 April 2023.
[41] Baker, Kurt. "What is Cyber Espionage? – CrowdStrike." *CrowdStrike*, 28 February 2023, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/. Accessed 16 April 2023.
[42] "Kaspersky report on cryptojacking in Q1–Q3 2022." Securelist, 10 November 2022, https://securelist.com/cryptojacking-report-2022/107898/. Accessed 16 April 2023.
[43] Stanger, James. "Why DDoS attacks are a major threat to industrial control systems." Control Engineering, 24 June 2021, https://www.controleng.com/articles/why-ddos-attacks-are-a-major-threat-to-industrial-control-systems/. Accessed 16 April 2023.
[44] Amazon Web Services. "What is Computer Networking?" Amazon Web Services, Inc, aws.amazon.com/what-is/computer-networking/.
[45] Cliff, Gerald. "Growing Impact of Cybercrime in Local Government." ICMA, 31 May 2017, https://icma.org/articles/pm-magazine/growing-impact-cybercrime-local-government. Accessed 16 April 2023.
[46] Vedova, Holly. "Spyware and Malware." *Federal Trade Commission*, https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware. Accessed 16 April 2023.
[47] *How To Recognize, Remove, and Avoid Malware*, https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware. Accessed 16 April 2023.
[48] Johansen, Alison Grace. "What is a Trojan? Is It Virus or Malware? How It Works." *Norton*, 24 July 2020, https://us.norton.com/blog/malware/what-is-a-trojan. Accessed 16 April 2023.
[49] "Stop Ransomware." *CISA*, https://www.cisa.gov/stopransomware. Accessed 16 April 2023.
[50] Morgan, S. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Cybercrime Magazine, 13 Nov. 2020, cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

One type of malware is **keyloggers or keystroke loggers**, which enable criminals to record what a person is typing for mainly malicious usage. Like other types of malware, keylogging can be installed into a device through downloads and through clicking on links. Through keylogging, criminals view the victim's activity and therefore access their information.

Keylogging doesn't damage devices or systems; however, the theft of information can lead to loss of personal information including credit card details, and loss of sensitive information held by organizations.[51] 80% of keylogging cannot be identified by firewalls or antivirus software, so keylogging malware is especially difficult to remove.[52] There are multiple tools that allow for keylogging. For example, the Kernel Computer Activity Monitor and the Ardamax Keylogger allow for the recording of all activity on a device.[53] Keylogging is an easy way for criminals to steal private information.



Similar to keylogging, **man in the middle (MITM) attacks** allow cybercriminals to steal information from their victims. This is often done through the hacking of public WiFi or personal hotspots, allowing the cybercriminal to place themself between the victim and the application and retrieve the information being transferred, usually credit card information or login details.[54] They can then use it,, for malicious purposes. There are multiple tools that can be used by cybercriminals for MITM attacks includingPacketCreator, dSniff, and Ettercap which are all software that can be used to interrupt communications between devices.[55]



Another common type of malware is a **virus,** which is able to develop and expand through devices by continuously

[51]"Keyloggers: How They Work & How to Detect Them." *CrowdStrike*, 2 February 2023, https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/. Accessed 16 April 2023.
[52]"What Is a Keylogger? [Everything You Need to Know]." *Techjury*, https://techjury.net/blog/what-is-a-keylogger/#gref. Accessed 16 April 2023.
[53]Chaudhary, Anju. "Top 10 Keylogger Software to Protect Data & Information." *Kernel Data Recovery*, 28 November 2022, https://www.nucleustechnologies.com/blog/best-keylogger-software/. Accessed 16 April 2023.
[54]"What is MITM (Man in the Middle) Attack | Imperva." *Imperva, Inc.*, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/. Accessed 16 April 2023.
[55]"What is a Man-in-the-Middle Attack? All About MITM Attack." *Intellipaat*, https://intellipaat.com/blog/man-in-the-middle-attack/. Accessed 16 April 2023.

replicating itself. Viruses can damage and slow computer operations, and forces the victim to transfer the virus between different systems. [56]

A ransomware attack is when cybercriminals block access to a victim's device and/or encrypt (seize) their data. They then demand a payment, or ransom from the victim to release access to the victim's device and/or data. Ransomware attacks are divided into two types. In **locker ransomware** attacks, a cybercriminal locks the basic functions of a victim's device. In **crypto ransomware attack**s, a cybercriminal encrypts a victim's data and computer files.[57]

Internet Network: Network of computers who transfer data between each other.

Spyware can be inserted into a victim's device. It then collects sensitive and personal information about the victim and tracks the victim's online activity from the device without the victim's consent. It can then send that to third parties.[58]

Internet traffic: a large amount of data traveling through the internet.

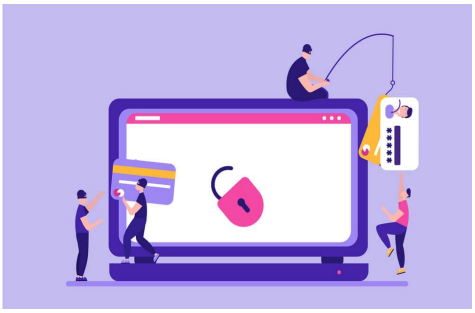
Server: Computer program which provides data and content to other computers.

A **distributional denial of service (DDoS) attack** targets businesses. Cybercriminals flood company networks and servers with internet traffic.[59] [60] [61] [62] This can often result in an organization's application performing slowly or being unavailable.[63] DDoS attacks can be used to disrupt industrial control systems (ICS) which manage machinery and technological infrastructure and are relied on by communities and businesses.[64] [65] A DDoS attack harms businesses by stopping them from providing services to customers, reducing

Bandwidth: Amount of information or data devices can receive

[56] "Computer Virus: What are Computer Viruses?" *Malwarebytes*, https://www.malwarebytes.com/computer-virus. Accessed 16 April 2023.
[57] Kaspersky. "Ransomware Attacks and Types | How do Locky, Petya and other ransomware differ?" *Kaspersky*, https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types. Accessed 30 April 2023.
[58] "What Is Spyware? Definition, Types And Protection." *Fortinet*, https://www.fortinet.com/resources/cyberglossary/spyware. Accessed 5 May 2023.
[59] "Cybercrime – #YouMayBeNext." Interpol, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-YouMayBeNext. Accessed 16 April 2023.
[60] "What Is Network Traffic? Definition and How To Monitor It." *Fortinet*, https://www.fortinet.com/resources/cyberglossary/network-traffic. Accessed 16 April 2023.
[61] Williams, Lawrence. "Difference Between Network and Internet." *Guru99*, 22 April 2023, https://www.guru99.com/difference-between-network-and-internet.html. Accessed 5 May 2023.
[62] Posey, Brien. "What is a Server? - Definition from WhatIs.com." *TechTarget*, https://www.techtarget.com/whatis/definition/server. Accessed 5 May 2023.
[63] "Cybercrime – #YouMayBeNext." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-YouMayBeNext. Accessed 16 April 2023.
[64] Stanger, James. "Why DDoS attacks are a major threat to industrial control systems." *Control Engineering*, 24 June 2021, https://www.controleng.com/articles/why-ddos-attacks-are-a-major-threat-to-industrial-control-systems/. Accessed 16 April 2023.
[65] "What are Industrial Control Systems (ICS) | HARTING Technology Group." *Harting*, https://www.harting.com/US/en/solutions/what-are-industrial-control-systems-ics. Accessed 16 April 2023.

productivity and leading to damage and loss of customers.[66] At times, DDos attacks can also hinder government services by targeting government networks.[67]



In 2007 Russian hackers used a DDoS attack against Estonian banks, telecom companies, news organizations and government entities that lasted for 4 weeks in response to the Estonian Government's removal of a Soviet war monument from the nation's capital, Tallinn. Hackers overloaded the bandwidth in Estonian servers by using fake traffic.[68][69] During the attack, Estonia's largest bank, Hansabank, had to halt their online services for more than an hour.[70]

Accessing Personal Data

In 2022, over 122 million people were affected by data compromisation globally.[71] This includes data breaches, where personal information is stolen and then used through malware where criminals hack and disrupt personal technology.

Identity theft

Criminals steal personal information to commit crimes.[72] In 2019, around 40% of people experienced identity theft online.[73]

Personal finances

The multiple forms of online shopping payment forms allow cybercriminals to obtain banking information, exploiting potential weaknesses in online payment.[74] After obtaining banking details, cybercriminals withdraw and steal money. In 2021, around $20 billion was lost in digital payment fraud.[75]

---

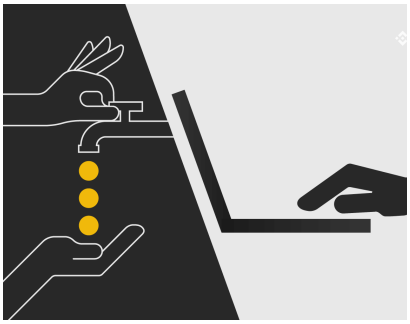
[66]Sansone, Isabella. "Why DDoS Attacks are So Damaging." *Corero*, https://www.corero.com/the-damaging-impacts-of-ddos-attacks/. Accessed 16 April 2023.
[67]De Tomas, Samuele. "Cyber attacks against Estonia (2007) - International cyber law: interactive toolkit." *Cyber Law Toolkit*, 17 September 2021, https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007). Accessed 16 April 2023.
[68]"What is Bandwidth - Definition, Meaning & Explanation." *Verizon*, 21 February 2023, https://www.verizon.com/articles/internet-essentials/bandwidth-definition/. Accessed 5 May 2023.
[69]De Tomas, Samuele. "Cyber attacks against Estonia (2007) - International cyber law: interactive toolkit." *Cyber Law Toolkit*, 17 September 2021, https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007). Accessed 16 April 2023.
[70]"What is Bandwidth - Definition, Meaning & Explanation." *Verizon*, 21 February 2023, https://www.verizon.com/articles/internet-essentials/bandwidth-definition/. Accessed 5 May 2023.
[71]Petrosyan, Ani. "Number of data breaches and victims U.S. 2022." *Statista*, 1 April 2023, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. Accessed 28 April 2023.
[72]Luthi, Ben. "What Is Identity Theft?" *Experian*, 19 September 2022, https://www.experian.com/blogs/ask-experian/what-is-identity-theft/. Accessed 16 April 2023.
[73]"Exploring Identity Theft Statistics in the Age of Data Breaches." *DataProt*, 27 March 2023, https://dataprot.net/statistics/identity-theft-statistics/. Accessed 16 April 2023.
[74]"Financial crime risk management in digital payments." *McKinsey*, 24 June 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments. Accessed 16 April 2023.
[75]Dopson, Elise. "9 Ecommerce Fraud Prevention Strategies for 2022." *Shopify*, 27 May 2022, https://www.shopify.com/enterprise/ecommerce-fraud-prevention. Accessed 16 April 2023.

Credit Card Fraud

Criminals use stolen credit card information to make purchases.. As of 2021, 127 million adults in the United States have been victims of credit card fraud.[76] In 2021, individuals lost about $32.34 billion to credit card fraud, and by 2031 this amount is expected to increase to $47.22 billion.[77]

There are two types of credit card fraud: **application fraud**, where the criminal opens an entirely new account with stolen personal information, and **account takeovers** where the criminal seizes an existing account.[78] In many cases, purchases made by criminals through the use of credit card fraud can lead to financial hardship, since the victim may not be able to pay the bill, which may affect the victim's credit score.[79] However, such issues may also be dealt with through the credit card company. When a complaint is made, the company looks through previously made transactions to identify any suspicious activity. Such a process may be as short as a few days, or as long as months. If the company decides that the transaction was a fraud, they may reimburse the customer, or file for a chargeback.[80]

Chargeback: the return of money to the customer of a credit card transaction



Cryptojacking

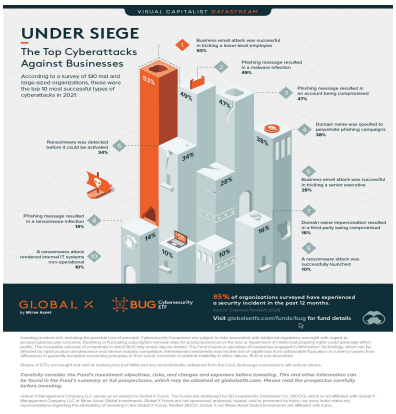
Cryptojacking involves a victim's device being used to mine cryptocurrency, and is often difficult to detect.[81] Cryptocurrencies, being digital, only require computer programs to be created. Therefore, criminals are able to profit without the victim's knowledge. This can lead to infection of the device, slowing its performance.[82] Because cryptojacking requires power from the victim's computer, victims face higher electricity charges.[83] The Monero (XMR) cryptocurrency is the

Cryptocurrency: a type of digital currency that acts as another option for payments

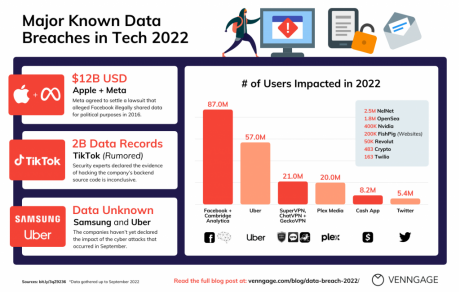
[76]Bingler, Liz. "Credit Card Fraud Statistics." *Bankrate*, 12 January 2023, https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/. Accessed 16 April 2023.
[77]Mullen, Caitlin. "Card industry's fraud-fighting efforts pay off: Nilson Report." *Payments Dive*, 5 January 2023, https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/. Accessed 16 April 2023.
[78]"credit card fraud | Wex | US Law | LII / Legal Information Institute." *Law.Cornell.Edu*, https://www.law.cornell.edu/wex/credit_card_fraud. Accessed 16 April 2023.
[79]"Credit Card Fraud: How It Happens and How to Protect Yourself." *CNBC*, https://www.cnbc.com/select/credit-card-fraud/. Accessed 16 April 2023.
[80]"How do Banks Conduct Credit Card Fraud Investigations?" *Chargebacks 911*, https://chargebacks911.com/credit-card-fraud-investigation/. Accessed 4 May 2023.
[81] "The Basics about Cryptocurrency | CTS." *SUNY Oswego*, https://www.oswego.edu/cts/basics-about-cryptocurrency. Accessed 24 April 2023.
[82]"Kaspersky report on cryptojacking in Q1–Q3 2022." Securelist, 10 November 2022, https://securelist.com/cryptojacking-report-2022/107898/. Accessed 16 April 2023.
[83]"Cryptojacking - Cybercrime." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking. Accessed 16 April 2023.

most common type created through cryptojacking, and in the first half of 2022, there were over 500,000 users attacked by cryptojacking.[84] Monero ensures its users remain anonymous.[85]

Effects on Businesses



Businesses are a common target of cybercriminals. Cybercriminals attack businesses by infecting their company servers, which provide data to other computers.[86] They also attack digital networks with malicious code and malware.[87] As a result, a business' data, intellectual property, and financial funds are stolen and operations are disrupted or even brought to a halt.[88] This poses irreparable harm in terms of finances, revenue stream, ability to operate and be productive, and overall reputation. Therefore, Businesses have to pay ransom to cybercriminals. The finance, healthcare, education, and energy and utilities industries have been the most targeted.[89] Between 2022 and 2023, 64% of businesses across the world reported facing some form of cyber attack.[90]



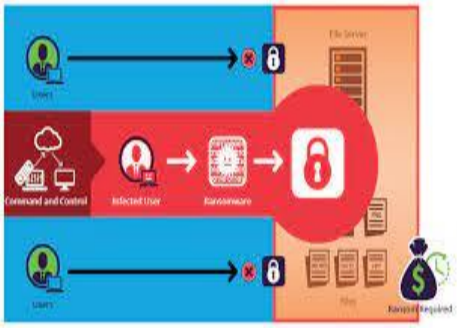
Business Operations

Business operations are targeted in multiple ways. DDoS attacks harm manufacturers by impacting Industrial Control Systems(ICS): computer systems that manage machinery and equipment.[91] [92] A business can lose up to $2.5 million from a DDoS attack after operations are disrupted.[93] Businesses facing a DDoS attack may be forced to pay ransom. This is known as a random DDoS attack and it costs businesses even more than a regular DDoS attack.[94]

---

[84]"Kaspersky report on cryptojacking in Q1–Q3 2022." *Securelist*, 10 November 2022, https://securelist.com/cryptojacking-report-2022/107898/. Accessed 16 April 2023.
[85] "What is Monero (XMR)?" *Monero*, https://www.getmonero.org/get-started/what-is-monero/. Accessed 24 April 2023.
[86]"What Is a Server?" *Lifewire*, 12 June 2021, https://www.lifewire.com/servers-in-computer-networking-817380. Accessed 16 April 2023.
[87]Logan, Michael. "6 Ways Cyber Crime Impacts Business - Cybersecurity." *Investopedia*, https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx. Accessed 16 April 2023.
[88]"Cybercrime – #YouMayBeNext." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-YouMayBeNext. Accessed 16 April 2023.
[89]"The Top 5 Industries Most Vulnerable to Cyber Attacks." *ProcessBolt*, https://processbolt.com/top-5-industries-most-vulnerable. Accessed 16 April 2023.
[90]"How Many Cyber Attacks Happen Per Day in 2023?" *Techjury*, https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref. Accessed 16 April 2023.
[91]Stanger, James. "Why DDoS attacks are a major threat to industrial control systems." *Control Engineering*, 24 June 2021, https://www.controleng.com/articles/why-ddos-attacks-are-a-major-threat-to-industrial-control-systems/. Accessed 16 April 2023.
[92]"What are Industrial Control Systems (ICS) | HARTING Technology Group." *Harting*, https://www.harting.com/US/en/solutions/what-are-industrial-control-systems-ics. Accessed 16 April 2023.
[93]Brook, Chris. "DDoS Attacks Can Cost Businesses Up to $2.5M Per Attack, Report Says." *Threatpost*, 2 May 2017, https://threatpost.com/ddos-attacks-can-cost-businesses-up-to-2-5m-per-attack-report-says/125357/. Accessed 4 May 2023.
[94]"What is a ransom DDoS attack?" *Cloudflare*, https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/. Accessed 4 May 2023.

Data breaches can also inflict significant damage. Company data includes information about employees, customers, inventory, sales, customer satisfaction, marketing, research and development, and more.[95] It is a crucial tool for decision-making and proper operation. In a data breach, cyber criminals access and/or steal data, resulting in business operations being halted.[96] In 2022, data breaches cost businesses on average $4.35 million.[97]



Ransomware costs businesses in terms of data and money. In 2021, at least 37% of businesses faced a ransomware attack and paid a ransom at an average of $1.85 million. However, only 65% of businesses that paid ransom actually received their data back.[98] Through data breaches, cybercriminals have the opportunity of stealing money from business bank accounts.[99] Businesses in the United States had lost up to $800 million between 2013 and 2015 from their bank accounts as a result of breaches.

Consumer Data

Data breaches also compromise customers.[100] Criminals access clients' names, contact information, addresses, IP numbers, social security numbers, and bank account information, and then target them through identity theft, phishing, financial fraud, extortion on massive scales.[101] .

In a 2014 JP Morgan data breach, cybercriminals accessed banking information for 76 million households.[102] The 2013 Yahoo data breach by Russian hackers is the largest in the world; the information of 3

[95]Guide, Step. "What Is Data in Business? (Plus Importance and Examples)." *Indeed*, 10 March 2023, https://www.indeed.com/career-advice/career-development/data-in-business. Accessed 16 April 2023.
[96]"30 Surprising Small Business Cyber Security Statistics." *Fundera*, 23 January 2023, https://www.fundera.com/resources/small-business-cyber-security-statistics. Accessed 16 April 2023.
[97]Henriquez, Maria. "$4.35 million — The average cost of a data breach." *Security Magazine*, 17 October 2022, https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach. Accessed 16 April 2023.
[98]Kochovski, Aleksandar. "Ransomware Statistics, Trends and Facts for 2022 and Beyond." *Cloudwards*, https://www.cloudwards.net/ransomware-statistics/. Accessed 4 May 2023.
[99]"Home." *YouTube*, https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5d5a3a96b616. Accessed 16 April 2023.
[100]Ydstie, John. "When Cyberfraud Hits Businesses, Banks May Not Offer Protection." *NPR*, 15 September 2015, https://www.npr.org/sections/alltechconsidered/2015/09/15/440252972/when-cyber-fraud-hits-businesses-banks-may-not-offer-protection. Accessed 16 April 2023.
[101] Pennsylvania Attorney General Michelle A. Henry. "Identity Theft Phishing, Pharming and Vishing." Pennsylvania Office of Attorney General, www.attorneygeneral.gov/protect-yourself/identity-theft/identity-theft-phishing-pharming-and-vishing/.
[102]"Home." *YouTube*, https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/. Accessed 16 April 2023.

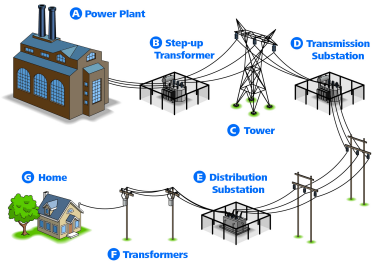
billion users was accessed including names and addresses.[103] Data breaches destroy a business' reputation as customers no longer trust them.[104]

Intellectual Property

Data breaches also result in the loss of intellectual property (IP), intangible assets such as inventions, designs, and/or trade secrets, including secret processes, devices, or techniques. [105] This leads to loss of customers, competitive advantage, and reputation.[106] It is known as economic espionage.[107] U.S. businesses lose about $600 billion annually due to IP theft by Chinese entities.[108]

Small Businesses

Small businesses are the most common targets of cybercriminals because, in addition to having resources cyber criminals want, such as data, money, and opportunities to hold ransom, they are not as prepared to combat cyber attacks because of their limited resources, unlike larger businesses. 43% of all cyber attacks target small businesses.[109] 70% of small businesses have sufficient resources and security expertise.[110] In 2021, more than 61% of small businesses were targets of cyber attack, facing on average $2.2 million in damages. 60% shut down 6 months later.

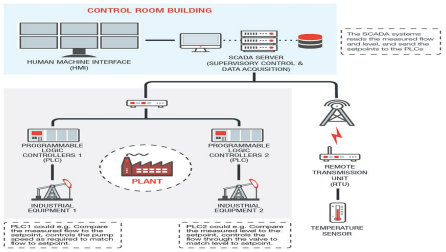


[103]Sen, Kaushik. "Biggest Data Breaches in US History [Updated 2023]." *UpGuard*, 2 March 2023, https://www.upguard.com/blog/big
[104]"What Happens to a Company's Reputation After a Data Breach?" *Digistor*, 17 December 2022, https://digistor.com/what-happens-t
April 2023.
[105]Gelinne, John Patrick, et al. "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property." *Deloitte*, 25 July 2016, https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html. Accessed 16 April 2023.
[106]Huang, Yukon, and Jeremy Smith. "China's Record on Intellectual Property Rights Is Getting Better and Better." *Foreign Policy*, 16 October 2019, https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/. Accessed 16 April 2023.
[107] National Counterintelligence and Security Center. "Foreign Economic Espionage in Cyberspace." *Home*, 2018, www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.
[108]Huang, Yukon, and Jeremy Smith. "China's Record on Intellectual Property Rights Is Getting Better and Better." *Foreign Policy*, 16 October 2019, https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/. Accessed 16 April 2023.
[109]"30 Surprising Small Business Cyber Security Statistics." *Fundera*, 23 January 2023, https://www.fundera.com/resources/small-business-cyber-security-statistics. Accessed 16 April 2023.
[110]"Cybersecurity Statistics All Small Businesses Should Know." *Nicolet Tech*, https://nicolettech.com/cybersecurity-statistics-all-small-businesses-should-know/. Accessed 16 April 2023.

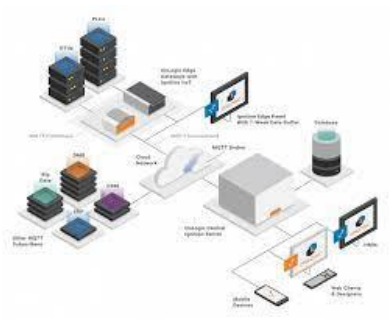
Effects on Communities: Power Outages

Power grids

Power grids are networks consisting of energy generator stations, transmitter lines and towers, and distribution lines responsible for providing power/energy.[111] The power grid provides critical services to millions of homes and businesses. The US government considers the power grids to be so important that "their incapacitation or destruction would have a debilitating effect on security, national economic security, and national public health or safety."[112]



As more power grids become digitized with new technologies, such as the Supervisory Control and Data Acquisition (SCADA) systems, a computer system which monitors electric substations in power grids, [113] they become more vulnerable to cybercrime.[114] Cybercriminals target any element of a power grid - its power generation, distribution, or transmission lines.[115] Cybercriminals also physically damage a power grid by targeting ICSs, which monitors power transmission and distribution.[116] [117]

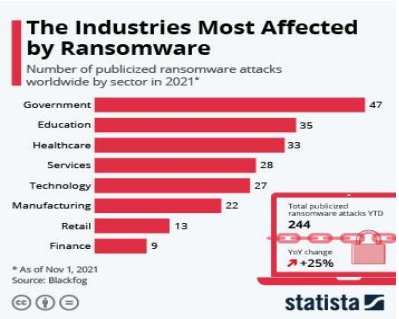


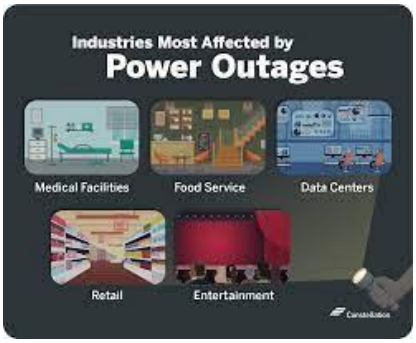
The first cyber attack against a power grid was on December 23, 2015, when Russian hackers used a malware known as BlackEnergy to attack the computer and SCADA systems of a Ukrainian power company to disconnect 30 substations for 3 hours. In that time, up to 230,000 Ukrainians lost power.[118]

[111] "Generac | How Power Grids Work." *Generac Power Systems*, https://www.generac.com/be-prepared/power-outages/power-grids. Accessed 16 April 2023.
[112] Livingston, Steve, et al. "Managing cyber risk in the electric power sector." *Deloitte*, 31 January 2019, https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html. Accessed 16 April 2023.
[113] Pugliesi, Daniele, and Abdur Rehman. "SCADA and Its Application in Electrical Power Systems." *AllumiaX Engineering*, 14 September 2020, https://www.allumiax.com/blog/scada-and-its-application-in-electrical-power-systems. Accessed 16 April 2023.
[114] Campbell, Heidi, and Paul Brandeis Raushenbush. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations*, 3 April 2017, https://www.cfr.org/report/cyberattack-us-power-grid. Accessed 16 April 2023.
[115] Campbell, Heidi, and Paul Brandeis Raushenbush. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations*, 3 April 2017, https://www.cfr.org/report/cyberattack-us-power-grid. Accessed 16 April 2023.
[116] "Cyber attacks on critical infrastructure." *Allianz Global Corporate & Specialty (AGCS)*, https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html. Accessed 16 April 2023.
[117] Love, David L. "Cybersecurity: Industrial Control Systems and the U.S. Electric Grid." *MS&E 238 Blog*, 26 July 2017, https://mse238blog.stanford.edu/2017/07/dllove/cybersecurity-industrial-control-systems-and-the-u-s-electric-grid/. Accessed 16 April 2023.
[118] Krigman, Amy. "Ukrainian Power Grid Attack - Blog." *GlobalSign*, 22 October 2020, https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history. Accessed 16 April 2023.

Effects of Power Outages on Communities

Power outages have disastrous effects on communities.





In addition to basic uses like lighting, heating, and cooling, electricity is needed in order to operate appliances, computers, electronics, machinery, and public transportation systems.[119] In homes, loss of air conditioning, heating, refrigeration, as well as access to common appliances such as computers and TV can have devastating effects. For example, electronics may also experience an electronic surge when power comes back after an outage, damaging them.

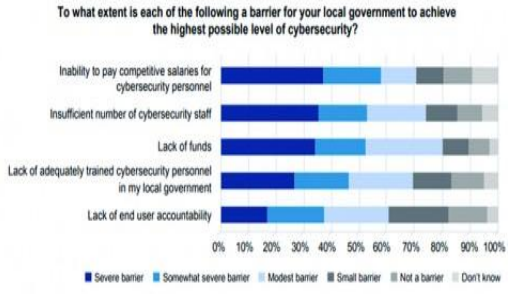
In businesses, power outages cause damage to inventory like refrigerated items that can spoil. Productivity can be impacted, and ripples in supply chains can follow.[120] In the United States, disruption in economic activity is estimated to cost up to $243 billion.[121]

In hospitals, power outages shut off medical equipment and machinery such as filtration and refrigeration systems, ventilators, incubators, dialysis machines, relied on by patients to be treated or even in extreme cases, to survive, thus causing a serious medical emergency.[122] Between 2019 and 2021, electrical outages in Venezuelan hospitals caused 233 hospital patients to die.[123]

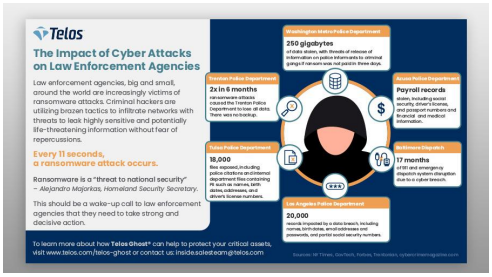
[119]"Use of electricity - U.S. Energy Information Administration." *EIA*, https://www.eia.gov/energyexplained/electricity/use-of-electricity.php. Accessed 16 April 2023.
[120]Suiskind, Ben. "7 Important Effects of Power Outages On Homes & Businesses." *All Dry USA*, https://www.alldryus.com/general/effects-of-power-outages-on-homes-businesses/. Accessed 16 April 2023.
[121]Campbell, Heidi, and Paul Brandeis Raushenbush. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations*, 3 April 2017, https://www.cfr.org/report/cyberattack-us-power-grid#chapter-title-0-4. Accessed 16 April 2023.
[122]Schwind, Kristopher. "What Happens When the Power Cuts Out at a Medical Facility?" *National Standby Repair*, https://www.nationalstandby.com/blog/what-happens-when-the-power-cuts-out-medical-facility/. Accessed 16 April 2023.
[123]"Venezuela report details 233 deaths due to hospital power cuts." *France 24*, 30 March 2022, https://www.france24.com/en/live-news/20220330-venezuela-report-details-233-deaths-due-to-hospital-power-cuts. Accessed 16 April 2023.

Effects on Governments and National Security

Cybercriminals have a history of hacking governments and public agencies [124] which impair a government's ability to provide public services and leads to substantial loss of taxpayer money. Between 2018 and 2021, government entities across the United States, serving 173 million citizens, faced 246 ransomware attacks which cost $52.88 billion, an average of $215 million of taxpayer money.[125]



Cybercrime against governments also leads to confidential information about citizens being accessed. In 2015,

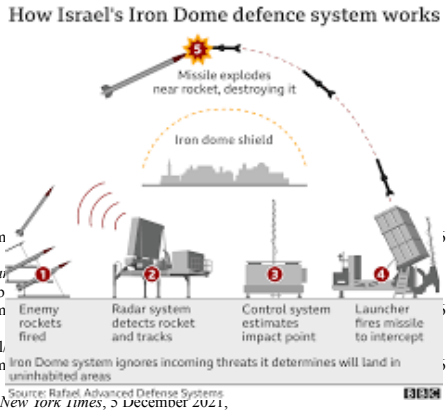


the Florida Department of Child and Family Services had a data breach where names and social security numbers of over 200,000 Floridians were stolen by a cybercriminal working within the Florida state government.[126]

Cybercriminals compromise **public safety** through attacks on law enforcement by accessing police department networks and holding them hostage as well as stealing valuable information.[127] For example, the Cockrell Hill Texas Police Department lost 8 years worth of digital evidence after a cyber attack.[128]

National Security Implications

Cybercrime can also be used against the national security of countries by compromising a nation's military or national defense system to demand a ransom or to fulfill a political agenda [129].



[124] Cliff, Gerald. "Growing Impact of Cybercrime in Local Government." *ICMA*, 31 May 2017, https://icma.org/articles/pm-m... April 2023.
[125] Axelrod, Jason. "Report: Ransomware attacks cost local and state governments over $18 billion in 2020." *American City a...* https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-b...
[126] Cliff, Gerald. "Growing Impact of Cybercrime in Local Government." *ICMA*, 31 May 2017, https://icma.org/articles/pm-m... April 2023.
[127] "Police are Victims Too: How to Protect Your Department from Cybercrime." *COPS OFFICE*, https://cops.usdoj.gov/html...
[128] Cliff, Gerald. "Growing Impact of Cybercrime in Local Government." *ICMA*, 31 May 2017, https://icma.org/articles/pm-m... April 2023.
[129] Barnes, Julian E. "U.S. Military Has Acted Against Ransomware Groups, General Acknowledges (Published 2021)." *The New York Times*, 5 December 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html. Accessed 16 April 2023.

In 2008, the United States military reported more than 300 million attacks on its military systems, often by Chinese entities.[130] Chinese hackers targeted and stole data from Israel's Iron Dome missile defense system in 2014.[131] The Iron Dome was responsible for withstanding 90% of Hamas missiles launched into Israel.[132] The Iron Dome's deactivation would allow terrorist groups to successfully unleash missiles into Israel, endangering millions of its citizens.

When targeting a country's national security, cybercriminals also aim to steal a country's intelligence, including military secrets. Chinese cybercriminals have been accused of stealing US aircraft designs by acquiring personal information of military soldiers as has numerous Russian hackers.[133] [134]

What Has Been Done?

International Community

The annual Internet Governance Forum and Convention on Cybercrime/Budapest Convention are both held to create agreements between countries to resist cybercrime.[135] A treaty was created that specified certain cybercrimes that would be criminalized and identified tools that could be used to investigate cybercrimes. Like INTERPOL, this treaty improved collaboration between countries, and helped reduce global cybercrime for its member nations.[136]

In December of 2019, the UN General Assembly created resolution 75/282 to counter criminal activity related to information and communications. This established an Ad Hoc intergovernmental committee with the purpose of creating an international cybercrime

[130]Rosenbach, Eric, et al. "Cyber Security and the Intelligence Community." *Belfer Center*, https://www.belfercenter.org/publication/cyber-security-and-intelligence-community. Accessed 16 April 2023.
[131]Gibbs, Samuel. "Chinese hackers steal Israel's Iron Dome missile data." *The Guardian*, 29 July 2014, https://www.theguardian.com/technology/2014/jul/29/chinese-hackers-steal-israel-iron-dome-missile-data. Accessed 16 April 2023.
[132]Williams, Dan. "Israel says Iron Dome scores 90 percent rocket interception rate." *Reuters*, 10 July 2014, https://www.reuters.com/article/us-palestinians-israel-irondome/israel-says-iron-dome-scores-90-percent-rocket-interception-rate-idUSKBN0FF0XA20140710. Accessed 16 April 2023.
[133] Handler, S., and L. Rowley. "The 5×5—Cybercrime and National Security." *Atlantic Council*, 7 July 2022, www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/.
[134]"Acts of an Adversary." *Center for American Progress*, 5 December 2017, https://www.americanprogress.org/article/acts-of-an-adversary/. Accessed 16 April 2023.
[135]"Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements." *Georgetown Law Research Guides*, 10 February 2023, https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties. Accessed 16 April 2023.
[136]"Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements." *Georgetown Law Research Guides*, 10 February 2023, https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties. Accessed 4 May 2023.

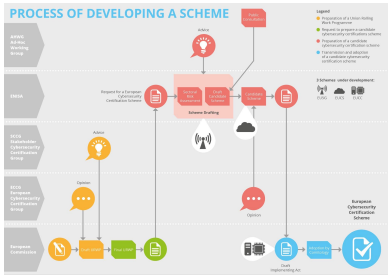
agreement.[137] The meetings are being held throughout 2023 and will present a draft convention to the General Assembly meeting in September.[138]

Europe

The European Union (EU) is at the forefront of cybersecurity with 18 of the top 20 countries in the global cybersecurity index. This relates to broad reforms designed to minimize cyberthreats in Europe.

In June 2019, The EU Cybersecurity Act introduced two new cybersecurity strategies. **The EU-wide cybersecurity certification framework** creates high security standards for information and communications technology (ICT) products and services to be certified (approved to be used) by the European Union. This framework is meant to build trust for ICT products among users and promote the growth of the EU cybersecurity market.[139] [140]

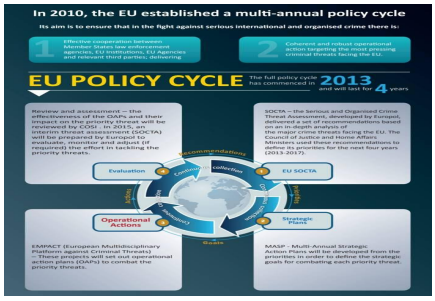
The EU Agency for Cybersecurity was originally the EU Agency for Network and Information Security, established in 2004. The agency has more resources and the key power of implementing the EU cybersecurity certification framework. The agency now has a permanent mandate.[141] [142] In 2013, **the European Cybercrime Center**, was established within Europol (the EU's criminal law enforcement agency) to assist in investigating cybercrimes and disbanding cybercriminal groups.[143][144][145]



[137] Giovannelli, Davide. "CCDCOE." *CCDCOE*, https://ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/. Accessed 16 April 2023.
[138] "." *" - Wiktionary*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement. Accessed 4 May 2023.
[139] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 4 May 2023.
[140] "The EU cybersecurity certification framework | Shaping Europe's digital future." *Shaping Europe's digital future*, 7 June 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. Accessed 4 May 2023.
[141] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 4 May 2023.
[142] "The EU Cybersecurity Act | Shaping Europe's digital future." *Shaping Europe's digital future*, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act. Accessed 4 May 2023.
[143] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 4 May 2023.
[144] "European Cybercrime Centre - EC3 | Europol." *Europol*, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. Accessed 4 May 2023.
[145] "About Europol | Europol." *Europol*, https://www.europol.europa.eu/about-europol. Accessed 4 May 2023.

In 2016, the EU's directive on network and information security introduced new security obligations for operators of essential services such as energy, transportation, health, and financial services, as well as digital service providers. It is meant to ensure that cybercriminals cannot target services. In December 2020, the directive was strengthened with elevated standards to respond to new cyber threats.[146]

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) EU member-states, institutions, and relevant partners cooperate in identifying and prioritizing threats by international organized crime. Cybercrime is prioritized under this initiative.[147][148]

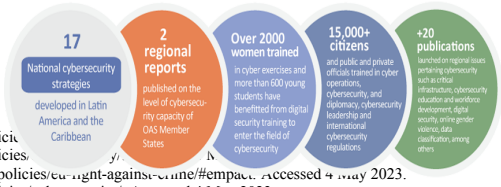


As of April of 2019, new regulations curb and limit digital payment fraud by clarifying fraud offenses, penalties for offenders, and the scope of jurisdiction for prosecution.[149][150] Additional proposals have been made to make it easier for European prosecutors to obtain electronic evidence (E-evidence) across borders of member states as well as US digital service providers.[151]

Latin America

The Organization of American States (OAS - a multinational organization of member-states from the Western Hemisphere), was the first regional body to create a framework to combat cybercrime in 2003.[152] Its strategy includes fostering cooperation between public and private sectors to promote cyber-security capabilities through technical assistance and training, policy discussions, crisis management exercises, and sharing of best practices for secure ICT products.[153]

The OAS' cybersecurity program has led to 2 regional reports on cybersecurity capabilities and over



[146] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policie
[147] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/
[148] "The EU's fight against organised crime - Consilium." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/#empact. Accessed 4 May 2023.
[149] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 4 May 2023.
[150] "EU puts in place tighter rules to fight non cash payment fraud." *Consilium.europa.eu*, 9 April 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/. Accessed 4 May 2023.
[151] "Cybersecurity: how the EU tackles cyber threats." *Consilium.europa.eu*, https://www.consilium.europa.eu/en/policies/cybersecurity/. Accessed 4 May 2023.
[152] "Raising the Political Priority of Cybersecurity in Latin America." *Council on Foreign Relations*, 16 March 2023, https://www.cfr.org/blog/raising-political-priority-cybersecurity-latin-america. Accessed 4 May 2023.
[153] "OAS :: Cyber Security." *Organization of American States*, https://www.oas.org/en/topics/cyber_security.asp. Accessed 4 May 2023.

20 publications which identify regional issues related to cybersecurity. More than 15,000 citizens in the public and private sectors have been trained to conduct cybersecurity operations.National cybersecurity strategies exist in at least 17 member states.[154] While Brazil has been a leader in cybersecurity, many Latin American countries have still not implemented policies to better cybersecurity. [155]

United States

The US Secret Service combats financial crimes in cyberspace,[156] through its **Electronic Crimes Task Forces** which identify and locate international cybercriminals linked to cyber intrusions, bank fraud, data breaches, and other online crimes responsible for US institutions and individuals losing hundreds of millions of dollars. The Secret Service also maintains **the National Computer Forensic Institute**, which focuses on giving law enforcement officers, prosecutors, and judges information and training about cybercrime.[157]

The Cybersecurity and Infrastructure Security Agency, under the Department of Homeland Security (DHS), is the US' cyber defense agency and minimizes the effect of cybercrime on US infrastructure by collaborating with businesses and government to develop infrastructure that is secure and resilient against cybercrime.[158]. The DHS also maintains **the US Immigration and Customs Enforcement Homeland Security Investigations Cyber Crimes Center** (C3) which provides technical

[154]"OAS :: CICTE: Cybersecurity." *Organization of American States*, https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp. Accessed 4 May 2023.
[155]"Raising the Political Priority of Cybersecurity in Latin America." *Council on Foreign Relations*, 16 March 2023, https://www.cfr.org/blog/raising-political-priority-cybersecurity-latin-america. Accessed 4 May 2023.
[156]"United States Secret Service." *United States Secret Service*, https://www.secretservice.gov/about/overview. Accessed 4 May 2023.
[157]"Combatting Cyber Crime." *CISA*, https://www.cisa.gov/combatting-cyber-crime. Accessed 4 May 2023.
[158]"About CISA." *CISA*, https://www.cisa.gov/about. Accessed 4 May 2023.

assistance to investigations in computer-related international crimes. It also uses its advanced facilities such as its forensics library to participate in digital evidence recovery in computer-related criminal investigations and trains local, state, federal, and international law enforcement officials in computer investigative and forensic skills.

The US Government also operates a reporting mechanism called **the Law Enforcement Cyber Incident Reporting** resource which provides information to local and state law enforcement authorities on how to report cybercrime to the Federal Government.[159]

Russia

Russia has proposed cybersecurity initiatives on a global scale, but they have been criticized for restricting and regulating internet use by individuals. On March 7, 2023, Russia proposed a UN Convention on Ensuring International Information Security to the UN's Open-Ended Working Group, or the OEWG.[160] Russia wanted to allow an increased amount of governmental internet supervision to reduce the amount of cybercrimes.[161] Russia's proposal is seen as a threat to digital human rights, as it requests sovereign equality. In the proposal, Russia asserted a country's sovereignty over crimes committed within its jurisdiction. Additionally, the proposal states that the right to freedom of expression may be regulated if it were to interfere with national security, and does not state people's right to other basic freedoms.[162] Overall such a proposal would drastically increase internet regulations, and many countries have not agreed to endorse this proposal.

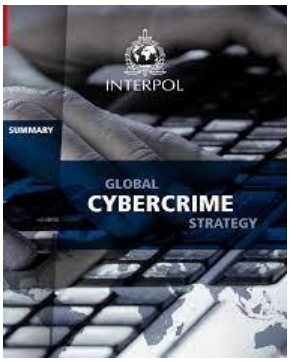
China

China has used the presence of cybercrime to control the use of the internet domestically. **The Cyberspace**

[159]"Combatting Cyber Crime." *CISA*, https://www.cisa.gov/combatting-cyber-crime. Accessed 4 May 2023.
[160]"Open-ended working group on information and communication technologies (2021) | United Nations." *UNODA Meetings Place*, https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021. Accessed 4 May 2023.
[161]"ОБНОВЛЕННАЯ КОНЦЕПЦИЯ КОНВЕНЦИИ." *UNODA.org*, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf. Accessed 4 May 2023.
[162]Campbell, Heidi, et al. "The Dangers of a New Russian Proposal for a UN Convention on International Information Security." *Council on Foreign Relations*, 21 March 2023, https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security. Accessed 16 April 2023.

Administration of China (CAC) was established by President Xi Jinping in 2014 to secure China's internet and data privacy.[163] Since that time, the CAC has radically increased internet oversight. In 2021, the CAC placed significant restrictions on online content and data usage by major technology companies such as Alibaba, a Chinese online retail company. [164][165] Xi Jinping said that the regulations were necessary to help solve long standing concerns over consumer rights and data protection on the internet. Critics point out that the regulations have significantly hampered China's business climate. The regulations may have wiped out $1 trillion from the market value of Chinese companies. In the year after the regulations, Alibaba lost $400 billion. Many entrepreneurs quit high profile jobs in response. In addition, China has banned children from playing online games for more than 3 hours a week.[166] It has banned cross-border online gambling and online cryptocurrency trading.[167]

INTERPOL Actions



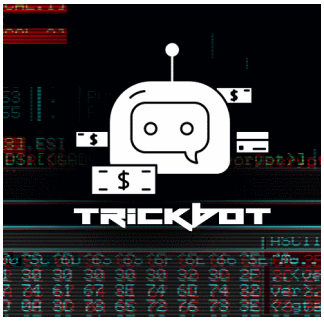
In 2015 INTERPOL created **the Global Cybercrime Programme** to help member countries fight cybercrime by increasing the efficacy of investigations, improving governmental response, and facilitating communication between countries.[168] The Global Cybercrime Programme helps member states in "capacity building and technical assistance," enabling an increase in a nation's analytical abilities.[169] In 2020 INTERPOL's Operation Night Fury was successful in identifying and assisting in arresting three cybercriminals in Singapore, who were stealing information on personal online forms of payment through malware.[170] INTERPOL has aided the South East Asian region in identifying compromised sites through analysis from relevant countries, creating multiple sources of

[163] "Combatting Cyber Crime." *CISA*, https://www.cisa.gov/combatting-cyber-crime. Accessed 4 May 2023.
[164] "China's 'unprecedented' crackdown stunned private enterprise. One year on, it may have to cut business some slack." *CNN*, 3 November 2021, https://www.cnn.com/2021/11/02/tech/china-economy-crackdown-private-companies-intl-hnk/index.html. Accessed 4 M
[165] *Alibaba.com: Manufacturers, Suppliers, Exporters & Importers from the world's largest online B2B marketplace*, https
[166] "China's 'unprecedented' crackdown stunned private enterprise. One year on, it may have to cut business some slack." *CNN*, 3 November 2021, https://www.cnn.com/2021/11/02/tech/china-economy-crackdown-private-companies-intl-hnk/index.html. Accessed 4 May 2023.
[167] "" - *Wiktionary*, https://www.recordedfuture.com/chinese-cybercrime-neighboring-countriesv. Accessed 4 May 2023.
[168] "Global Programme on Cybercrime." *unodc*, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html. Accessed 4 May 2023.
[169] "Global Programme on Cybercrime." *unodc*, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html. Accessed 4 May 2023.
[170] "Cybercrime operations." *Interpol*, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations. Accessed 16 April 2023.

information to help them identify criminals. Over 270 compromised websites were found. [171]

Case Study: Trickbot

Trickbot is a Russian criminal organization that commits cyber crimes against the United States and other countries. Specifically, Trickbot is a trojan virus that steals financial data and creates attacks such as ransomware. During the Covid-19 crisis Trickbot attacked multiple hospitals and medical sites within the US. This group is connected to Russian Intelligence Services.



US and UK sanctions mandate that no American or British citizen can transfer the property of prohibited individuals without reporting it to the OFAC, or the Office of Foreign Assets Control. Additionally, people who trade products with located participants of the Trickbot organization may be subjected to prosecution.[172] As such, this organization has become limited in its actions.

[171] "INTERPOL-led cybercrime operation across ASEAN unites public and private sectors." *Interpol*, 24 April 2017, https://www.interpol.int/en/News-and-Events/News/2017/INTERPOL-led-cybercrime-operation-across-ASEAN-unites-public-and-private-sectors. Accessed 16 April 2023.
[172] "United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang." *Treasury Department*, 9 February 2023, https://home.treasury.gov/news/press-releases/jy1256. Accessed 16 April 2023.

Questions to Consider/Guide to Position Papers

- How can cybercrimes affect individuals and institutions?
- How are cybercrimes committed (specific ways, such as malware)?
- What ideas do you have to prevent cybercrime?
- What has your position done or said in response to cybercrime?
- How does cybercrime most affect the country your position is from?
- How should governments supporting cyber criminal organizations should be held accountable for their actions?

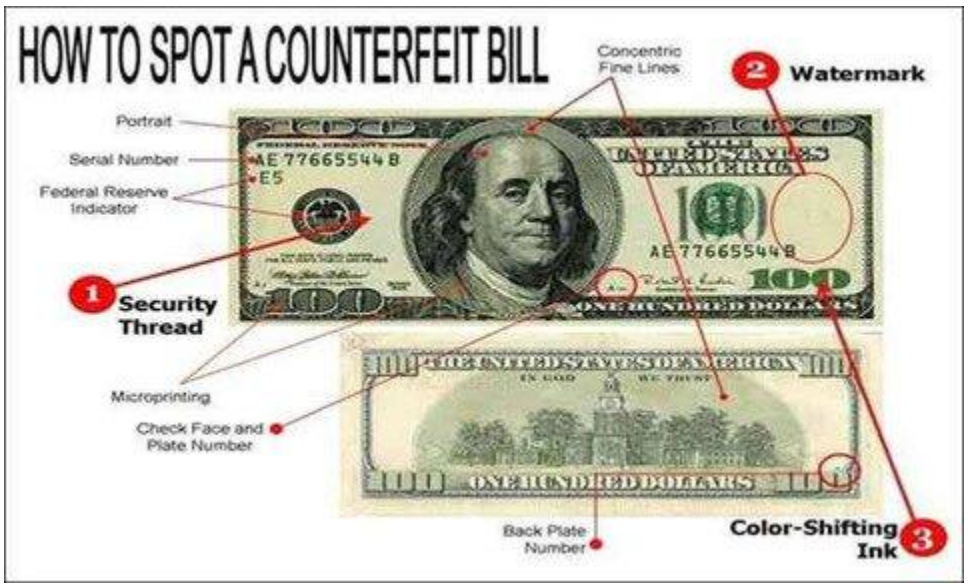
Possible Solutions

- Creation of a rigorous cybersecurity protocol for governments and institutions in member-states to follow
- Creation of a cybersecurity database consisting of the names, pictures, and IP addresses of known cybercriminals as well as the data breached by those cybercriminals
- National law enforcement agencies of member-states can allow INTERPOL to better monitor devices being used by citizens in those member-states
- Establishment of a fund to help promote cybersecurity among public and private institutions

Helpful Websites:

1. Cybercrime
2. More Than 70 Cybercrime Statistics
3. Number of Data Breaches and Victims
4. 6 Ways Cyber Crime Impacts Business
5. A Cyberattack on the US Power Grid
6. Cybercrime and National Security

Topic B: Counterfeit Currency



What is Counterfeit Currency?

All countries use money as a medium of exchange for goods and services called currency.[173] The currency of the United States is the dollar, which you use to buy things in your daily life.[174] Currencies such as the dollar are authorized by the government of their countries, making them legitimate in that they are printed with special traits that make them recognizable and distinguishable from counterfeit currency.

Currency: Medium of exchange for goods and services used by countries.

Counterfeit currency is fake currency which criminals produce without the legal authority or permission of a country.[175] [176] Counterfeit currency is designed to imitate legitimate forms of currency with the intention of deceiving others who possess it.[177]

Counterfeit Currency: Fake currency made without government authorization meant to deceive others it is circulated to.

Counterfeiting currency has had a long and rich history, dating from 400 B.C.E. when Greek coins were counterfeited by covering less valuable metal with a layer of more valuable metal.[178] When notes became a legal form of tender (currency) in America during the 1860s, Mary Butterworth created a new counterfeiting technique of using starched cloth and hot iron to transfer the ink pattern of a Dollar onto a piece of paper, pioneering the counterfeiting of banknotes.[179] [180] During the American Civil War, over a third of all currency in the United States was counterfeit.[181]

Today, counterfeiting currency requires a very careful process of using the right paper and printing the right marks and security features of the currency being replicated in order to be seen

[173]Kelly, Robert. "Currency: What It Is, How It Works, and How It Relates to Money." *Investopedia*, 22 July 2022, https://www.investopedia.com/terms/c/currency.asp. Accessed 2023.
[174]Chen, James, and Hans Daniel Jasperson. "What Is USD (United States Dollar)? Definition, Uses, Importance." *Investopedia*, https://www.investopedia.com/terms/forex/u/usd-united-states-dollar.asp. Accessed 2023.
[175]"Counterfeiting - Manufacturing or Altering Currency - Impact Law." *IMPACT LAW*, https://www.impactlaw.com/criminal-law/white-collar/counterfeiting. Accessed 2023.
[176]"Counterfeit Money." *Kansas City Police Department*, https://www.kcpd.org/crime/crime/economic-crimes/criminal-offenses-investigated/counterfeit-money/. Accessed 2023.
[177]*How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 2023.
[178]Finlay, Richard. "A Brief History of Currency Counterfeiting | Bulletin – September 2019." *Reserve Bank of Australia*, 19 September 2019, https://www.rba.gov.au/publications/bulletin/2019/sep/a-brief-history-of-currency-counterfeiting.html. Accessed 2023.
[179]"History of United States Currency." *MyCreditUnion.gov*, 8 February 2023, https://mycreditunion.gov/financial-resources/history-united-states-currency.
[180]"Great Historical Counterfeits | History Detectives." *PBS*, https://www.pbs.org/opb/historydetectives/feature/great-historical-counterfeits/.Accessed 2023.
[181]"Counterfeiting - Manufacturing or Altering Currency - Impact Law." *IMPACT LAW*, https://www.impactlaw.com/criminal-law/white-collar/counterfeiting. Accessed 2023.

as legitimate.[182] It also requires a great deal of technique, equipment, and financial investment.[183] [184] A variety of methods such as offset printing and bleaching can be used to produce counterfeit currency.[185] [186] With the rise of digital technology, it is also possible to produce counterfeit currency through digital image acquisition, processing, and printing methods.[187]

Counterfeit currency has a direct impact on both countries and individuals . The unauthorized circulation of money into an economy can cause significant inflation.[188] It can be used to fuel organized crime by providing a means financing criminal activity.[189] Beyond this, counterfeit currency also endangers the legitimacy of currencies as it undermines confidence if there are too many counterfeit versions of a currency circulating in an economy.[190] In 2020, the United States Secret Service captured more than $505 million in counterfeit currency, a 40% increase from the year before.[191] In the United Kingdom in 2019, the Bank of England discovered more than 427,000 counterfeit banknotes.[192] The committee will address how to curb and combat the circulation of such currency.

Why Do People Counterfeit Currency?

Criminals of course use counterfeit currency to finance criminal activity.[193] Sometimes, counterfeit currency can be used as a political weapon to undermine national governments. An example of this is Operation Bernhard, undertaken by Nazi Germany between 1942 and 1945

[182]Brain, Marshall, and Dave Roos. "How Counterfeiting Works | HowStuffWorks." *Money | HowStuffWorks*, https://money.howstuffworks.com/counterfeit.htm.Accessed 2023.
[183]Office of Justice Programs. "MODERN TECHNIQUES OF COUNTERFEITING MONEY." https://www.ojp.gov/ncjrs/virtual-library/abstracts/modern-techniques-counterfeiting-money. Accessed 27 April 2023.
[184]Pratte, Emma. "How It Is Made, How It Moves." *American Numismatic Society*, https://numismatics.org/how-it-is-made-how-it-moves/. Accessed 2023.
[185] Pratte, Emma. "How It Is Made, How It Moves." *American Numismatic Society*, https://numismatics.org/how-it-is-made-how-it-moves/.Accessed 2023.
[186] Dri Mark. "Everything You Need to Know about Bleached Bills." 1 March 2023, https://www.drimark.com/everything-you-need-to-know-bout-bleached-bills/. Accessed 2023.
[187] The National Academies Press. "Read "Is That Real?: Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes" at NAP.edu." https://nap.nationalacademies.org/read/11638/chapter/4. Accessed 2023.
[188]"Large number of counterfeit notes may impact inflation."' *The Economic Times*, 14 December 2012, https://economictimes.indiatimes.com/news/economy/finance/large-number-of-counterfeit-notes-may-impact-inflation/articleshow/17615199.cms?from=mdr. Accessed 4 May 2023.
[189]"Counterfeit currency." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency. Accessed 4 May 2023.
[190]"The Social Costs of Currency Counterfeiting." *Reserve Bank of Australia*, 5 May 2015, https://www.rba.gov.au/publications/rdp/2015/pdf/rdp2015-05.pdf. Accessed 4 May 2023.
[191]"UNITED STATES SECRET SERVICE." *Secret Service*, 17 March 2021, https://www.secretservice.gov/sites/default/files/reports/2021-03/2020-Annual-Report.pdf. Accessed 4 May 2023.
[192]Allen, James. "29+ Alarming Counterfeit Money Statistics & Facts (2023)." *Billpin.com*, 18 February 2023, https://www.billpin.com/counterfeit-money-statistics-facts/. Accessed 4 May 2023.
[193]"Counterfeit currency." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency. Accessed 4 May 2023.

during World War 2.[194] Nazi officials produced 134 million British Pounds worth of counterfeit

currency using labor from concentration camps and funneled the money through a network of agents into Britain in order to cause inflation and undermine the country economically.[195] [196] Politically motivated counterfeiting of currency can additionally blur the actions of criminals and the government, which the committee must address. For example, in the 1700s the British created counterfeit Continental currency on boats in the New York Harbor, and was effective in devaluing the currency within the colonies. This aided Britain in weakening the American colonies during the time of the American Revolution. Other times, counterfeit currency is used simply for personal gain as it can provide individuals with an easy way to buy things.[197]

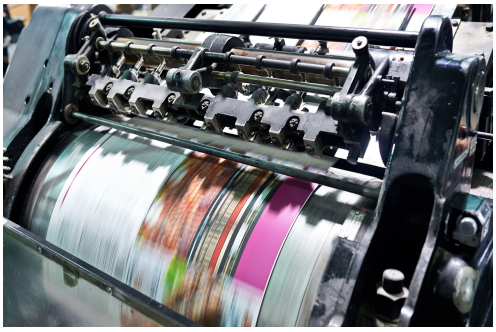
The Process of Counterfeiting

Counterfeiting paper money and counterfeiting coins have different processes. Counterfeiting paper currency requires certain materials that are difficult for a regular consumer to find. The process of bleaching, which will be further explained, was used by Colombian drug cartels, and they used the bills until they were caught by the Secret Service.[198] Columbia has become one of the most major counterfeiting countries of US dollars, so many counterfeit bills are often found as Secret Service agents investigate in Columbia. In January of 2018, a duffel bag of around $953,000 was found to be transported to Orlando from Columbia.[199]

[194]"Operation Bernhard Printing Plate." *International Spy Museum*, https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/operation-bernhard-printing-plate/. Accessed 4 May 2023.
[195]Nye, Logan. "Nazi Germany tried to counterfeit its way to victory." *We Are The Mighty*, 22 October 2020, https://www.wearethemighty.com/mighty-history/nazi-germany-tried-to-counterfeit-its-way-to-victory/. Accessed 4 May 2023.
[196]"Operation Bernhard Printing Plate." *International Spy Museum*, https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/operation-bernhard-printing-plate/. Accessed 4 May 2023.
[197]Finlay, Richard. "A Brief History of Currency Counterfeiting | Bulletin – September 2019." *Reserve Bank of Australia*, 19 September 2019, https://www.rba.gov.au/publications/bulletin/2019/sep/a-brief-history-of-currency-counterfeiting.html. Accessed 4 May 2023.
[198]Pratte, Emma. "How It Is Made, How It Moves." *American Numismatic Society*, https://numismatics.org/how-it-is-made-how-it-moves/. Accessed 4 May 2023.
[199]"." *" - Wiktionary*, https://www.orlandosentinel.com/2003/03/01/secret-service-tracks-mystery-of-fake-fortune/. Accessed 4 May 2023.

Counterfeiting Paper Money

The counterfeiting of paper money involves multiple processes. One is **offset printing**, since it is often used to print real money. Offset printing is the process of mass printing with metal plates that are then placed onto rubber rollers.[200] Offset printing does not mean that the money will look exactly like authorized currency, since it is difficult to replicate the way money feels and looks.[201]



Another process is bleaching, where bills of low value are bleached until all existing marks disappear. These bills can then be remade as bills of higher value.[202] Legal bills use types of paper that are hard to replicate, so this method allows for the criminal to create money that seems authentic. For example, US paper currency requires a special type of paper called rag paper, which is generally much thinner than regular paper and doesn't wear away if washed

Currency can also be counterfeited through digital imaging technology. The criminal copies the image of the paper money digitally through scanners. The image then goes through a process that gives it more depth. After capturing the image of the currency, it then undergoes processing to ensure perfect replication including adjusting the colors of the bills and fixing small mistakes, such as dust or brightness.. After all mistakes are removed from the image, it is printed. A small number of specific expensive printers can produce high quality currency.[203]

Counterfeiting Coins

Like paper currencies, coins can also be altered to seem like they have more value. This is often done to fake rare coins that reach high prices from collectors.

---

[200] "What is offset printing (offset lithography)? | Definition from TechTarget." *TechTarget*, https://www.techtarget.com/whatis/definition/offset-printing-offset-lithography. Accessed 4 May 2023.
[201] "<B><H1> Offset Printing Counterfeit Money - Is it Possible?</B></H1> ." *The Offset Pressman*, 21 July 2020, http://www.offsetprinting.info/2020/07/offset-printing-counterfeit-money-is-it.html. Accessed 4 May 2023.
[202] "Everything You Need to Know about Bleached Bills." *Dri Mark*, 1 March 2023, https://www.drimark.com/everything-you-need-to-know-bout-bleached-bills/. Accessed 4 May 2023.
[203] "Read "Is That Real?: Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes" at NAP.edu." *The National Academies Press*, https://nap.nationalacademies.org/read/11638/chapter/4#20. Accessed 4 May 2023.

There are three types of counterfeit coins: struck counterfeits, cast counterfeits, and altered and doctored counterfeits. Struck counterfeit coins are created using hand engraved coin dies, which are metal tools used to stamp the coins' imprints.[204] However, coin dies are expensive so this method is used for more expensive coins. Cast counterfeit coins are made by pouring metal into coin molds. This type of counterfeit is the least authentic. Lastly, altered and doctored counterfeit coins use regular coins and make modifications so that they look like coins of higher value.[205] All of these types of counterfeit coins are sold for high prices, scamming collectors.

Confidence in Currencies:

As counterfeit currency become more prevalent , people lose trust in their country's currency. This can have extremely negative consequences, since the value of money is based on what can be done with it. If people believe that there is a risk that they may be earning or accepting counterfeit currency instead of government authorized currencies, then confidence in the currency weakens.[206] This can lead to currency devaluation, where a currency's value decreases, generally due to government monetary policy.[207] As the value of a currency decreases, both imports and exports of goods become more expensive, since they have to pay more of their own currency to match the value of the product. This can lower overall economic productivity and GDP.[208]

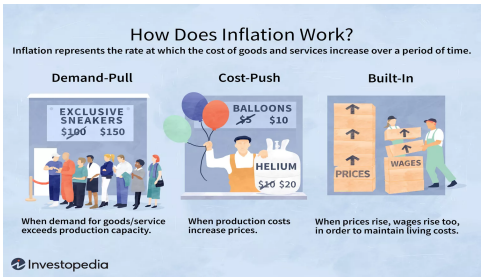
[204]Unser, Mike. "What is a Coin Die? Are They Worth Anything? | CoinNews." *Coin News*, 6 July 2007, https://www.coinnews.net/2007/07/06/what-is-a-coin-die-are-they-worth-anything/. Accessed 4 May 2023.
[205]Bucki, James. "How to Detect Counterfeit Coins." *The Spruce Crafts*, 21 September 2022, https://www.thesprucecrafts.com/how-to-detect-counterfeit-coins-4163525. Accessed 4 May 2023.
[206]"The Social Costs of Currency Counterfeiting." *Reserve Bank of Australia*, 5 May 2015, https://www.rba.gov.au/publications/rdp/2015/pdf/rdp2015-05.pdf. Accessed 4 May 2023.
[207]"What is devaluation and how does it affect my finances?" *Banco Santander*, 5 September 2022, https://www.santander.com/en/stories/devaluation. Accessed 4 May 2023.
[208]Hayes, Adam. "3 Reasons Why Countries Devalue Their Currency." *Investopedia*, https://www.investopedia.com/articles/investing/090215/3-reasons-why-countries-devalue-their-currency.asp. Accessed 4 May 2023.

Additionally, a decrease in trust in a country's currency means that consumers will use a different type of payment method. Generally, electronic payments are chosen instead of physical currencies. In Australia, this had a social cost of about A$7 million, or around 4,684,400 US dollars, as the amount of counterfeit money amounted to around A$140,000.[209] Furthermore, there is also greater general risk of hacking with the usage of online payment forms. Thus, the usage of alternative methods of payment can further undermine a country's economy.

The Difficulty in Identifying Counterfeit Currency

The process used to counterfeit currency allows such currency to seem fully authentic. With the information that is provided online, it is very easy for criminals to counterfeit both paper money and coins.[210]

Economic Effects



Inflation

One of the principal effects of the circulation of counterfeit currency into an economy is inflation, an increase in prices for goods and services in an economy. As the money supply of a country grows, people in that country, now having more money, can buy more goods and services. This causes a shortage in the supply of goods and services while demand for those goods and services increases. As a result, goods and services become more scarce and in turn more valuable, causing the prices of those goods and services to increase.[211] This specific form of inflation is referred to as demand-pull inflation, which exists along with cost-push inflation.[212]

When criminals produce counterfeit currency, they are putting an increased amount of currency in the money supply,

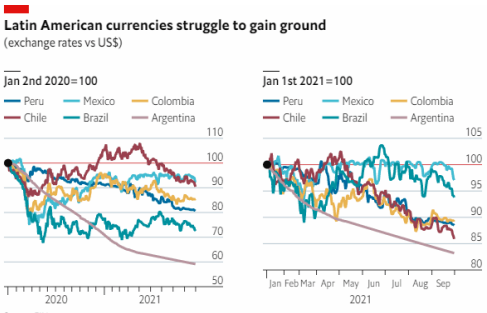
[209] "The Social Costs of Currency Counterfeiting." *Reserve Bank of Australia*, 5 May 2015, https://www.rba.gov.au/publications/rdp/2015/pdf/rdp2015-05.pdf. Accessed 4 May 2023.
[210] Trundy, Sean. "Why is Counterfeit Currency so Hard to Detect?" *Fraud Prevention Blog*, https://blog.fraudfighter.com/bid/75690/Why-is-Counterfeit-Currency-so-Hard-to-Detect. Accessed 6 May 2023.
[211] *How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[212] "Inflation: What It Is, How It Can Be Controlled, and Extreme Examples." *Investopedia*, https://www.investopedia.com/terms/i/inflation.asp. Accessed 4 May 2023.

which creates higher inflation.[213] The consequences of counterfeit currency-induced inflation begin with its harm to consumers. When the prices of goods and services in a particular country increase as a result of such inflation, consumers in that country can now buy less with the wages they earn , leading to a reduction in their purchasing power.[214] This eventually hurts people's accessibility to goods and services[215] and can lead to an affordability crisis.[216] Argentina, which has suffered from a high level of counterfeit currency, has experienced alarming levels of inflation, which has historically been attributed to a rapid increase in the money supply, thus indicating a correlation between counterfeit currency and inflation in the country.[217][218] In 2022, it faced an inflation rate of 90%, which had increased to 100% by 2023.[219][220]

Devaluation of Currencies

The circulation of counterfeit currency in the economy can lead to the devaluation of legitimate currencies because less goods and services can be purchased with the currency of a particular country when counterfeit currency-induced inflation occurs in that country, that currency becomes less used and in turn less valuable compared to currencies from other countries.[221][222] As a result, it becomes more expensive to convert that currency to other currencies in other countries.

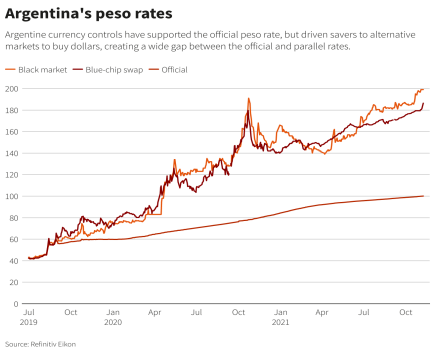
It becomes harder for countries suffering from such currency devaluation to participate in international financial markets and for consumers in those countries to purchase goods imported from other

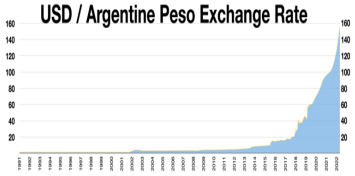


[213] *How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[214] "Inflation: Prices on the Rise." *International Monetary Fund*, https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Inflation. Accessed 4 May 2023.
[215] "Tackling inflation and margin pressure in the sporting goods industry." *McKinsey*, 5 July 2022, https://www.mckinsey.com/industries/retail/our-insights/tackling-inflation-and-margin-pressure-in-the-sporting-goods-industry. Accessed 4 May 2023.
[216] Smith, Carl. *Record Inflation Deepens America's Affordable Housing Crisis*, 17 March 2022, https://www.governing.com/community/record-inflation-deepens-americas-affordable-housing-crisis. Accessed 4 May 2023.
[217] "Fake Money in Argentina." *San Telmo Loft*, 22 July 2011, https://santelmoloft.com/2011/07/22/fake-money-in-argentina/. Accessed 4 May 2023.
[218] "Argentina attempts to tame hyperinflation." *GIS Reports*, 17 November 2022, https://www.gisreportsonline.com/r/argentina-hyperinflation-economy/. Accessed 4 May 2023.
[219] "How Argentines Cope With Inflation That's 64% and Rising." *The New York Times*, 7 August 2022, https://www.nytimes.com/2022/08/06/business/inflation-argentina.html. Accessed 4 May 2023.
[220] "Argentina attempts to tame hyperinflation." *GIS Reports*, 17 November 2022, https://www.gisreportsonline.com/r/argentina-hyperinflation-economy/. Accessed 4 May 2023.
[221] *How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[222] Lowry, Christy. "Inflation, Interest & Exchange Rates." *Western Union*, 9 December 2022, https://www.westernunion.com/blog/en/us/how-inflation-affects-currency-and-interest-rates/. Accessed 4 May 2023.

countries as converting between currencies becomes more expensive.

An example can be seen in a hypothetical scenario, let's say country A's currency is the Ruby, and country B's currency is the Silver. So far, the Ruby and Silver are equally valuable with 1 Ruby equaling 1 Silver in currency exchanges. As a result of inflation caused by counterfeit currency artificially increasing the money supply in Country A, Country A's purchasing power decreases and less goods and services can be bought with the Ruby, causing less people to use the Ruby. Instead, demand for the Silver goes up and more people in Country A begin using the Silver when making purchases as they see it as a more stable currency. Now, the Silver, purchased more in exchanges, is twice as valuable as the Ruby, and in currency exchanges 1 Silver now equals 2 Rubies. Or, 1 Ruby equals 0.5 Silvers. If somebody from Country A wants to purchase financial assets from Country B and needs 100 Silvers to do so, before, it would have cost them 100 Rubies. But now, it would cost 200 Rubies. Likewise, the price of a good imported from Country B to Country A worth 10 Silvers was 10 Rubies before, but is now 20 Rubies. However, when countries face currency devaluation, the goods which they export to other countries become cheaper and may as a result be purchased more. If Country A exports a good to Country B worth 10 Rubies, while it may have costed 10 Silvers in Country B before, because 1 Ruby now equals 0.5 Silvers, it would only cost 5 Silvers in Country B now, and more people from Country B may buy that good as it is now cheaper.[223] [224]





In Argentina, the nation's high rates of inflation, partly caused by counterfeit currency, has made the country's national currency, the Peso, rarely used as citizens in the country have lost confidence in its stability. . The US Dollar, seen as a more stable currency, has

[223] Lowry, Christy. "Inflation, Interest & Exchange Rates." *Western Union*, 9 December 2022, https://www.westernunion.com/blog/en/us/how-inflation-affects-currency-and-interest-rates/. Accessed 4 May 2023.
[224] "Importing & Exporting Economic Impacts Explained." *Investopedia*, https://www.investopedia.com/articles/investing/100813/interesting-facts-about-imports-and-exports.asp. Accessed 4 May 2023.

become more commonly used in place of the Peso.[225] [226] As a result, the Peso's value has collapsed in international currency exchanges. In one currency exchange in January of 2022, $1 equaled 102.679 Pesos in exchanges, and by January of 2023, $1 equaled 176.71 Pesos, the Peso losing roughly 72.0% of its value against the US Dollar.[227]

Effects on Businesses and Employment

The circulation of counterfeit currency can have dangerous effects on business and employment as well. One way is through the dumping of cheap goods by foreign countries. When a country faces counterfeit currency-induced inflation with consumers in that country requiring goods at lower prices, foreign countries, seeing the demand for cheap goods in that country, may export, or "dump," large quantities of cheap quality goods at cheap prices to that country.[228] When this occurs, the consumers of that country will buy more cheap foreign goods and less goods produced by domestic businesses. And as a result, those businesses will lose money and may have to scale down operations by reducing production and laying off workers, causing higher unemployment.[229]

Non-Reimbursements

As a result of counterfeit currency being circulated , it can land in the hands of individuals and businesses without them realizing.[230] In many countries, including the United States, when someone does realize they have acquired counterfeit currency, they are not allowed to use or pass such currency on

[225]"How Argentines Cope With Inflation That's 64% and Rising." *The New York Times*, 7 August 2022, https://www.nytimes.com/2022/08/06/business/inflation-argentina.html. Accessed 4 May 2023.
[226]"Argentina attempts to tame hyperinflation." *GIS Reports*, 17 November 2022, https://www.gisreportsonline.com/r/argentina-hyperinflation-economy/. Accessed 4 May 2023.
[227]"US Dollar to Argentine Peso Exchange Rate Chart." *Xe*, https://www.xe.com/currencycharts/?from=USD&to=ARS&view=2Y. Accessed 4 May 2023.
[228]*How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[229]"Do Cheap Imported Goods Cost Americans Jobs?" *Investopedia*, 1 May 2023, https://www.investopedia.com/articles/economics/09/free-market-dumping.asp. Accessed 4 May 2023.
[230]Gustafson, Katherine. "Banking 101: What to Do If You Receive Fake Money." *Deposit Accounts*, 19 June 2019, https://www.depositaccounts.com/blog/fake-money.html. Accessed 4 May 2023.

and must turn in to government authorities.[231] [232] [233] [234] Similarly, when counterfeit currency is discovered in banks, it is confiscated.[235] However, it is unlikely that banks or governments will reimburse individuals and businesses by providing them real currency.. As a result, individuals and businesses can face serious financial losses when counterfeit currency is circulated to them.[236] [237]

Black Marketing

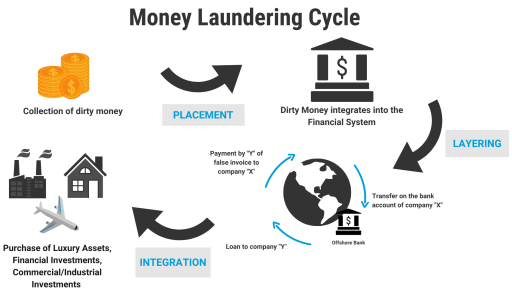
When consumers buy more goods with the increase in money supply from the circulation of counterfeit currency, the subsequent shortage of the supply of goods can lead to another phenomenon, called black marketing.[238] During a shortage of goods, entities with enough inventory can hoard such goods and sell them at higher prices.[239] Transactions are usually made in cash without any records in order to evade taxes.[240] The increases in prices caused by black marketing are similar to that of the effects of inflation and serve to make goods and services less accessible to the public.[241] In fact, black marketing can exacerbate the effects of inflation on society. In Venezuela, at the same time inflation had hit 180% by the end of 2015, increases in prices in the black market were more than 2 times more at 380%.[242][243]

[231]"What to do if you get a fake note, what's the punishment for offence related to counterfeit currency?" *The Economic Times*, 27 March 2023, https://economictimes.indiatimes.com/news/how-to/what-to-do-if-you-get-a-fake-note-whats-the-punishment-for-offence-related-to-counterfeit-currency/articleshow/99035131.cms. Accessed 4 May 2023.
[232]"Criminal Code." *Criminal Code*, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-58.html. Accessed 4 May 2023.
[233]"How do I determine if a banknote is genuine? What should I do if I think I have a counterfeit note?" *Federal Reserve Board*, 4 January 2018, https://www.federalreserve.gov/faqs/currency_12597.htm. Accessed 4 May 2023.
[234]Gustafson, Katherine. "Banking 101: What to Do If You Receive Fake Money." *Deposit Accounts*, 19 June 2019, https://www.depositaccounts.com/blog/fake-money.html. Accessed 4 May 2023.
[235]"Could I Accidentally Receive Fake Money From a Bank?" *Carnation Money Counter*, https://carnation-inc.com/blogs/money-handling-blog/could-i-accidentally-receive-fake-money-from-a-bank. Accessed 4 May 2023.
[236]Gustafson, Katherine. "Banking 101: What to Do If You Receive Fake Money." *Deposit Accounts*, 19 June 2019, https://www.depositaccounts.com/blog/fake-money.html. Accessed 4 May 2023.
[237]*How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[238]*How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[239]Vaidya, Dheeraj. "Rationing - Meaning, Examples, Economic Effects, Advantages." *WallStreetMojo*, https://www.wallstreetmojo.com/rationing/. Accessed 4 May 2023.
[240]Khartit, Khadija. "Black Market Definition." *Investopedia*, https://www.investopedia.com/terms/b/blackmarket.asp. Accessed 4 May 2023.
[241]*How Does Counterfeit Money Affect the Economy and Society?*, https://opinionfront.com/how-does-counterfeit-money-affect-economy. Accessed 4 May 2023.
[242]Cerra, Valerie. "Inflation and the Black Market Exchange Rate in a Repressed Market: A Model of Venezuela." *International Monetary Fund*, https://www.imf.org/external/pubs/ft/wp/2016/wp16159.pdf. Accessed 4 May 2023.
[243]Cerra, Valerie. "Inflation and the Black Market Exchange Rate in a Repressed Market: A Model of Venezuela." *International Monetary Fund*, https://www.imf.org/external/pubs/ft/wp/2016/wp16159.pdf. Accessed 4 May 2023.

Promotion of Criminal Activity

Counterfeit currency can be used to finance criminal activity. Criminal organizations can use counterfeit currency to pay for weapons, equipment, training, traveling, as well as food and shelter and transportation.[244] [245]

Money Laundering



Criminals launder counterfeit currency to turn their counterfeit currency into legitimate funds.. Smurfing involves the deposit of small denominations of counterfeit currency into multiple bank accounts, allowing criminals to transfer their illicit currency into legitimate bank funds and minimize the chance of raising any detection or suspicion.[246]

Criminals can launder counterfeit currency through currency exchanges where they purchase foreign currency using their counterfeit currency followed by a purchase of assets to provide an income stream. They can also transfer their funds internationally to offshore accounts. Using foreign currency allows criminals to hide the origins of their funds and makes it harder for law enforcement authorities to track down their financial movements. [247]

Criminals can also launder counterfeit currency through performing complex financial transactions involving shell companies and offshore accounts and using fake invoices (bills companies make to charge for goods and services) or receipts (documents certifying payments),[248] through which they can move around their counterfeit funds.[249] [250] [251] [252]

---

[244] "Counterfeit currency." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency. Accessed 4 May 2023.
[245] "Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors." *OECD*, 10 June 2019, https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf. Accessed 4 May 2023.
[246] "Blog / Money Laundering Related to Counterfeiting Of Currency." *Sanction Scanner*, https://sanctionscanner.com/blog/money-laundering-related-to-counterfeiting-of-currency-423. Accessed 4 May 2023.
[247] "Blog / Money Laundering Related to Counterfeiting Of Currency." *Sanction Scanner*, https://sanctionscanner.com/blog/money-laundering-related-to-counterfeiting-of-currency-423. Accessed 4 May 2023.
[248] "Free Receipt Templates | Samples - Word | PDF – eForms." *eForms*, 15 December 2022, https://eforms.com/receipt/. Accessed 4 May 2023.
[249] "Blog / Money Laundering Related to Counterfeiting Of Currency." *Sanction Scanner*, https://sanctionscanner.com/blog/money-laundering-related-to-counterfeiting-of-currency-423. Accessed 4 May 2023.
[250] "money laundering | Wex | US Law | LII / Legal Information Institute." *Law.Cornell.Edu*, https://www.law.cornell.edu/wex/money_laundering. Accessed 4 May 2023.
[251] "What is an Invoice? How do I Make an Invoice?" *Square*, https://squareup.com/us/en/the-bottom-line/operating-your-business/invoices. Accessed 4 May 2023.
[252] "money laundering | Wex | US Law | LII / Legal Information Institute." *Law.Cornell.Edu*, https://www.law.cornell.edu/wex/money_laundering. Accessed 4 May 2023.

Terrorism

Terrorist networks often employ counterfeit currency in order to acquire resources and finance attacks.[253] In India in 2015, before the 500 Rupee note was removed as a legal form of currency, more than 95% of counterfeit 500 Rupee notes were found to be in the hands of terrorists who were using it to fund terrorist activities.[254] In the 26/11 Terrorist Attacks of 2011, the Kashmir based group, Lashkar-e-Taiba, launched a major attack on Mumbai, Before the attack, one of the individuals involved was given 40,000 Rupees in counterfeit currency to pay for his expenses while gathering information on the city. In The United States in 2009, 4 individuals were indicted by Federal authorities for selling $9,800 in counterfeit US currency in order to raise funds for Hizbollah (Hezbollah), a Lebanese terrorist group supported by Iran.[255] [256]

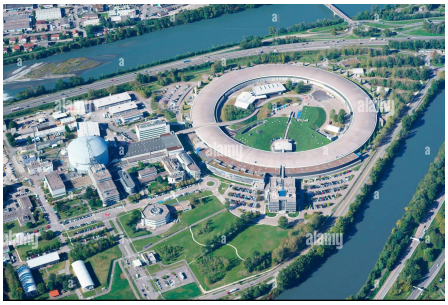
What Has Been Done?

International Community

The global community has acted multi-laterally to combat counterfeit currency. In 1929, the International Convention on the Suppression of Counterfeiting Currency criminalized counterfeit currency globally.[257]

Europe

The European Union (EU)'s strategy to minimize the presence of counterfeit currency is based on 4 pillars: prevention, repression, training, and cooperation. The EU prevents the proliferation of counterfeit Euros through a system of information sharing related to counterfeit currency,



[253]"Money Laundering and Terrorist Financing Related to Counterfeiting of Currency." *FATF*, 11 December 2012, https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-terrorist-financing-related-to-counterfeit-currency.pdf. Accessed 4 May 2023.
[254]GURUNG, SHAURYA KARANBIR. "Pakistan, the biggest contributor of fake Rs 500, Rs 1000 notes; PM Narendra Modi's historic move justified." *The Economic Times*, 10 November 2016, https://economictimes.indiatimes.com/news/defence/fake-currency-worth-rs-167-crore-seized-by-government-in-five-years-pakistan-a-big-contributor-to-it/articleshow/55355933.cms. Accessed 4 May 2023.
[255]"Four Indicted for Conspiring to Support Hizballah; Six Others Charged with Related Crimes." *FBI*, 24 November 2009, https://archives.fbi.gov/archives/philadelphia/press-releases/2009/ph112409.htm. Accessed 4 May 2023.
[256]Hamiyah, Talal. "Lebanese Hezbollah." *CRS Reports*, 11 January 2023, https://crsreports.congress.gov/product/pdf/IF/IF10703. Accessed 4 May 2023.
[257]"Papers relating to the foreign relations of the United States, 1929, Volume I - Office of the Historian." *History State Gov*, https://history.state.gov/historicaldocuments/frus1929v01/d236. Accessed 4 May 2023.

cash authentication systems employed by credit card and cash institutions, as well as the use of national authorities designated to analyze information related to counterfeit currency and national central offices in member states to coordinate and oversee investigations related to counterfeit currency.

The European Technical and Scientific Centre assists national authorities in analyzing and investigating counterfeit currency through technical assistance, training, and provides information on the types and classifications of counterfeit currency.

Directive 2014/62/EU looks to repress the circulation of counterfeit currency through new criminal law measures, mandating national authorities to authenticate, detect, and dispose of all Euro coins unsuitable for circulation (counterfeit coins). **The Pericles 2020 Programme** is an initiative undertaken by the European Central Bank, Europol, and the Directorate-General for Economic and Financial Affairs which aims to train law enforcement authorities, judicial authorities, banks, and other financial institutions by providing funding for staff exchanges, seminars, as well as training and study materials. Experts Group, an EU organization, brings together various experts from EU member states, the European Central Bank, Europol, as well as INTERPOL to engage in multidisciplinary and multilateral cooperation in discussing solutions towards counterfeit currency.[258]

The Bank of England (the UK's Central Bank) uses a 5 step strategy: investing in the development of new counterfeit-resilient banknotes, collaborating with financial institutions to ensure only authentic currency can be issued and recirculated, providing a new framework for financial companies to test that their equipment maintains minimum standards for authenticating cash, developing close relations with law enforcement agencies in the UK in order to target currency counterfeiting operations, as well as establishing an educational program to teach individuals and businesses how to recognize counterfeit currency. As the scope of individuals affected by counterfeit currency increases, more people may be motivated to learn

[258]"Anti-counterfeiting - Anti-counterfeiting measures." *Economy and Finance*, https://economy-finance.ec.europa.eu/euro/anti-counterfeiting/anti-counterfeiting-measures_en. Accessed 4 May 2023.

from educational programmes such as this These steps appear to be working as less than 1 in 30,000 notes of UK currency in circulation are counterfeit in 2022.[259]

Latin America

Latin America is also restricting the circulation of counterfeit currency. The Financial Task Force of Latin America was formed in 2020, consisting of 17 countries to help curb the spread of illicit cash and financing by creating a set of recommendations for member states to follow.[260][261] So far, multiple member states have made considerable progress in implementing these recommendations.[262]

There have also been examples of interregional efforts to combat counterfeit currency. Columbia has a history of extensive cooperation with the United States Secret Service in operations to identify and seize counterfeit currency.[263] One such operation was in Toro, where the Colombian National Police Service worked with the US Secret Service in 2003 uncovering more than 20 million US Dollars in counterfeit currency on a farm. This operation is one of the biggest seizures of an active counterfeiting plant in Colombian history.[264] This level of cooperation helped reduce Colombian-made counterfeit currency circulating in the United States by 37% between 2002 and 2003.[265]

United States

The United States Secret Service protects the integrity of US financial institutions and the US Dollar, employing sophisticated resources and partnerships with

[259]"Counterfeit banknotes." *Bank of England*, 24 April 2023, https://www.bankofengland.co.uk/banknotes/counterfeit-banknotes. Accessed 4 May 2023.
[260]"Financial Action Task Force of Latin America (GAFILAT)." *FATF*, https://www.fatf-gafi.org/en/countries/global-network/financial-action-task-force-of-latin-america--gafilat-.html. Accessed 4 May 2023.
[261]"International cooperation." *Sepblac*, https://www.sepblac.es/en/abt-sepblac/international-cooperation/. Accessed 4 May 2023.
[262]"Financial Action Task Force of Latin America (GAFILAT)." *FATF*, https://www.fatf-gafi.org/en/countries/global-network/financial-action-task-force-of-latin-america--gafilat-.html. Accessed 4 May 2023.
[263]Faries, Bill. "Made in South America: new breed of fake US dollars." *Christian Science Monitor*, 14 April 2005, https://www.csmonitor.com/2005/0414/p10s01-woam.html. Accessed 4 May 2023.
[264]"Colombian Police and United States Secret Service Seize $20 Million in Counterfeit U.S. Currency | United States Secret Service." *Secret Service*, 12 February 2003, https://www.secretservice.gov/press/releases/2003/02/colombian-police-and-united-states-secret-service-seize-20-million. Accessed 4 May 2023.
[265]Faries, Bill. "Made in South America: new breed of fake US dollars." *Christian Science Monitor*, 14 April 2005, https://www.csmonitor.com/2005/0414/p10s01-woam.html. Accessed 4 May 2023.

businesses as well as local, state, federal, and international law enforcement agencies in investigations and law enforcement operations on illicit financial activities..[266]

A pilot secret service website was made by the US Government which allowed law enforcement agencies and currency handlers around the world to report instances of counterfeit currency.[267] This program has had success in countries like Peru where the US Secret Service seized more than 75 million US Dollars in counterfeit currency between 2009 and 2016.[268]

The Federal Reserve Bank of New York has cash depots at foreign banks to replace old US currency with new US currency without it having to be transported from the US. This allows the US Government to collect any overseas counterfeit US currency and better promote the circulation of real US currency. US law enforcement agencies have been collaborating with foreign authorities to better target countries where counterfeit currency is first moved to in order to impede the global distribution of counterfeit currency.[269]

In addition, the US Government has established **the Advanced Counterfeit Deterrence Steering Committee** consisting of representatives from the US Treasury Department, Federal Reserve Board, and the Secret Service tasked with creating a new design for US currency with advanced security featuring new emerging technologies in order to lower the ability for criminals to successfully counterfeit US currency.[270]

The US Government also integrated new security adjustments to US Dollars in the 2000s, such as utilizing microprinting technology, adding a 3-D security ribbon, setting different roughness for different parts of a bill (raised printing), adding a security thread and watermark, and the addition of more changes in color throughout the bill.[271]

[266]"United States Secret Service." *United States Secret Service*, https://www.secretservice.gov/about/overview. Accessed 4 May 2023.
[267]"U.S. EFFORTS TO COMBAT GLOBAL COUNTERFEITING ARE WORKING." *Treasury Department*, https://home.treasury.gov/news/press-releases/ls428. Accessed 4 May 2023.
[268]Holley, Peter. "They make the finest counterfeit money in the world. The U.S. just recovered $30 million worth." *The Washington Post*, 22 November 2016, https://www.washingtonpost.com/news/post-nation/wp/2016/11/22/they-make-fake-money-worth-more-than-cocaine-the-u-s-just-recovered-30-million-of-it/#. Accessed 4 May 2023.
[269]"U.S. EFFORTS TO COMBAT GLOBAL COUNTERFEITING ARE WORKING." *Treasury Department*, https://home.treasury.gov/news/press-releases/ls428. Accessed 4 May 2023.
[270]"U.S. Currency Getting a Facelift - Puloon ATMS." *Puloon ATMs*, 27 January 2023, https://puloonatms.com/u-s-currency-getting-a-facelift/. Accessed 4 May 2023.
[271] United States Government. "The Latest In U.S. Currency Design." *The U.S. Currency Education Program*, www.uscurrency.gov/sites/default/files/download-materials/en/--new100--100_booklet.pdf.

So far, many of these steps have been considered fairly effective given the considerably low rate of US counterfeit currency. There is 1 counterfeit US currency note for every 10,000 legitimate notes.[272]

Russia

Russia has special characteristics on their rubles, such as a metallic thread in the note, a type of nonmetallic ink, etc.[273] However, as the ruble decreases in value, the amount of US counterfeit currency in Russia continues to rise. People have started to use USD instead of rubles in order to try and prevent inflation for their businesses, leading to an increased amount of

counterfeit dollars in circulation. Russia has found over a million counterfeit dollars from an international crime organization.[274] For imports and exports, Russia has its Law on Customs Regulations, trademark holders may send a record of their rights to the Customs IP Register. This allows customs to make routine inspections of goods including intellectual property. Governments can submit their "trademark" to this organization to have better restrictions on traveling counterfeit goods.[275]

China

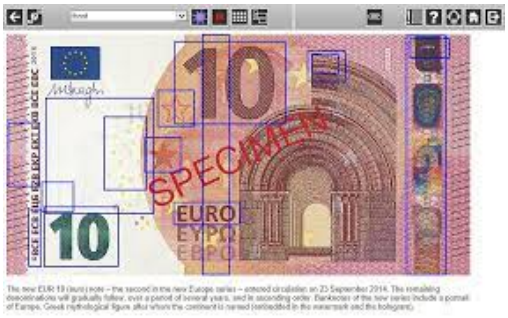
In 2015, China released new 100 yuan notes with special characteristics, such as color changing ink and more complicated designs, which makes them more difficult to replicate[276] . Additionally, the Chinese government has implemented punishments

[272]Allen, James. "29+ Alarming Counterfeit Money Statistics & Facts (2023)." *Billpin.com*, 18 February 2023, https://www.billpin.com/counterfeit-money-statistics-facts/. Accessed 4 May 2023.
[273]"Banknotes | Bank of Russia." *Banknotes | Bank of Russia*, 30 June 2022, https://www.cbr.ru/eng/cash_circulation/banknotes/100rub/?tab.current=y2004. Accessed 4 May 2023.
[274]CHAZAN, GUY. "Russia seizes 1 million counterfeit dollars." *UPI.com*, 17 December 1992, https://www.upi.com/Archives/1992/12/17/Russia-seizes-1-million-counterfeit-dollars/2989724568400/. Accessed 4 May 2023.
[275]Aylen, David. "Procedures and strategies for anti-counterfeiting: Russia." *World Trademark Review*, 18 May 2017, https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2017/article/procedures-and-strategies-anti-counterfeiting-russia. Accessed 4 May 2023.
[276]Quito, Anne. "China subtly redesigned its new 100-yuan bill to confound counterfeiters." *Quartz*, https://qz.com/549621/china-subtly-redesigned-its-new-100-yuan-bill-to-confound-counterfeiters. Accessed 4 May 2023.

for those who counterfeit currency, such as fines or imprisonment.[277]

INTERPOL Actions

One of the original mandates of INTERPOL was to combat counterfeit currency. INTERPOL provides several online tools and services to law enforcement authorities of member states to keep them alert and informed about the circulation of counterfeit currency. These include counterfeit alerts, counterfeit currency statistics, detailed alerts by the European Central Bank and Europol about counterfeit Euro banknotes, as well as Documentchecker Banknotes, a reference database by a company called Keesling Technology which allows authorities to authenticate more than 4,800 types of banknotes, containing information on security features of various currencies and a library of 70,000 images of currencies.[278]



INTERPOL has established a research project with 120 forensic examiners from 54 member states to create a new forensic protocol for identifying counterfeit documents such as counterfeit currency by examining ink patterns. The resulting protocol provides a way for investigators of counterfeit currency to analyze how the movement of ink patterns on counterfeit notes can be used to date such notes (find the time it was created). The protocol also gives investigators a way to investigate such notes in a non-destructive manner such that the evidence investigators use can be preserved.[279]

In 2011, INTERPOL collaborated with the United Nations Office on Drugs and Crime (UNODC) to create the Train-the-Trainer Programme, which teaches law enforcement authorities in member states including immigration officers, forensic analysts,

[277] "Article Content Title: Criminal Code of the Republic of China (2013.06.11 Amended) Part 1 General Provisions Chapter 1." *ILO*, 4 November 2014, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/80254/112858/F-1444561515/CHN80254%20Eng.pdf. Accessed 4 May 2023.
[278] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.
[279] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.

prosecutors, and judicial officials how to recognize counterfeit documents and allows them to share intelligence on counterfeit documents. INTERPOL created an E-Learning module on security document examination, funded by the US Department of State, which provides officials a virtual space to learn about counterfeit documents.[280]

Project S-Print brings together law enforcement authorities and more than 25 businesses in the security printing industry across the world to share knowledge about counterfeit documents. Businesses in the program are encouraged to take security practices such as maintaining full records of transactions, verifying customers, avoiding supplying materials to suspicious customers, reporting suspicious orders to the police, and responsibly disposing of obsolete equipment.[281]

In 2019, INTERPOL convened the Conference on Counterfeit Currency in Lyon, France, in which 120 experts from law enforcement authorities, monetary authorities (such as central banks), international organizations, and businesses, from 47 countries, met to discuss new trends in counterfeiting currency, new developments in security and authentication tools for banknotes, the role of the Darknet (shady websites where many criminals sell counterfeit currency), and how to better secure banknotes.[282] [283] [284] [285]

Case study: Frank Bourassa

In 2004, Frank Bourassa, a Canadian former factory owner and cannabis grower, began the process of creating an illegal counterfeit currency operation. In 2008, Bourassa was successfully able to convince a Swiss paper mill to provide him paper which was 75% cotton and 25% linen which he would need to print fake 20 US Dollar counterfeit bills. He lied to the company saying that he was working in an investment company

[280] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.
[281] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.
[282] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.
[283] "The Dark Web: what is it and why do people use it?" *CEOP Education*, https://www.thinkuknow.co.uk/professionals/our-views/the-dark-web/. Accessed 4 May 2023.
[284] Muncaster, Phil. "Dark Web Posts Advertising Counterfeit Cash Surge 90%." *Infosecurity Magazine*, 26 January 2023, https://www.infosecurity-magazine.com/news/dark-web-posts-advertising/. Accessed 4 May 2023.
[285] "Counterfeit currency and documents conferences." *Interpol*, https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences. Accessed 4 May 2023.

and needed paper to print $20 bond bills. After receiving the paper in 2009 and with the help of a printing expert, he used several Heidelberg 4-color offset presses, a type of offset printer, to print 12.5 million counterfeit $20 bills with the paper he received worth a total of 250 million US Dollars of fake currency. The operation cost him a total of 325,000 Canadian Dollars but in 2010 he was ready to sell the currency at 30% of their fake value to criminal gangs involved in the import/export business.

In 2012, after selling $50 million of fake currency, earning a profit of $15 million Dollars, he was apprehended and arrested by Canadian authorities. After spending 6 weeks in prison and getting out on bail, he made a deal with Canadian authorities in 2013 to provide them with $200 million of fake currency. In exchange, the authorities would not extradite him to the United States and he would get to walk free. Today, Bourassa runs a security company and works with the police to catch other counterfeiters.[286] [287] [288]

[286]Gillespie, Tom. "Money for nothing: The story of the biggest counterfeiter in US history." *Sky News*, 8 March 2020, https://news.sky.com/story/money-for-nothing-the-story-of-the-biggest-counterfeiter-in-us-history-11942377. Accessed 4 May 2023.
[287]"Famous and notorious paper money counterfeiters! - Littleton Coin Blog." *Littleton Coin Company Blog*, 18 June 2018, https://blog.littletoncoin.com/paper-money-counterfeiters/. Accessed 4 May 2023.
[288]Gold, Andrew, and Jordan Harbinger. "488: Frank Bourassa | The World's Greatest Counterfeiter Part One." *PodcastOne*, 30 March 2021, https://www.podcastone.com/episode/488-Frank-Bourassa--The-Worlds-Greatest-Counterfeiter-Part-One. Accessed 4 May 2023.

Questions to Consider

- How does confidence in a currency affect its value?
- How does the usage of counterfeit money impact a country's rate of inflation?
- How is counterfeiting used to promote criminal activity?
- What are some ways in which countries can make the process of counterfeiting more difficult?

Possible Solutions

- Create a protocol establishing new standards for security features for currency notes
- Have member states create foreign cash depots from which member states can recycle their currencies, check for counterfeit currency notes, and distribute legitimate currency notes in foreign countries
- Raise capital to invest in new technologies which can embed modern security features in currency notes
- Develop the Documentchecker Banknote database so that it can have up to date information on reports of counterfeit currency being discovered

Helpful Websites:

- https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency
- https://www.rba.gov.au/publications/rdp/2015/pdf/rdp2015-05.pdf
- https://www.drimark.com/everything-you-need-to-know-bout-bleached-bills/
- https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-terrorist-financing-related-to-counterfeit-currency.pdf
- https://www.interpol.int/en/Crimes/Counterfeit-currency-and-security-documents/Counterfeit-currency-and-documents-conferences

Position Descriptions

Each delegate is assigned one of the positions below. These positions are government officials who oversee the national law enforcement apparatus of their respective countries. You will be responsible for representing your assigned position during the committee sessions and when writing your position paper. The degree to which you meet these expectations will help determine whether or not you will receive an award.

Director of the United States Federal Bureau of Investigation You are Christopher Wray. You have been the Director of the United States Federal Bureau of Investigation since August 7, 2017. You are fighting cybersecurity threats from nation-state actors and ransomware attacks, and see Russia, Iran, North Korea, and especially China as your biggest threats. You have been facing increased challenges in regards to financial fraud from criminal organizations.

Director of the Canadian Security Investigation Service You are David Vigenalaut. You have been the Director of the Canadian Security Investigation Service since June 19, 2017. You have implemented public reporting systems through which Canadian individuals and businesses report instances of cybercrime. You have taken steps to try to limit economic espionage in Canada, specifically the exploitation of Canadian technology, trade secrets, and other forms of economic information. You have named China a major threat to Canadian national security.

Director General of the United Kingdom National Crime Agency You are Graeme Biggar. You have been the Director General of the United Kingdom National Crime Agency since August 12, 2022. You have encouraged sanctions to be imposed on cybercriminals and have

supported the British Government's actions of freezing the bank accounts and issuing travel bans on 7 Russian cybercriminals. You have taken involvement in reforms which look to better law enforcement capabilities in identifying and combating financial criminals including money launderers. Under your watch, the NCA had arrested a Russian businessman linked to money laundering activities.

Director General of National Police of France You are Frédéric Veaux. You have been the Director General of National Police of France since February 3, 2020. You have investigated extortion phishing campaigns by cybercriminals. You have further collaborated with INTERPOL to discuss solutions to curb cybercrime as well as financial frauds. Similarly, you have also collaborated with regional police chiefs in examining issues such as cybercrime as well as financing of terrorism in the 2015 Europol Police Chiefs Convention.

President of the Federal Criminal Police Office of Germany You are Holger Münch. You have been the President of the Federal Criminal Police Office of Germany since December, 2014. You have called for German law to be more stricter on cybercrime, citing the considerable level of damage cybercriminals can inflict. You have also talked about the possibility of law enforcement officers recruiting Russians in German prisons who can provide information about Russian criminal activity in order to combat Russian organized crime in areas such as cybercrime and money laundering.

Minister of Interior of Spain You are Fernando Grande-Marlaska. You have been the Minister of Interior of Spain since June 7, 2018. You have allocated more funding and resources for law enforcement authorities to tackle cybercrime in response to the alarmingly high levels of cybercrime occurring in Spain. You have also launched a public awareness campaign to educate the public on the dangers of

cybercrime and what to do to fend against it. You have collaborated with experts on handling priority issues such as cybercrime and money laundering.

Commissioner of the Australian Federal Police You are Reece P. Kershaw. You have been the Commissioner of the Australian Federal Police since October 2, 2019. You have extensively worked with domestic law enforcement agencies as well as INTERPOL to combat cybercrime. You have also held the AFP-INP Senior Officer's Meeting to discuss cybercrime with the Indonesian National Police in which you signed a cooperation and intelligence sharing agreement with them to better collaborate in tackling cybercrime. You have also taken steps to try to employ effective methods in curbing the supply of counterfeit currency and counterfeit currency distribution networks.

Commissioner General of the National Police Agency of Japan You are Yasuhiro Tsuyuki. You have been the Commissioner General of the National Police Agency of Japan since August 30, 2022. You have worked with other countries such as Vietnam to help counter cybercrime. You have faced new challenges amid recent cyber attacks by North Korean hackers. You have also worked with the United Nations in finding steps against money laundering.

Commissioner General of the National Police Agency of the Republic of Korea You are Yoon Hee-keun. You have been the Commissioner General of the National Police Agency of the Republic of Korea since August 10, 2022. You have worked with the United States Federal Bureau of Investigation to increase cooperation in combating cybercrime. You have called for increasing cooperation in terms of increased personnel exchanges and educational cooperation. You have discussed with INTERPOL measures taken to try to tackle issues such as

intellectual property theft, counterfeit currency, and money laundering in the 15th Intellectual Property Crime Conference, calling for increased international cooperation.

Commissioner of Israeli Police You are Kobi Shabtai. You have been the Commissioner of Israel Police since January 17, 2021. You have called for more aggressive and stringent laws against cybercriminals in discussions with the Federal Bureau of Investigation. Israel Police under your leadership has however been alleged of using spyware to spy on Israeli citizens, though such claims are staunchly denied by you. Forces under your command have taken steps to uncover financial criminal schemes in Israel, with 21 individuals associated in a money laundering scheme arrested.

Director General of the Central Bureau of Investigation of India You are Subodh Kumar Jaiswal. You have been the Director General of the Central Bureau of Investigation of India since May 25, 2021. Under your leadership, the Bureau works with law enforcement authorities in more than 100 countries to detect instances of cybercrime. You have been confident of your Bureau's ability to address and investigate instances of cybercrime. You have been looking for ways to better investigate and prosecute those accused of financial crimes.

National Police Commissioner of South Africa You are Selahle Fannie Masemola. You have been the National Police Commissioner of South Africa since March 31, 2022. You have been looking at intensifying the department's capacity to fight cybercrime. You have cracked down on crime groups, arresting individuals in South Africa accused of engaging in fraud, money laundering, and online racketeering.

Director General of the Investigations Police of Chile You are Sergio Munoz Yanez. You have been the Director General of the

Investigations Police of Chile since June 2022. You have called for more regional collaboration and cohesion in Latin America to help solve organized crime such as cybercrime. You have also been looking to further advance the skills of officers in the Chilean Police to better tackle local crime networks, specifically narcotic criminal activity, and cybercrime.

Commissioner General of the Argentine Federal Police You are Nestor Roncaglia. You have been the Commissioner General of the Argentine Federal Police since November 21, 2018. You encourage police and other law enforcement authorities to adapt and evolve to new technological developments to protect people from the growing threat of cybercrime. You have been facing increased contemporary challenges in regards to the growth of counterfeit currency.

Minister of Justice and Public Security of Brazil You are Flávio Dino. You have been the Minister of Justice and Public Security of Brazil since January 1, 2023. You have been faced with the challenge of creating a better strategy in regards to combating cybercrime, something which Brazil has struggled on. You have helped implement an initiative between law enforcement and the military to protect schools in Brazil from attacks such as cyber attacks. Your terms as Minister have encountered increased occurrences of counterfeit currency occurring across Brazil as a result of the economic downturn in the country during the COVID-19 pandemic.

Minister of Public Security of the People's Republic of China You are Wang Xiaohong. You have been the Minister of Public Security of the People's Republic of China since June 2022. To combat cybercrime, you have called for the Ministry of Public Security to strengthen law enforcement to "resolve overseas security risks". You have outlined many goals to combat counterfeit currency including making more laboratories to test currency, following the previous Ministry of Public

Securities other labs. You are most likely to follow goals set by the Chinese government and often find yourself against an Americans point of view.

Minister of Interior of the Russian Federation You are Vladimir Kolokoltsev. You have been the Minister of Interior of the Russian Federation since May 2012. You have called for interstate cooperation to protect people from cyber attacks which have grown over 50% in the last 2 years and it has kept on growing. You have also recognized counterfeit currency and products as an issue in India, so you signed an agreement of Security Cooperation with India's home minister Rajnath Singh. You are looking for ways to spread the great security of Russia across the world to nearby countries to stop cybercrime and counterfeit currency manufacturing.

Director-General of the Myanmar Police Force You are Zin Min Htet. You have been the Director-General of the Myanmar Police Force since May 2022. To combat transnational cybercrime you met with the Royal Thai Police Force in June to discuss monitoring systems of different servers. Additionally, your force further discussed the rule of law about capturing criminals that participate in cyber attacks on countries outside of their own. Currently, the police force is investigating the spread of counterfeit notes as they are becoming a national issue. Recently your group has raided produce in Karen state's Myawaddy township and found more than 1700 fake kyat bills.

Supreme Leader of Iran You are Ali Khameni. You have been supreme leader of the Islamic Republic since 1989. You have direct control over the Law Enforcement Command of Iran. After his high ranking commanders informed him of an upcoming propaganda war, he called the people for a cyber "jihad". This means that if a leader calls for a jihad, all followers must follow what he has said for them to do. In this case he called for university students to use cyberwarfare to counter

attacks by Iran's enemies. You have faced issues regarding counterfeit US Dollars being printed in neighboring countries and then being spread in your market.

Commander General of the Internal Security Forces of Lebanon You are Joseph Aoun. You have been the commander of the Lebanese armed forces (LAF) since 2017. To address cybersecurity, Lebanon's strategy is to make a national security agency. For counterfeit currency, your armed forces have recently apprehended a group that had over 480$ million counterfeit US dollars. It would have been detrimental to the economy had that not been stopped.

Minister of Internal Affairs of Belarus You are Ivan Kubrakov. You have been the Minister of Internal Affairs of Belarus since October 29th, 2020. You have aimed to utilize the operational capabilities and strong experience of staff members of the Ministry to try to neutralize and combat organized criminal entities including cybercriminal entities. You have also cooperated with China to find solutions related to issues such as cybercrime. You have stressed further international cooperation on the areas of cybercrime as well as money laundering.

Minister of Interior of Syria You are Mohammad Kahled al-Rahmoun. You have been the Minister of Interior of Syria since November 26, 2018. You have established a special subdivision of the Ministry's Cybercrime Combatting Branch to monitor and oversee digital communication devices and create a database to hold information on instances of cybercrime. You have encountered certain challenges in relation to the growth of counterfeit currency in certain Syrian cities such as the city of Raqqa.

Inspector-General of Police of Nigeria You are Usman Alkali Baba. You have been the IGP of Nigeria since April 6, 2021. You have recently approved of the merging of subdivisions that fight against cybercrimes in Nigeria, creating the new Nigeria Police Force National Cyber-crime Centre. You have also recently arrested and prosecuted many Nigerians who were caught in the act of selling naira, the national currency, and have stated that all those who commit the same crimes will be punished.

Minister of Interior of Pakistan You are Rana Sanaullah Khan. You have been The Minister of Interior of Pakistan since May 4, 2019. You have stated that the usage of social media for immoral activities will be prohibited. However, you have also been arrested for defamation of the president while you were intoxicated.

Minister of Interior of Saudi Arabia You are Abdulaziz bin Saud Al Saud. You have been the Minister of Interior since June 21, 2017. You have stated that it is necessary for cybercrime to be addressed during the a meeting of the Arab Interior Ministers Council, however have not taken many actions regarding counterfeit currency.