

Forum: United Nations Office on Drugs and Crime (UNODC)

Issue #1: Measures to address the exploitation of digital platforms by transnational crime organizations.

Student Officers: Marisol Schmitz and Juan Diego Oblitas

Position: Chair of the United Nations Office on Drugs and Crime



Gudakunst, Dani. "Organized Crime Has Gone High Tech." *Police Chief Magazine*, 6 Sept. 2017, <https://www.policechiefmagazine.org/organized-crime-has-gone-high-tech/>. Accessed 13 Apr. 2026.

Introduction

Digital platforms, such as social media or various types of connection platforms, have become the most essential tool for committing transnational crime. Numerous cybercriminals worldwide have been able to exploit the gaps and loopholes in internet data-sharing platforms, abusing the system for their own gain. Messaging apps, often used by criminal networks to conceal identities, expose users to significant risks. To

further explain, the nations that often face these issues are the nations with a weak cybersecurity system due to the insufficient resources economically to build on their system to protect their citizens. Though most nations do have measures to a certain extent to focus on platform monitoring, they may often overlap with other policies, which creates gaps between the systems. In an international aspect of this issue, nations are able to see how multiple of them face this issue due to the exploitation of loopholes to traffic illegal goods. Nations that are heavily affected by this issue have been in Western Europe, which has one of the biggest hubs for trafficking illegal goods through digital platforms. According to a global initiative, they state, "In early 2023, a Europol-backed operation took down two of the world's largest cybercrime forums." ("The Digital Drug Revolution: How Online Markets Are Reshaping Global Illicit Trade"). This overall gives insight into how fraud comes hand in hand with cybergroups that exploit digital platforms to traffic different kinds of goods. The controversy on this topic is due to the different viewpoints of nations when it comes to their balancing of international cooperation, which includes security and privacy. Such as the UNODC, which is the head of this issue, with their viewpoint being to combat this issue and focus mainly on privacy, and raise awareness by improving the structure and actions of the users of the media. They state that the UNODC Cybercrime unit "fights against cybercrime through supporting national structures and action." While in the EU, they are trying to coordinate operations across states to ensure more safety for children's sexual exploitation and general fraud being committed. In the past, they hosted the European Cybercrime Conference back in 2024, which included over 400 participants from over 80 countries, whose main goal was to create a pathway to prevent and lower the rates of cyberattacks. Ultimately, this issue is controversial due to the different goals and actions that have been taken in the past to prevent this issue.

In an international aspect, many nations worldwide have been working together to find stability in these problems. Due to the low regulations on the internet, this creates no limits to an extent so that cybercriminals are not restricted to just focusing on one nation, which makes unilateral national responses not work due to the intensity of the problem. Different international affairs, such as the EU, have been working together in the Budapest Convention on Cybercrime to harmonize laws worldwide. (European Treaty Series No. 185), "Convinced of the need to pursue, as a matter of priority, a

common criminal policy aimed at the protection of society against cybercrime, *Inter alia*, by adopting appropriate legislation and fostering international cooperation." Ultimately, the illegal trafficking and fraud seem to be deeply intertwined in creating challenges in the transnational crime organizations.

Definition of Key Terms

Transnational Organized Crime(TOC): When illicit activities such as trafficking, extortion, and money laundering are performed by criminal organizations across borders using digital platforms(United Nations).

Cyber-enabled crime: When digital tools and platforms allow common crimes to be easier or on a larger scale("Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime").

Cyber-dependent crime: Crimes that are exclusive to the digital world such as hacking, ransomware, and account takeover, which are frequently committed by organized crime groups("Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime").

Dark web marketplaces: Online markets that are hidden (frequently accessed through encrypted browsers) that facilitate criminal organizations to do illicit activities such as drug trafficking, identity theft, counterfeit goods distribution, and other cybercrime (Owen et al.).

Cyberspace: The facilitation of internet use due to computers, networks, and other devices, creating a non-physical realm that is digital (Lasky).

Cybersecurity: The use of many technologies, processes, and policies to combat cyberattacks, protecting targeted people, systems, and data (Lindemulder et al.).

Online scams and fraud: Deceptive schemes performed digitally, such as phishing, tech support swindles, and false investment opportunities, are often ran by transnational organized crime groups ("Online and Digital Scams | OCC").

Encrypted Communication: Methods and channels of securely sharing information, allowing criminal organizations to plan activities with limited law-enforcement monitoring (Faure).

General Overview

The Main Idea

This issue focuses on how illicit activities like fraud, money laundering, and trafficking are performed all around the world by transnational organized crime groups that utilize digital platforms, such as social media, messaging apps, e-commerce websites, and payment platforms. Solving this issue will take precise design of measures, in which states and multinational organizations will have to hold platforms, nations, and criminal networks accountable, and at the same time, maintain privacy, security, and freedom of expression(Union). Delegates will have to find solutions ensuring that cyberspace stops being exploited by criminals, but making sure that regulation and surveillance in the digital world are not extreme.

The challenge of enforcing security against privacy and digital rights

A fundamental disagreement when it comes to this issue is how much a nation is willing to share data and accept monitoring to combat organized crime. Some states can be more focused on security, preferring mandatory backdoors, more surveillance, and expanded data-sharing rules. On the other hand, states that value rights more argue that the measures mentioned previously are a threat to privacy, an amount too high of surveillance, and removing freedom of expression and encryption(Anuradha). That leaves a main concern that must be resolved, if tech companies weaken encryption or hand over user data automatically, in addition to protecting people from over-broad targeting.

The debate of sovereignty when faced upon an international tech-company power

The question of who is in charge in cyberspace and all its rules is a clash to say the least. On one side, states believe that national law must manage and hold authority over digital platforms, with foreign governments and companies being unable to make

changes, while on the other end, states argue that binding international rules, oversight from multiple places, and regimes of platform liability help combat transnational crime("Cybersecurity | United Nations - CEB"). There must be an agreement on how much impact tech companies can have on the rules, to what extent internet-governers should take external orders from, and if there should be a United Nations treaty that holds supreme on digital platforms.

Inequality of Resources and Capacity

Developing nations lack the necessary resources and capacity for advanced measures. These states don't have enough personnel and adequate institutions to study cybersecurity, organize platforms and keep its citizens safe in the digital world. Due to this, the debate stands, if treaties and international laws should be made with the mind of wealthier states and big tech companies, at the expense of developing countries. Yes, rules might be great, but with developing countries not having sufficient financial and technical support, they will be left out and still suffering(World Bank Group). Digital colonialism can also take place, with these rich nations and big tech corporations having all the power of cyberspace, leading to domination, with developing countries having no choice but to oblige(Transnational Institute).

Major Parties Involved and Their Views

United Nations Office on Drugs and Crime (UNODC)

UNODC has been one of the biggest responsible bodies when it comes to building an international framework to create collaboration between nations, while focusing mainly on safety and maintaining privacy. "Some 67.4 percent of the world's population accessed the Internet in 2023" ("Five Reasons Why the New Cybercrime Convention Matters"). This citation gives insight into how global and essential the internet has become, which can lead the vulnerable population towards the issue of cybercrime. UNODC has said, "The finalization of this Convention is a landmark step as the first multilateral anti-crime treaty in over 20 years and the first UN Convention against Cybercrime at a time when threats in cyberspace are growing rapidly" ("United Nations: Member States Finalize a New Cybercrime Convention"), which indicates how they have taken measures to ensure safety and how they are responding to cybercrime.

UNODC's essential goal is to create a structure that is sustainable by giving assistance and law enforcement so that nations collaborate as a whole.

United States

The United States of America has been the most targeted nation in dealing with cybercrimes and attacks. In an international perspective, the FBI has found more than 850,000 reports of cybercrime violations in 2024. "At \$16.6 billion, cybercrime in 2024 out-earned the U.S. box office, the entire U.S. airline industry's net profits, and the U.S. recorded music market—combined. Hackers aren't just stealing data; they're surpassing the financial scale of major, everyday industries," Povolny said (Ionut Arghire). This has cost the United States more than \$16.6 billion, resulting in a major problem due to the high number of attacks and the increased cost required to address them, which has also led to numerous arrests of cybercriminals. "In 2024, more than 215 arrests were made through 11 joint operations between the FBI and India's Central Bureau of Investigation" (Otto). Overall, the United States lacks major tech support and government monitoring of different scams that the United States government has faced.

Russia

As Russia is one of the biggest sources of transnational cybercrime from an international perspective, it has challenged the geopolitical tools to ensure the safeguarding of human rights in international treaties. The University of Oxford has stated that Russia is the biggest index in the cybercrime world, which creates tension between Russia and other nations due to Russia's bad reputation and how other nations now fear Russia as a whole. "Russia for activities ranging from phishing and identity theft to malware distribution, fraud scams, child sexual abuse materials, and command and control servers for botnets and distributed denial of service (DDOS) attacks" (Seeger). This cite from the 'Just Security' article shows how Russia has been one of the risks in the cyberworld due to the high attack rates and the different reasons for how they treat cybersecurity issues.

INTERPOL

INTERPOL has shown to be a key organization when coordinating police from an international perspective. INTERPOL has shown to be significant when targeting the issue of cybercrime networks in Latin America and Africa. "Cybercrime continues to outpace the legal systems designed to stop it," INTERPOL said, adding, "75% of countries surveyed said their legal frameworks and prosecution capacity needed improvement." (News). This site indicates how INTERPOL has proven that many nations are in danger due to their weak system of cybersecurity. In 2024, INTERPOL managed to arrest over 1,000 cyber criminals. The global crime costs were estimated to be around 10 trillion US dollars by the end of 2025, which is an exponential scale in comparison to 2015, when they were 3 trillion US dollars. which highlights the severity of the problem that the INTERPOL organization is taking responsibility for and trying to ultimately combat the issue. "In 2024, a US cybersecurity company revealed that over 30 000 vulnerabilities were disclosed globally that year, a 17 per cent increase from previous figures." ("Resilience to Cyber-Dependent Crimes Is Rising, yet Threats Continue to Outpace It")

India

If India is heavily reliant on technological advancements, it has severe loopholes, which make it one of the heavily targeted nations in Asia for cyberattacks. And he has proven to be ranked third by the 'Security Week' organization due to over 4000 cyberattack complaints, which often targeted the India-based networks. "In 2024, India was the most targeted country in Asia and number seven in the world, with 100 listed victims on extortion websites." (Group) Despite being victims of cyberattacks, India has also repeatedly proven to be vulnerable to scamming foreign victims. India has made a key proposal during the UN cybercrime treaty negotiations, which includes constant global communication and constant monitoring between nations. "The United Nations Convention against Cybercrime was officially adopted in December 2024 by the General Assembly (United Nations Office on Drugs and Crime, n.d.b.)." (Beyer)

Europol

The EU's primary goals are to coordinate losses between the nations in the cybercrime operations with countries such as Germany, Italy, and the Netherlands. They have found serious and organized crime threats in 2025, which include full-scale migration and cybercriminals using the darknet market to coordinate different attacks. "From

trafficking and fraud to extortion and recruitment, the internet is both a tool and a target. Criminals use encrypted messaging, social media, and darknet markets to coordinate operations, launder money, and exploit victims—particularly youth" (Werner). According to the EU's 2024 report, only 2% of illegal proceeds are currently known. Well, this highlights the need for more cybersecurity. The EU is working with other global organizations to combat this issue together. Primarily, the EU is looking for stability and unity.

Timeline of Events, Relevant Resolutions, Treaties, and Events

Date	Description of Event
1980	In 1980, the first computer networks were established, while bulletin board systems (BBS) were created to regulate early access to digital communication. (Hafner and Lyon)
1990	Public internet gets expanded with little to no regulations, the government begins to recognize how internet exploitation is slowly becoming a risk factor to society, while trying to coordinate frameworks to work effectively. (UNODC)
2000	According to unodc.org, the UNODC has recognized how transnational crime has become one of their major problems, which is why the UN decided to host the "United Nations Convention against Transnational Organized Crime," where they state: "The Convention represents a major step forward in the fight against transnational organized crime and signifies the recognition by Member States of the seriousness of the problems posed by it, as well as the need to foster and enhance close international cooperation to tackle those problems" ("United

Nations Convention against Transnational Organized Crime")

- 2001/2 In 2002, Budapest held its 'Budapest Convention on Cybercrime' after many nations had recognized the issue of transnational crime through digital platforms. The Budapest Convention on Cybercrime, adopted by the Council of Europe, was a treaty that brought together laws from different nations to harmonize their regulations and create an international framework. According to the Council of Europe, they state, "The Budapest Convention is more than a legal document; it is a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases." ("About the Convention - Cybercrime - [Www.Coe.Int](http://www.coe.int)")
- 2004 2004 was a crucial year when there was a major shift in Europol (European police office) when they now had 10 more members added to their treaty. This was crucial because it marked a change in how nations were thinking; they shifted into becoming more dominant in the issue and wanting to take accountability. Most of the nations that joined the Europol were obligated to do so because they were part of the European Union (EU) despite also wanting more security; an example of this would be the Nation of Poland, according to the "Poland has become the latest country to join an international initiative to tackle the growing problem of cybercrime, such as payment fraud and malware," stated globalgovernmentfinance.com.
(Hall)
- 2006 The UNODC has witnessed one of the biggest security threats by witnessing the smuggling of immigrants, which leads to insecure social security. They noticed how it has become a very serious issue. "The threat posed by transnational and non-State actors

involved in drugs and crime was one of the greatest challenges to international security and peace," an official from the United Nations Office on Drugs and Crime ("Client Challenge")

2017/18 Europol has taken significant accountability in the years of 2017 and 2018. According to europol.europa.eu, they stated, "For the SOCTA 2017, Europol has undertaken the largest-ever data collection on serious and organized crime in the EU." (Europol) The Europol committee in the EU has investigated the increase in crime rates in recent years, which made them undertake an investigation of the differences between past years.

2020 The COVID-19 pandemic was a crucial time when society was highly technologically dependent. According to PMC, they stated in an article released in 2020 that "The Covid-19 pandemic has led to an inevitable surge in the use of digital technologies due to the social distancing norms and nationwide lockdowns." (De' et al.) This marks a crucial time for cyberattacks due to the high usage; more people started to become too reliant on the internet, which then led society to start to rely on the internet blindly. According to the article, "The pandemic has created a scenario of insecurity that is inviting fraudsters to exploit the crisis by extracting money or information or by creating vulnerabilities." This overall created an internet-reliant society where everybody was blindly trusting the internet without any further questioning, which came as a benefit towards the cyber hackers.

2024 In 2024 Europol hosted the 'Cyber Crime Conference,' where later came the 'Consolidated Annual Activity Report.' Which gave the result of a positive test. In the activity report, which was released by Europol, they state, "The European Serious and Organised Crime Centre (ESOCC) supported 1,187 operations

during the year and produced 4,854 operational reports." (Europol Public Information). As of the conference, Europol's goal was to be "focused on the theme 'Detect, investigate, and disrupt'" (Europol). In this conference, over 82 nations were able to attend to discuss the past rates of the past years in cybercrime. This created enormous significance between nations because as a result of this conference, nations faced a major shift to collaborate together and harmonize their laws while also securing safety for their citizens in the European Union.

2025 In 2025, the UN decided to open itself up to the Convention on Cybercrime and more international relations. The UNODC states that it "opened for signature on 25 October 2025 at a signing ceremony held in Hanoi, Vietnam, and will remain open for signature at United Nations Headquarters in New York until 31 December 2026." ("Convention Main")

United Nations Involvement

The United Nations has held a significant role over the years concerning the issue of the misuse of digital platforms by transnational criminal organizations.

United Nations Convention against Cybercrime 2024

The UN Cybercrime Convention marked a significant step in the right direction toward solving this issue, being the first international treaty focused on addressing crimes committed through digital platforms and technological means. This treaty was adopted on the 24 of December 24, 2024, by the UN General Assembly under resolution 79/234. This happened in past years of talking stages and collabs through the Open-Ended Working Group (OEWG) and Ad Hoc Committee on Cybercrime. This treaty was opened for signature in Hanoi, Viet Nam, on the 25 of October of 2025, and signatures

will be accepted until the end of 2026, highlighting the United Nations' commitment to solving this alarming issue. After 40 states become Parties, this convention will officially be underway, with its implementation being overseen by the Conference of the States Parties ("United Nations Convention against Cybercrime"). Some measures this convention will implement include punishing cyber-dependent offences, such as hacking, malware deployment, and denial-of-service attacks, thereby strengthening cybersecurity. This promotes international cooperation, making nations unite to solve the issue, and better cybersecurity means fewer techniques that transnational organisations have to cause harm in the digital world(Plumb).

United Nations Convention against Transnational Organized Crime (UNTOC, Palermo Convention, 2000)

This convention is the principal global treaty addressing transnational crime, such as trafficking, drug crime, and money laundering, which are becoming easier with the rise of digital platforms. It was adopted by the UN General Assembly on the 15th of November in the year 2000, under resolution 55/25, and was officially implemented in 2003, with ratification and support from more than 190 countries. This convention establishes clear criminalization, in terms of participating in organized crime, money laundering and corruption, setting clear protocols in terms of trafficking, smuggling of migrants, and tracking firearms. As the digital world gets more advanced, the UNODC has worked on trying to make changes and update the treaty for the modern world and the challenges that will arise with technology. This treaty remains an important part of the fight against the issue, focusing on transnational organized crime("UN Convention against Transnational Organized Crime - the Alliance").

United Nations Convention against Corruption (UNCAC), 2003

This convention is the main treaty against corruption worldwide. It was adopted on the 31st of October of 2003 by the UN General Assembly. This convention played a key role in highlighting the joint realization of fighting against corruption and its importance. It includes key measures, such as punishing bribery and money-laundering, in addition to strengthening international cooperation. This connects to transnational organized crime, as corruption, in many cases, allows these illicit actions to take place, showing

how keeping strict rules in terms of corruption is crucial to solving this issue ("Learn about UNCAC").

Evaluation of Previous Attempts to Resolve the Issue

The Budapest Convention on Cybercrime

As of 2001/2002, the Council of Europe has widely acknowledged this issue. In 2001, the Budapest Convention on cybercrime was held, with over 80 participants. Nations across the world, but mainly in Europe, have found the solution in unity. EU-related nations have been required to comply with this convention to harmonize laws and promote safety and unity within their countries. According to the document "International Cooperation to Fight Transnational Cybercrime" (Javier Lopez), they state, "The computer and the internet have created several potentially new misuses or abuses that may be criminal as well." This article was written by a Spanish journalist, who ultimately concludes that nations need to continue collaborating to achieve peace and unity. Ultimately, the Budapest Convention on Cybercrime has led to more unity and international relations to find a solution for this problem altogether.

Operation Bayonet 2017

As of 2017, two of the major dark web markets were successfully shut down by Europol and the Department of Justice of the United States. This dark web market shut down due to the high allegations of selling illegal data while also trafficking narcotic drugs. Alpha Bay, which was the most used dark web market, was shut down first by the authorities, while Hansa was still very active. After the successful shutdown of Alpha Bay, the authorities closely monitored the Hansa market, which led to the arrest of more than a thousand criminals. As a result, the thirdway.org stated that "global developments in cybercrime cases and efforts from the last five years in boosting international cooperation on cybercrime." This overall shows the importance of unity in combating this issue and finding possible solutions.

Possible Solutions

Launch Capacity Building and Support Programs for Developing Nations

A big issue that comes to mind when finding solutions is the fact that many developing nations simply don't have the resources to carry out these plans. They lack the specialization and tools to combat exploitation in the digital world, making them behind. A way this can be addressed is by developing cybersecurity in these nations with international assistance, such as training cybersecurity personnel and improving border control and financial intelligence systems to help these nations be able to stand on their own.

Build rules that balance strictness and encryption

Encryption is very important for users of the digital world, but there must be a balance between strictness and encryption. To combat this issue, states could make it a requirement of digital platforms to take action such as removing illicit content, overseeing valid takedown requests, and working with law enforcement. It is also essential that companies and governments refrain from silencing criticism, thereby encouraging transparency and independent review systems to maintain full honesty.

Sustainable Development Goal (SDG)

SDG 17: Partnership for the Goals

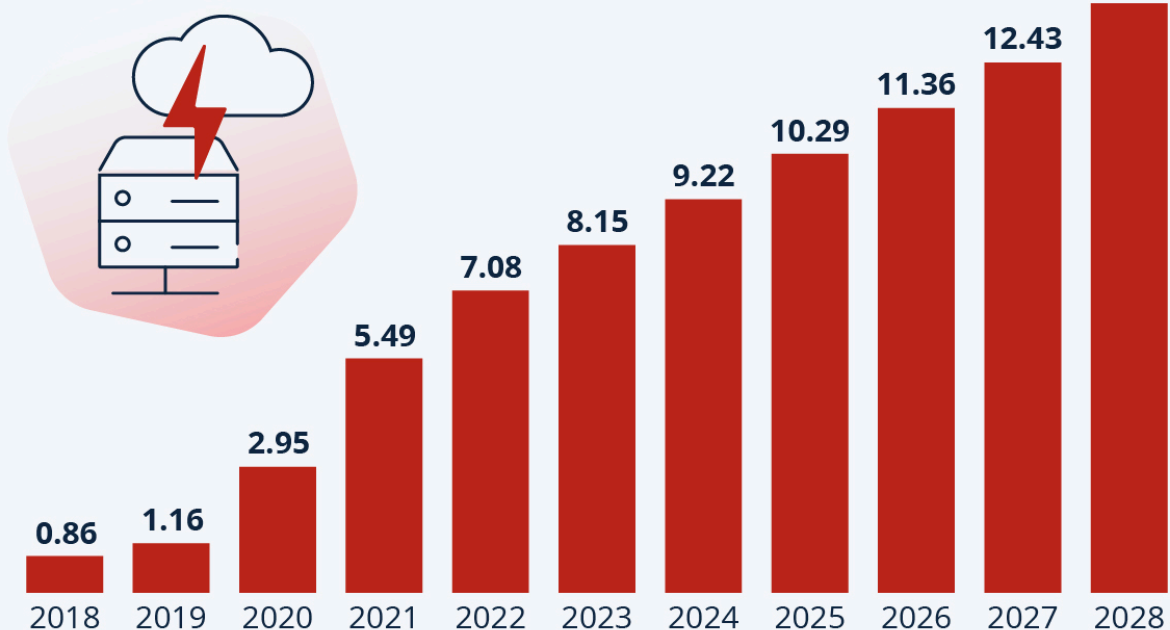
By forming a partnership to achieve a more sustainable and secure security system, citizens will be able to feel more connected to one another while also maintaining secure online connections. If nations decide to collaborate, there will be more security and partnerships between governments, which can then protect users in their ultimate use of it. An example of this would be how if Meta (which has been one of the websites used for transnational crime as a whole) collaborated with governments despite being a company, the government would overall help Meta improve their reputation. In addition, the SDG 17 goal also promotes overall training and technology sharing, which helps nations with their responses to cybercrime.

Appendix

This section of the issue bulletin is focused on providing delegates with great sources to utilize during their research.

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide
(in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights

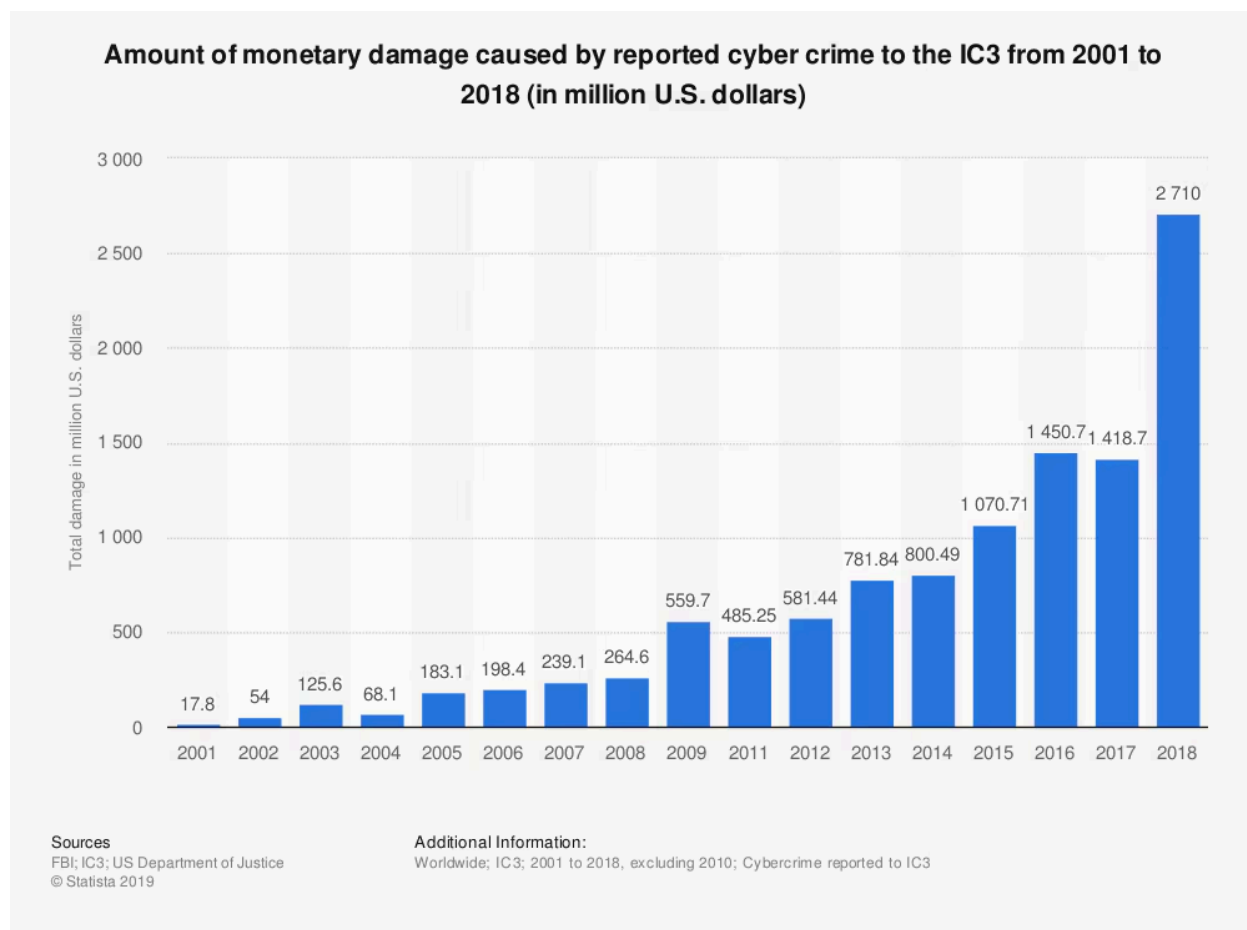


statista

<https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/?srsltid=AfmBOoqhaVg4aGQeO25ZJCwth6TiWAJ7CRTcp6kLozGGxdegBJ5a2Vzy>

Source A: The image above is a bar graph showing the already increasing financial cost of cybercrime, and the alarming increase in financial cost it is projected to have over the next few years until 2028. The cost of cybercrime worldwide is projected to reach 13.82 billion dollars in 2028, showing how cybercrime is growing very fast, making it a very worrying issue affecting economic growth and businesses. This projected

increase highlights the need for more cybersecurity to prevent the negative financial impacts of cybercrime from becoming even more worrisome.



<https://www.weforum.org/stories/2019/10/cyber-crime-and-security-business/>

Source B: The image above is a bar graph that shows the alarming increase of damage done to the IC3 due to cybercrime, up until 2018. The fact that this is until 2018 is very worrying, as technology has developed even more since then, meaning that cybercrime has had to have reached new heights. This shows how cybercrime has not only done harm to individuals emotionally, but has also had a massive negative impact on finances. Going from 17.8 million in 2001 to 2710 million dollars in 2018 shows

cybercrime's rise and its horrific impact, making it a major issue in the digital world.

<https://www.unodc.org/toc/en/crimes/organized-crime.html>

Source C: The source above talks all about transnational organized crime, including but not limited to the different types of it and it's global threats.

<https://www.ibm.com/think/topics/end-to-end-encryption>

Source D: The source above talks all about end-to-end encryption, and it's process to secure data.

<https://www.ibm.com/think/topics/cybersecurity>

Source E: The source above talks all about cybersecurity, including topics such as its importance.

Bibliography

"An Introduction to the Dark Web and Cybercrime." Nisos, 24 Oct. 2023, nisos.com/understanding-dark-web-cybercrime/.

Anuradha, Ms. "Issue 3 Wwww.jetir.org (ISSN-2349-5162)." *JETIRGT06029 Journal of Emerging Technologies and Innovative Research*, vol. 12, no. 3, 2025, www.jetir.org/papers/JETIRGT06029.pdf.

Beyer, Jessica. "Cybersecurity Profile 2025: India - the Henry M. Jackson School of International Studies." *The Henry M. Jackson School of International Studies*, 25 Apr. 2025, jsis.washington.edu/news/cybersecurity-profile-2025-india/.

Cerezo, Ana I., et al. "International Cooperation to Fight Transnational Cybercrime." *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*, Aug. 2007, <https://doi.org/10.1109/wdfia.2007.4299369>.

Council of Europe. "Budapest Convention and Related Standards." *Council of Europe*,

2025, www.coe.int/en/web/cybercrime/the-budapest-convention.

"CRIMINAL INVOLVEMENT by TRANSNATIONAL, NON-STATE ACTORS POSES MAJOR THREAT to INTERNATIONAL SECURITY, THIRD COMMITTEE TOLD | Meetings Coverage and Press Releases." *Un.org*, 4 Oct. 2006, press.un.org/en/2006/gashc3848.doc.htm.

"Cybercrime Module 12 Key Issues: Online Child Sexual Exploitation and Abuse." : , 2016, www.unodc.org/cld/zh/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html.

"Cybersecurity." *Www.itu.int*, www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

"Cybersecurity | United Nations - CEB." *Unsceb.org*, unsceb.org/topics/cybersecurity.

"Cyberspace | Research Starters | EBSCO Research." *EBSCO*, 2022, www.ebsco.com/research-starters/science/cyberspace.

"Dark Web." *Group-IB*, 28 July 2025, www.group-ib.com/resources/knowledge-hub/dark-web/. Accessed 6 May 2026.

De, Rahul, et al. "Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice." *International Journal of Information Management*, vol. 55, no. 102171, 2020, p. 102171. *NCBI*, www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/, <https://doi.org/10.1016/j.ijinfomgt.2020.102171>.

"Encrypted Communications." *DIGITPOL*, digitpol.com/encrypted-communications/. *European Treaty Series -No. 185*. 2001.

"European Union Serious and Organised Crime Threat Assessment 2017." *Europol*,

www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

“Europol.” *Europol*, 2024, www.europol.europa.eu/publications-events/events/cybercrime-conference-2024. Accessed 5 May 2026.

Europol. “Global Cybercrime Crackdown: Over 373 000 Dark Web Sites Shut Down.” *Europol*, 20 Mar. 2026, www.europol.europa.eu/media-press/newsroom/news/global-cybercrime-crackdown-over-373-000-dark-web-sites-shut-down.

Europol Public Information. 2025.

Faure, Quentin. “The Role of Encrypted Messaging in Transnational Organized Crime.” *Policechiefmagazine.org*, 2025, www.policechiefmagazine.org/digital-shadows-encryption/.

FBI. “AlphaBay Takedown.” *Federal Bureau of Investigation*, 20 July 2017, www.fbi.gov/news/stories/alphabay-takedown.

fromiti. “Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime.” *Www.unodc.org*, www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

Gercama, Ingrid. “Data Dealers and Bomb Plots: Inside the Netherlands’s Shadowy Market for Stolen Data.” *OCCRP*, 2025, www.occrp.org/en/feature/data-dealers-and-bomb-plots-inside-the-netherlands-s-shadow-market-for-stolen-data. Accessed 5 May 2026.

Group, Insikt. “Dark Covenant 3.0: Controlled Impunity and Russia’s Cybercriminals.”

- Recordedfuture.com, 2024,
www.recordedfuture.com/research/dark-covenant-3-controlled-impunity-and-russias-cybercriminals.
- Hafner, Katie, and Matthew Lyon. *WHERE WIZARDS STAY up LATE (the ORIGINS of the INTERNET)*.
- Hall, Ian. "Poland Joins Europol's Cyber-Crime Taskforce -." *Globalgovernmentfinance.com*, 25 Apr. 2019, www.globalgovernmentfinance.com/poland-joins-europols-cyber-crime-taskforce/. Accessed 5 May 2026.
- "International Cooperation against Cybercrime." *Cybercrime*, www.coe.int/en/web/cybercrime/international-cooperation.
- Internet Organised Crime Threat Assessment (IOCTA)* 2023. www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf, https://doi.org/10.2813/587536.
- Laks, Alycia. "COVID-19 and Organized Crime: The Politics of Illicit Markets, States, and the Pandemic - Georgetown Journal of International Affairs." *Georgetown Journal of International Affairs*, 19 May 2021, gjia.georgetown.edu/global-governance/covid-19-and-organized-crime-the-politics-of-illicit-markets-states-and-the-pandemic/. Accessed 5 May 2026.
- "Learn about UNCAC." *United Nations : Office on Drugs and Crime*, www.unodc.org/corruption/en/uncac/learn-about-uncac.html.
- Lindemulder, Gregg, et al. "Cybersecurity." *IBM*, 12 Aug. 2024, www.ibm.com/think/topics/cybersecurity.
- Marchini, Camila Silvi. "Resilience to Cyber-Dependent Crimes Is Rising, yet Threats

Continue to Outpace It." *Global Initiative*, 2025, globalinitiative.net/analysis/the-cybercrime-arms-race/.

National Security Council. "Transnational Organized Crime: A Growing Threat to National and International Security." *The White House*, 2025, obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat.

Nations, United. "Basic Facts about the Global Cybercrime Treaty | United Nations." *United Nations*, 2024, www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty.

News, The Hacker. "Europol Dismantles \$540 Million Cryptocurrency Fraud Network, Arrests Five Suspects." *The Hacker News*, 30 June 2025, thehackernews.com/2025/06/europol-dismantles-540-million.html.

"Online and Digital Scams | OCC." *OCC.gov*, 2025, www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/online-and-digital-scams.html.

Oolman, Mike, et al. "Identifying Drug Couriers in Airports." *Journal of Airport Management*, 2019, hstalks.com/article/2377/identifying-drug-couriers-in-airports/. Accessed 5 May 2026.

Otto, Greg. "10 Key Numbers from the 2024 FBI IC3 Report." *CyberScoop*, 23 Apr. 2025, cyberscoop.com/fbi-ic3-cybercrime-report-2024-key-statistics-trends/.

Owen, Anthony, et al. *Dark Web Marketplaces and the Role of Cryptocurrency in Criminal Financial Transactions*. 1 Aug. 2025,

www.researchgate.net/publication/394471483_Dark_Web_Marketplaces_and_the_Role_of_Cryptocurrency_in_Criminal_Financial_Transactions.

Peters, Allison, and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime – Third Way." *Thirdway.org*, 2018, www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.

Seger, Alexander. "Russian Motivations behind the "Hanoi Convention" against Cybercrime." *Just Security*, 7 Oct. 2025, www.justsecurity.org/122000/russian-motivations-hanoi-convention-cybercrime/.

"Tax Agency: A Passenger Was Arrested at Barcelona Airport with Almost 11 Kilos of Heroin Hidden in Bags..." *Agenciatributaria.gob.es*, 27 Nov. 2025, sede.agenciatributaria.gob.es/Sede/en_gb/informacion-institucional/sobre-agencia-tributaria/2025/noviembre/27/detenido-aeropuerto-barcelona-pasajero-11-cafe.html. Accessed 5 May 2026.

"The Future of Learning: AI Tutors or Human Instructors? Or Hybrid? | Media Education Lab." *Mediaeducationlab.com*, 26 Oct. 2024, mediaeducationlab.com/blog/future-learning-ai-tutors-or-human-instructors-or-hybrid.

"UN Cyber Norms | Digital Watch Observatory." *Digital Watch Observatory*, 27 Aug. 2025, dig.watch/cyber-norms.

Union, European. *The Changing DNA of Serious and Organised Crime SERIOUS and ORGANISED CRIME THREAT ASSESSMENT*. 2025.

United Nations. "United Nations." *Un.org*, United Nations, 2025, www.un.org/en/.

---. "United Nations Convention against Cybercrime." *United Nations : Office on Drugs*

- and *Crime*, 2021,
www.unodc.org/unodc/en/cybercrime/convention/home.html.
- . "What Is Transnational Organized Crime?" *United Nations*, 2024,
www.un.org/en/peace-and-security/transnational-crime.
- . "With Criminal Groups Using Sophisticated Technologies to Ply Their Wares, Third Committee Stresses Urgent Need to Collectively Combat Transnational Crime | UN Press." *Press.un.org*, 2 Oct. 2023, press.un.org/en/2023/gashc4374.doc.htm.
- United Nations Office on Drugs and Crime. "Convention on Psychotropic Substances." *Unodc.org*, 2019, www.unodc.org/unodc/en/treaties/psychotropics.html.
- . "Treaties." *United Nations : Office on Drugs and Crime*,
www.unodc.org/unodc/en/treaties/index.html.
- . "United Nations Convention against Transnational Organized Crime." *Unodc.org*,
 United Nations, www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
- University Of Oxford. "World-First "Cybercrime Index" Ranks Countries by Cybercrime Threat Level | University of Oxford." *Www.ox.ac.uk*, 10 Apr. 2024,
www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level.
- "UNODC Cybercrime." *United Nations : Office on Drugs and Crime*, 2021,
www.unodc.org/unodc/en/cybercrime/index_new.html.
- Werner, Jeremy. "Europol Warns of Transforming Threats in 2025 Crime Report: AI, Online Platforms, and Global Instability Fueling Surge in Organized Crime." *BABL AI*, 4 Apr. 2025,
babl.ai/europol-warns-of-transforming-threats-in-2025-crime-report-ai-online-platforms-and-global-instability-fueling-surge-in-organized-crime/. Accessed 5 May

2026.

World Bank Group. "Enhancing Cyber Resilience in Developing Countries." *World Bank*,
World Bank Group, 30 Jan. 2025,
www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries.