INTERPOL

AGENDA ITEM:

Preventing Criminal Activities on the Dark Web

Under Secretary General:
Efe Deniz Yağcı

Academic Assistant:
Mustafa Aslan

NERİMAN EROL YILMAZ SOCIAL SCIENCES HIGHSCHOOL
MODEL UNITED NATIONS CONFERENCE 2025

1.Letter from the Secretary-General

Most Esteemed Participants of Neriman Erol Yılmaz Social Sciences High School Model United Nations Conference, on behalf of myself and of other members of the Executive Team,

My name is Yasemin Raithel, I am a senior graduating from Private Açı Science College. It is my great honor and pleasure to be serving as the Secretary-General of this fabulous conference. Model United Nations conferences are not just a place where diplomatic views are discussed; they are events that provide you with the ability to fully express yourself in critical situations, giving speeches in a confident way in multi-person committees, bringing solutions to problems from the perspective of countries, and many other skills like these. That's why these conferences are like an open door for you to improve yourself. Step out of your comfort zone and don't miss this opportunity. I have no doubt that your experience will be the best you have had in a long time.

Both our academic and organisation teams have dedicated limitless hours and put so much work to deliver to the whole Antalya Model United Nations Society one of the most incredible MUN experience you have seen to this day. Last but not least, let this be a new beginning, as befits the motto of the conference: The Dawn of the Moon. Lastly, I would like to leave a quote with hopes of a marvellous conference;

“Men become builders by building and lyreplayers by playing the lyre; so too we become just by doing just acts, temperate by doing temperate acts, brave by doing brave acts.”

-Aristotle

Sincerely,

Yasemin RAITHEL

Secretary-General of NEYMUN’25

2. Letter from the Under-Secretary-General

First of all, let me extend a hearty welcome to everyone on the INTERPOL committee for NEYMUN'25. Serving as your Under Secretary General in this committee gives me great pleasure. Our primary objective during the conference will be to guarantee the committee's operational state, whether that means delivering this comprehensive study guide to you, responding to all of your inquiries, or giving you more information if necessary. We are here to help, so you can relax. First and foremost, I would like to express my gratitude to the NEYMUN'25 Secretariat for providing me with the opportunity to serve at the conference as an Under Secretary General. Without a doubt, the committee will proceed as smoothly as we anticipated, and this study guide will give you all the information your delegates need to conduct the most productive debates. Do not hesitate to get in touch with me or Mustafa if you have any questions about the process, the schedule, or the conference. Pleasant regards,

Under Secretary General, Efe Deniz YAĞCI

dnzefe0707@gmail.com

3. Letter From the Academic Assistant

Dear Participants,

First of all, I would like to welcome you all to the NEYMUN’25 INTERPOL committee.
I am Mustafa Aslan, a 12th grade student at Bahçeşehir Aspendos Campus, and I am honored to serve as the Academic Assistant of the committee.

I have been attending Model United Nations conferences in Antalya and many other cities for the last two years and this is my 21st conference.
I would like to thank Yasemin Raithel, Kayra Duran and İdil Tekin for giving me an opportunity to be here as a member of the academic team.
Besides these, if you have any questions about the committee, please contact me from my contact information below, even for the tiniest thing you want to ask.
We have added all the necessary information in the committee to the study guide with Efe.
I wish you all success in advance.

Academic Assistant, Mustafa ASLAN

+05324246907 whatsapp
aslanmustafa0770@gmail.com

4. Introduction to committee

Interpol, intergovernmental organization that facilitates cooperation between the criminal police forces of more than 180 countries. Interpol aims to promote the widest-possible mutual assistance between criminal police forces and to establish and develop institutions likely to contribute to the prevention and suppression of international crime. Headquartered in Lyon, France, it is the only police organization that spans the entire globe.

Interpol is the world's largest international police organization, with 194 member countries.
Established in 1923, it enables cross-border police cooperation and supports and assists all organisations, authorities and services whose mission is to prevent or combat international crime.

Interpol has an objective to facilitate international police cooperation even where diplomatic relations are not present between certain countries.
Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. Interpol's constitution prohibits 'any intervention or activities of a political, military, religious or racial character.

i. Organizations and Functions

Interpol concentrates on three broad categories of international criminal activity: terrorism and crimes against people and property, including crimes against children, trafficking in human beings, illegal immigration, automobile theft, and art theft; economic, financial, and computer crimes, including banking fraud, money laundering, corruption, and counterfeiting; and illegal drugs and criminal organizations, including organized crime. Interpol's day-to-day operation is managed by a General Secretariat under the direction of a secretary general, who is appointed for a five-year term by the General Assembly. The General Assembly, consisting of one delegate from each member country, is Interpol's supreme decision-making body. An Executive Committee of 13 members, each representing a different region of the world, is appointed by the General Assembly at its annual meeting. The Executive Committee oversees the implementation of decisions made by the General Assembly and supervises the work of the secretary general.
Each member country has a domestic clearinghouse—called the National Central Bureau, or NCB—through which its individual police forces may communicate with the General Secretariat or with the police forces of other member countries. Interpol relies on an extensive telecommunications system and a unique database of international police intelligence. Each year, Interpol's telecommunications staff handles millions of messages in the organization's four official languages: Arabic, English, French, and Spanish. An automatic search facility, introduced in 1992, allows specially equipped NCBs to search a large database of information; search results are automatically sent in the language of the query. A system known as I-24/7, introduced in 2003, provides NCBs with quick access to a wide variety of data, including fingerprints, DNA records, watch lists of criminal suspects and persons wanted for questioning, and lists of stolen identification documents.

In contrast to the image occasionally conveyed on television and in the movies, Interpol agents do not make arrests, a practice that would unacceptably infringe on the national sovereignty of member countries. Instead, the organization, at the request of NCBs, sends out "red notices," based on warrants issued by member countries, calling for the arrest and extradition of specific individuals. Interpol also issues other "coloured" notices: yellow to help locate missing persons, blue to collect information on illegal activities or on an individual's identity, black to request information needed to identify a body, green to warn agencies about criminals from one country who may commit additional offenses in other countries, and orange to warn law-enforcement agencies of dangers from bombs and other weapons.

ii. History

Interpol traces its history to 1914, when a congress of international criminal police, attended by delegates from 14 countries, was held in Monaco. In 1923, following a significant increase in international crime that particularly affected Austria, representatives of the criminal police forces of 20 countries met in Vienna and formed the International Criminal Police Commission (ICPC) that year. The ICPC's headquarters were established in Vienna, and the head of the Vienna police, Johann Schober, became the organization's first president. The ICPC flourished until 1938, when Nazi Germany annexed Austria; the ICPC's records were subsequently relocated to Berlin. The outbreak of World War II effectively ended the ICPC's activities.

After the war the ICPC accepted an offer from the French government of a headquarters in Paris together with a staff for the General Secretariat consisting of French police officials. The ICPC was thus revived, though the loss or destruction of all its prewar records required that it be completely reorganized. In 1949 the ICPC was granted consultative status by the United Nations. From 1946 to 1955 its membership grew from 19 countries to 55. In 1956 the ICPC ratified a new constitution, under which it was renamed the International Criminal Police Organization (Interpol). The organization moved to its present headquarters in Lyon in 1989.

Interpol was at first mainly a European organization, drawing only limited support from the United States and other non-European countries (the United States did not join the ICPC until 1938). Under the leadership of French Secretary General Jean Népote (1963–78), Interpol became increasingly effective. By the mid-1980s the number of member countries had risen to more than 125, representing all of the world's inhabited continents; by the early 21st century membership had surpassed 180.

In the 1970s the organization's ability to combat terrorism was impeded by Article 3 of its constitution—which forbids "intervention or activities of a political, military, religious or racial character"—and by a 1951 resolution of the General Assembly that defined a "political" crime as that whose circumstances and underlying motives are political, even if the act itself is illegal under criminal law. One source of these obstacles was removed in 1984, when the General Assembly revised the interpretation of Article 3 to permit Interpol to undertake antiterrorist activities in certain well-defined circumstances.
Interpol was reorganized in 2001 following the September 11 attacks on the United States. The new post of executive director for police services was

created to oversee several directorates, including those for regional and national police services, specialized crimes, and operational police support.

5. Introduction to the Agenda Item

The dark web hosts many of the more critical marketplaces for several criminal organisations and individual illegal activities in Europe and around the world. Due to its structural specificities – the possibility to buy and sell anonymously and the fact that it is a digital space that knows no national borders – it is a fertile environment for criminals.
In these specific marketplaces, where bitcoins were the dominant payment method, different types of illegal goods and criminal services were sold, even though more than two thirds of transactions were for illicit drugs and chemical substances.

Despite the progress made in combating cybercrime, legal and technical challenges remain significant. National and international laws must be adapted to address the challenges generated by the dark web and law enforcement agencies must be equipped with the necessary technical skills to investigate criminal activities online.
Online criminal activities are constantly evolving and authorities must continuously adapt to counter them. In response, Interpol has developed several tools to support its agents in their fight against cybercrime. One example of an online training program available to investigators worldwide, is the Cybercrime Investigation Curriculum (CIC). The program includes modules on various types of online crimes, digital investigation methods and evidence collection techniques.

Interpol has also developed a cyber threat database (ICB), which enables authorities to share information on online threats internationally. The database contains information on IP addresses, domain names, email addresses and usernames linked to online criminal activities.

i.What is “Dark Web”

The dark web is the World Wide Web content that exists on darknets (overlay networks) that use the Internet but require specific software, configurations, or authorization to access.Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small

part of the deep web, the part of the web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

The dark web is known to have begun in 2000 with the release of Freenet, the thesis project of University of Edinburgh student Ian Clarke, who set out to create a "Distributed Decentralised Information Storage and Retrieval System." Clarke aimed to create a new way to anonymously communicate and share files online. That groundwork was the basis for the Tor Project, which was released in 2002 and launched a browser in 2008. With the creation of Tor, users could now browse the internet completely anonymously and explore sites that were deemed part of the "dark web."

Originally used by the United States Department of Defense to communicate anonymously, the dark web has now become a hub for users wishing to remain anonymous around the world. People use the dark web for both legal and illegal purposes. It uses a technology called "onion routing," which protects users from surveillance and tracking through a random path of encrypted servers. When users access a site through Tor, their information is routed through thousands of relay points that cover the user's tracks and make their browsing virtually impossible to trace. While using the dark web may seem suspect on the surface, it is perfectly legal, and there are many legitimate uses of Tor and anonymous browsing. For example, in countries where government surveillance may be used to spy on and oppress political dissidents, the dark web is often a place for communication that avoids government censorship and scrutiny. Despite these added layers of security, users should still be cautious using the dark web and take proper security measures, such as periodically updating their security software, browsing with a robust VPN, and avoiding the use of a standard email address.

Given its anonymous nature, the dark web is also used for illicit and even illegal purposes. These include the buying and selling of illegal drugs, weapons, passwords, and stolen identities, as well as the trading of illegal pornography and other potentially harmful materials. Several sites hosting illegal material have been discovered by government agencies and shut down in recent years, including Silk Road, AlphaBay, and Hansa. The dark web's anonymity has also led to cybersecurity threats and various data breaches over the last few decades.

Key Dark Web Statistics

The dark web remains a hidden world where millions connect every day. It's part of the deep web, which includes all pages that search engines can't index.

The dark web makes up less than 1% of the entire network. Even then, this space is vast and constantly evolving.
Take a look at these dark web facts to get a quick overview:
Dark web size: The deep web comprises about 90% of the internet, while the dark web accounts for approximately 0.01%.
Market size and growth: Recent reports project that the market will expand to nearly $2.92 billion by 2032, growing at a compound annual growth rate of 21.8%. (Market.us) Daily dark web users: The number of daily users visiting the dark web rose from 2 to 3+ million between the beginning and end of March 2025. (Tor) Dark web users by country: The United States has the highest number of Tor users, followed by Germany, India and Finland. (Tor)

- United States: 17.6%
- Germany: 13.47%
- India: 4.74%
- Finland: 3.43%
- Netherlands: 3.33%
- Spain: 3.19%
- United Kingdom: 2.95%
- Indonesia: 2.88%
- France: 2.73%
- Republic of Korea: 2.61%

Italy alone sees over 76,000 Tor users each day — that's about one-fifth of all daily Tor users in Europe. (Information Geographies)
In 2023, over half of Italy's online population got a warning that their data had been breached. Of those alerts, 77.5% were about data found on the dark web. (Statista)
Illegal content share: As of 2020, nearly 57% of the content on the dark web was illegal. (Research Gate)
The United States has the maximum number of mean daily Tor users: 387,456 (17.6%). Germany comes next with 296,712 (13.47%) users. (Tor)

Language preferences: Around 83.27% of dark web sites are in English.

1–3% 4–6% 7–9% 10%+

Country	Users	Country	Users
United States	17.60%	Spain	3.19%
Germany	13.47%	United Kingdom	2.95%
India	4.74%	Indonesia	2.88%
Finland	3.43%	France	2.73%
Netherlands	3.33%	Republic of Korea	2.61%

Source: Tor

Dark Web Sites and Marketplaces

The dark web hosts a range of sites that provide different services for cybercriminals and other users. These dark web websites include marketplaces, discussion forums and sites offering illegal services. They operate under high anonymity, making it challenging for law enforcement to track the operators.

Here are some key facts about dark web sites and marketplaces that fuel an underground economy:

- Familiarity level: As of October 2022, nearly 50% of adults in the United States reported being somewhat familiar with the dark web; 21% stated they were very familiar. (Statista)

- Cryptocurrency transactions on the dark web nearly doubled from 2020 levels, reaching an estimated value of nearly $25 billion in 2022. (Market.us)

- Cybercriminals can buy details for a credit card with a $5,000 balance for only $110. (Statista)

- Employee login credentials, including company names, addresses, emails and passwords, are among the leading items that get traded on the dark web.

- Identity theft is the most common crime on the dark web, accounting for over 65% of all monitored illicit activities. (Market.us)

- Credit card fraud represents about 15% of dark web activities, with the volume of card dumps rising by 6% from 2021, surpassing 192 million listings with an average credit limit of roughly $8,700. (Market.us)

- Dark web drug sales increased by around 15% in 2022, with an estimated $1.7 billion generated from illicit drug transactions. (Market.us)

- Marketplace evolution: High-profile dark web marketplaces like Silk Road, AlphaBay and Hydra Market have been shut down, while newer sites like InTheBox, Genesis Market and 2Easy continue to operate.

- 92% of cybercriminal marketplaces offer dispute resolution services. (HP)

- 77% require vendors to hold a license, which can cost around $3,000. (HP)

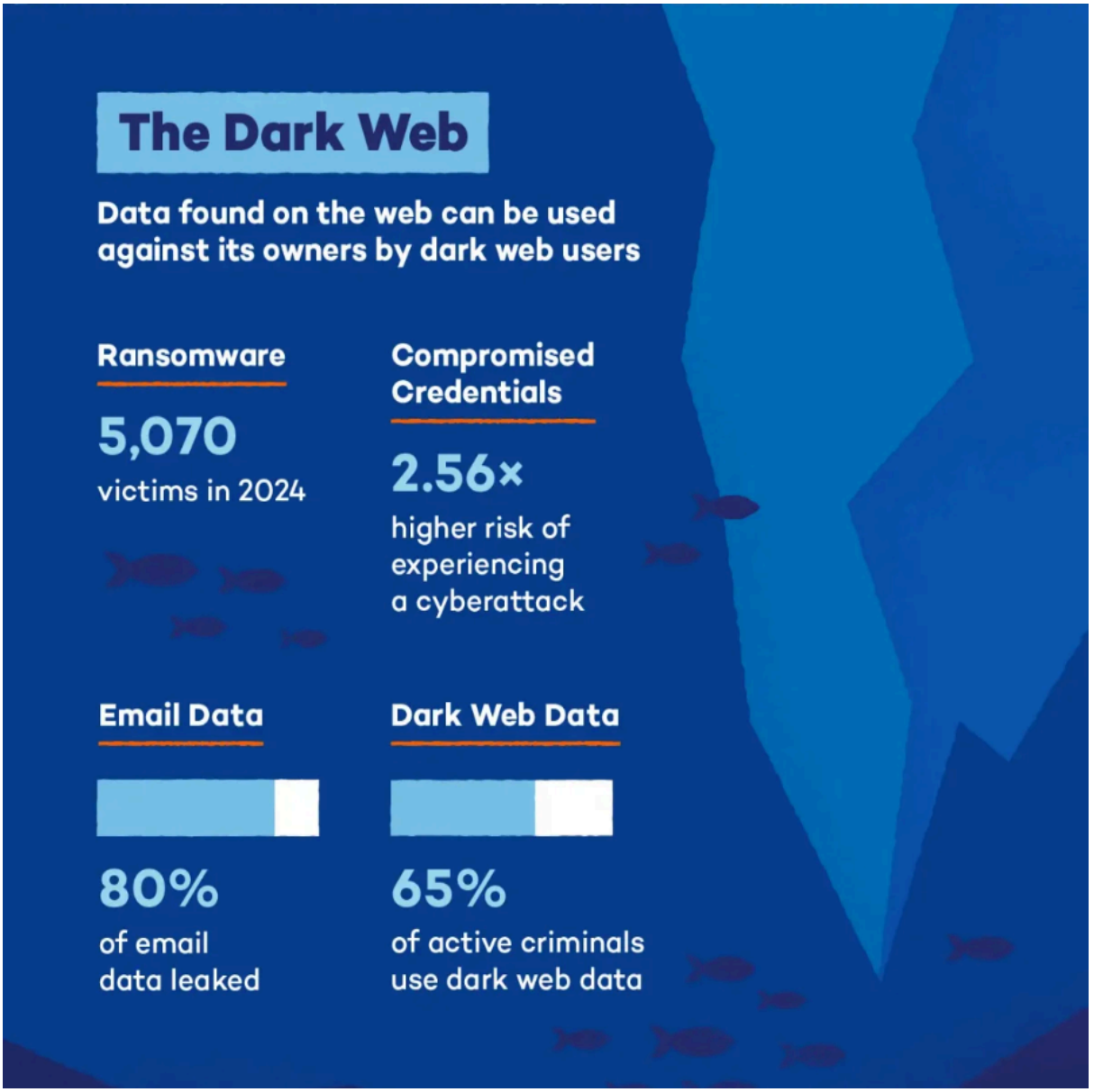
Dark Web Cybersecurity Attacks

The dark web is not only a marketplace for illicit goods — it also serves as a launching pad for sophisticated cyberattacks. Cybercriminals use the dark web to plan and coordinate attacks ranging from different types of phishing and

credential stuffing to ransomware and distributed denial-of-service (DDoS) attacks.

With the wealth of stolen data circulating in hidden forums and marketplaces, there's a heightened risk of data breaches and operational disruptions. Even casual mentions of a company in dark web circles can serve as a prelude to an attack.
Here are some key statistics that highlight dark web-related cybersecurity risks:

- Dependence on dark web data: 65% of active criminals use dark web data for cyberattacks. (Market.us)
- Email vulnerability: Approximately 80% of email data has been leaked to the dark web. (Market.us)
- Ransomware surge: In 2023, ransomware groups saw unprecedented success, with a 55.5% surge in victims, totaling 5,070, a quick rise from the previous year. (Cyberint)
- Compromised credentials risk: Organizations with compromised credentials found on the dark web face a 2.56x higher risk of experiencing a cyberattack. (ID Agent)
- Market listings impact: Dark web market listings increase an organization's likelihood of a cyber incident by 2.41x. (ID Agent)
- Special exposure hazards: Exposure from Telegram chats and forum posts can raise cyberattack risk by up to 1.75x. (Searchlight Cyber and Marsh McLennan)



Dark Web Crime Statistics

Cybercriminals exploit the dark web's hidden nature to conduct a wide range of illicit activities — from hacking and doxing to fraud and ransomware

Here are some dark web statistics that underscore the magnitude of different types of cybercrimes and the growing threat they pose:

- Staggering escalation in cybercrime: In 2023, there were 880,418 internet crime complaints in the U.S., resulting in $12.5 billion in losses — a 22% rise compared to 2022. (FBI)

- Massive daily traffic: As of March 2025, over 3 million visitors access dark web platforms daily, with illegal websites constituting about 60% of all domains. (Tor, Market.us)
- Illicit revenue generation: The dark web economy is estimated to generate around $1.5 billion in annual revenue from the sale of stolen data, counterfeit goods and other illegal products. (Market.us)
- Credential surge: Stolen account credentials available on the dark web surged by 82% in 2022, reaching an estimated 15 billion credentials — a major enabler of subsequent cyberattacks. (Market.us)
- In 2023, 298,878 entities reported falling victim to phishing scams — only slightly lower than the 300,497 reported in 2022. (FBI)
- In contrast, incidents of personal data breaches (55,851), non-delivery or non-payment (50,523), extortion (48,223) and tech support scams (37,560) were significantly lower.

6. Goals and strategy of Interpol

i.Strategies of Interpol

In 2015, Interpol launched a training program on the dark web to raise awareness among its agents about underground criminal activities and to equip them with technical and legal skills to combat cybercrime, marking an important step in the fight against it. The program covered various topics, including the use of VPNs, encrypted messaging services and anonymous browsing software to conceal the identities of criminals, as well as identifying online black markets where illegal products and services are sold.
Legal issues related to combating cybercrime were also addressed, considering the challenges in obtaining and using evidence from the dark web in legal proceedings due to differing laws between countries. As such, the training focused on investigating online criminal activities while complying with national and international laws. Interpol Secretary General Jürgen Stock emphasized the importance of combating cybercrime and stated that the training program has better prepared law enforcement to investigate criminal activities on the dark web.
While the dark web training program was a significant step in strengthening law enforcement's capacity to investigate cybercrime, it remains a challenging issue that needs international coordination, legal adaptation and continuous training of law enforcement agencies.
Despite the progress made in combating cybercrime, legal and technical challenges remain significant. Online criminal activities are constantly evolving and authorities must continuously adapt to counter them. In response,

Interpol has developed several tools to support its agents in their fight against cybercrime. One example of an online training program available to investigators worldwide, is the Cybercrime Investigation Curriculum (CIC). The program includes modules on various types of online crimes, digital investigation methods and evidence collection techniques.
Interpol has also developed a cyber threat database (ICB), which enables authorities to share information on online threats internationally. The database contains information on IP addresses, domain names, email addresses and usernames linked to online criminal activities. Authorities can use this information to investigate criminal activities and identify perpetrators.
In addition to these tools, Interpol works closely with other organizations, such as Europol, to strengthen international cooperation in the fight against cybercrime. For instance, the two organizations collaborate on the Joint Cybercrime Action Taskforce (J-CAT), which aims to enhance the operational response to cybercrime and increase cooperation between law enforcement agencies.
The ongoing challenge of combating cybercrime and the need for continued collaboration and innovation. Overall, the fight against cybercrime requires a concerted effort from international law enforcement agencies, governments and the private sector. Through the development of training programs, databases and collaborative initiatives, Interpol is playing a crucial role in this fight.

In an effort to fight online crimes perpetrated on the dark web, international police agency Interpol has created its own cryptocurrency, as well as a simulated version of a market place similar to the notorious Silk Road. The training initiative is thought to be the first of its kind and could be a precursor to a significant international crackdown on dark web activities.
During a recent five-day training course, participants role-played as vendors, buyers and administrators of black market websites on the dark web. Live law enforcement "take downs" of the simulated sites were also carried out to help improve the understanding of the technical infrastructure of the Tor network.
Darknets are fast emerging as the preferred trading venue for organised crime networks and individuals to carry out illicit activities, with cryptocurrencies the preferred medium for paying for these criminal services," said Madan Oberoi, the director of cyber innovation and outreach unit at Interpol's Global Complex for Innovation (IGCI).

The specialised training provided by Interpol equips law enforcement with the understanding and tools they need to take very real action targeting criminals in the virtual world."
The training is set to continue in November in Brussels, while the agency will also look at law enforcement policy surrounding existing virtual currencies.

The IGCI will also be reaching out to companies and organisations in both public and private sectors in order to better tackle cybercrime issues. "Cybercrime is a domain where information and expertise lie outside the domain of law enforcement agencies," Oberoi said. "We have to reach out to other stakeholders... consult each other and work closely."

Ahead of the 90th Congress, INTERPOL Secretary-General Jürgen Stock announced that the world's largest police force, with 195 member countries, will establish a specialized unit in Singapore to assist countries around the world in the fight against crimes involving virtual assets, including dark web crimes.

Stock said at a press conference that the lack of a regulatory framework for cryptocurrencies such as bitcoin and ethereum poses significant difficulties for law enforcement agencies. Stork said cryptocurrencies and cybercrime (dark web crime) will be a major topic of discussion at Interpol's conference in India.

Stork said: "Because often, law enforcement agencies are not properly trained and properly equipped… Cryptocurrencies are becoming a major threat on a global scale: the ICPO Global Innovation Centre in Singapore is working on a mechanism to address the challenges from these countries. "

Praveen Sinha, Special Director of India's Central Bureau of Investigation (CBI), reiterated that monitoring cybercrime has become increasingly challenging. In addition, he stressed the importance of Interpol in establishing and promoting global police cooperation. The Indian official said, "The only answer is international cooperation, coordination, trust and real-time information sharing."

Both officials emphasized the important role Interpol plays in enhancing global police cooperation. Stork detailed that to complete the organization's Vision 2030, its member countries will investigate the future of policing in an increasingly digital society.

This comes after Europol, the EU's law enforcement cooperation agency, acknowledged last month that criminal activity has risen with the widespread use of cryptocurrencies across borders and industries. Europol has also expressed interest in using blockchain technology to investigate organized crime and money laundering.

Since at least 2015, Interpol has been working to gain more knowledge about bitcoin trading and identify illegal activity on the dark web.

Interpol partnered with cybersecurity firm Trend Micro in 2020 to prevent cryptojacking from affecting Southeast Asian routers, and in March 2020, the agency partnered with South Korean data intelligence firm S2W Labs to investigate dark web activity, including bitcoin trading.

Several years ago, the INTERPOL Global Innovation Integration Center completed specialized training to identify techniques and tactics used to evade detection on the dark web, which often uses non-standard communication protocols and ports.

After the destruction of the Silk Road dark web marketplace, many government agencies and law enforcement have been investigating the remaining dark web marketplaces and how transactions are handled and "hidden". Some of these dark web marketplaces have taken control of the cryptocurrency market.

Cybercrime is one of Interpol's Four Global Programs

Interpol operations are centered around four global programs. In addition to cybercrime, the three other major areas the organization covers are terrorism, organized crime, and financial crime and corruption

- Interpol Doesn't Directly Lead Cyber Investigations

One of the common misconceptions about Interpol is that it directly leads investigations and that its agents are the ones that make arrests of cyber kingpins. The reality is that Interpol is more like a program management agency. It helps different countries' law enforcement agencies work with one another; it brings analysis of data about cybercrime from different countries and can help track down global cybercriminal organizations; and it can offer significant administrative support and professional training to law enforcement at different agencies around the world. In many ways, Interpol is the largest threat intelligence operation in the world.

"I cannot lead an investigation. I can coordinate, I can support, I can help facilitate those operations, but I can't directly tell a country what to do," explained Interpol's Jones.

While Interpol may issue advisories about criminals, it is up to local law enforcement agencies to make the arrests when they find these lawbreakers. It takes coordination and negotiation between countries to decide on criminal jurisdiction, depending on where the crime was determined to happen, where the criminal is from, and where they were nabbed.

- Work Is Coordinated Across 196 Member Countries

Interpol is a politically neutral organization that is run through a constitutional system that operates through the full support and representative governance of its 196 member countries.

"We have elections, and in 2024 we'll have a new Secretary General elected, and that Secretary General sets the direction for the organization," Jones said. "We have a constitution, and we have different articles in that constitution that precludes us from being involved in anything of political, military, racist, or religious."

Think of member countries as a pyramid, Jones said, where at the top there are 30 to 40 countries with advanced cybercrime fighting capabilities.

"They can run a full investigation, they can do everything that needs to be done and they can work very, very effectively together in that trust model with certain countries, but also in those 30 to 40 countries there are going to be those that are not going to speak to each other," he said.

In those instances, Interpol acts as a neutral go-between to help coordinate between those different countries that may not play nicely together and to help them safely collaborate on what they each know about cybercriminal activities in order to help aid global investigations.

Meantime, in the middle strata are the countries who have a "reasonable capability and capacity" for fighting cybercrime. For these countries, a big part of the focus is global information-sharing and analysis.

"So, we look in their countries and say: 'Okay, where are the victims? Where are the threat actors? Where did they structure that country?' Then, through our response, we activate those data sets, we share that information into those countries affected by that activity, and we offer to help support and coordinate those operations with them," he said.

Finally, there are the counties that have very few capabilities and very little capacity for fighting cybercrime. In those cases the goal is to help them prevent crime in their country, feed them information, and help them build out their capabilities through training and support.

- Interpol's Global Cyber Program Consists of Three Major Components

The mission statement of the Interpol cybercrime program is "Reducing the global impact of cybercrime and protecting communities for a safer world." According to Jones, while this may mean helping to orchestrate arrests and shut down criminal groups, a lot of this work is around investigating cybercriminal activity and gathering evidence, disrupting cybercriminal capabilities, and helping countries build up their internal capacity to do this work themselves — and also to prevent attacks in the future.

In order to carry out this mission, the program is broken up into three major components.

Cybercrime Threat Response covers the aggregation of data and information from law enforcement and private sector partners around the globe. This is Interpol's threat intel powerhouse, which puts out threat advisories and threat assessment reports. Then there is the Cyber Strategy and Capabilities Development component, which handles a lot of the outreach and training between agencies and private enterprises. And, finally, there's Cybercrime Operations, which handles not only law enforcement coordination but also takedowns of compromised infrastructure.

"Over the last five years we've become more operationally focused," Jones said, explaining that this means that they've blended capabilities development with operational work, so they're training countries as they help them run investigations. "The way we've moved is that now when we do a training, it comes with an operation — we'll provide the training to the countries that

don't have those capabilities and that want to increase their capacity to deal with cybercrime."

- Coordinated Through Regional Desks

Coordinating investigative and operational cyber research can be a tough task when Interpol deals with its members on a country-by-country basis, explains Jones, who says that this kind of 1:1 communication doesn't scale well. In order to help facilitate investigations and operations, Interpol organizes a lot of its work through four regional operations desks in Africa, Asia & the South Pacific, Europe, and the Americas.

"When we go into a single country at a time, that's not always really effective or the best use of our resources, which is why we have a regional model to do that work," Jones said.

Each of the regions is an important spoke of the work, though a lot of the leadership for Interpol's cybercrime program is based in Singapore, which is where the ASEAN regional desk is located and where Jones himself is headquartered. Singapore is the home of the Interpol Innovation Centre, which runs four labs for facilitating research around responsible AI, emerging threats, digital forensics, and global developments around tech, strategy, and policy.

Built and funded in partnership with the Singapore government, this hub was built to help break Interpol out of its mold as a "Western-leaning" organization and to tap into Singapore's position as a leader in tech and finance.

"You have all the big tech companies that have their regionals there, and all of the banking networks are there as well," Jones explained. "I'm able to jump on a bus, go down to Microsoft, and have a meeting with the APAC CISO without having to fly 13 hours somewhere."

- Public Partnership Depends on Reporting and Data

In addition to coordinating data collection and action across law enforcement and other government agencies, another big part of Interpol's cybercrime program is collaboration with private partners. Whether it is financial organizations or giant global tech firms, private partners feed Interpol with valuable data that feeds its threat intelligence capabilities. The giant tech firms are also big partners in helping to disrupt cybercrime operations, taking down infrastructure that feeds illicit activity "without breaking the Internet," Jones said.

ii. Goals of Interpol

Digital crime has evolved from isolated incidents to a sophisticated underground economy reaching into every aspect of society and affecting everyone from individuals to big companies.

A single attack might have threat actors coordinating from several countries, malicious infrastructure hosted across multiple jurisdictions, and victims

located around the world. Cybercrime's global reach requires a global strategic approach and a collaborative mindset to effectively fight back.

The total value lost to cybercrime yearly is now comparable to the gross domestic product of major economies. As this financial impact continues to grow exponentially, with projected costs expected to more than double in just a few years, the resulting shadow economy funds further criminal innovation and attracts more participants to these illicit activities.

It comes as no surprise that as digital technologies become increasingly embedded in our daily lives, the traditional boundaries between cybercrime and conventional criminal activity continue to disappear. Even crimes once considered purely physical now incorporate cyber elements.

Yet despite the technical nature of these threats, the human element remains the most common vulnerability. Most breaches involve some form of human interaction - often unintentionally as we are all susceptible to manipulation by increasingly sophisticated criminal techniques.

Combating these evolving threats presents unprecedented challenges for law enforcement worldwide. Digital evidence can be volatile, criminals often operate behind layers of anonymity-enhancing technologies, and investigations become entangled in a web of differing legal systems and political sensitivities.

At the same time, cybercriminals can acquire powerful 'off-the-shelf' tools, commercial kits, and hacking services with minimal effort, lowering the barriers to entry and enabling even less technically skilled individuals to launch complex attacks.

Addressing this growing global threat requires coordinated international efforts with the public and private sectors. Only through strategic collaboration, enhanced information sharing, and increased public awareness can we work toward building a safer digital world for everyone in this interconnected age.

The Global Cybercrime Strategy outlines INTERPOL's plan to support its 195 member countries in combating cybercrime in line with INTERPOL's Strategic Framework for the period 2022 to 2025.

EXPECTED OUTCOMES OF THE OBJECTIVES

OBJECTIVE 1

- Enhanced processes for obtaining information from member countries and private-sector partners for the proactive development of actionable intelligence.
- Development of high-quality intelligence, assessments and analytical products that meet member countries' law enforcement purposes and actions.
- Stronger member country engagement in information sharing at the national, regional and global level in order to develop an in-depth understanding of the cybercrime threat landscape.

OBJECTIVE 2

- Prevention of cybercrime to better protect communities through coordinated law enforcement action and raising public awareness by collaborating with external partners.
- Disruption of organized crime groups and their ecosystem, both proactively and reactively.
- Attribution of criminal acts and actors behind cybercrime by coordinating global law enforcement cooperation and by leading regional coordination through the Regional Cybercrime Operations Desk model for judicial outcomes.

OBJECTIVE 3

- Delivery of capabilities development and the implementation of capacity-building projects to increase member countries' ability to fight cybercrime.
- Wider use of INTERPOL tools and platforms through which law enforcement agencies and partners can share information, knowledge and experience on cybercrime.
- Enhanced and expanded partnerships through joint activities, strategic alignment and policy formulation based on trust that is induced by technological and regulatory means.

OBJECTIVE 4

- Development of INTERPOL's position on cyber policy and an international convention on cybercrime, reflecting the global law enforcement perspective.
- Adoption of strategic recommendations and briefings for member countries to promote INTERPOL's channels, services and capabilities.
- Stronger INTERPOL leadership in the global security architecture and in the global ecosystem of cybersecurity.

CAPABILITIES

- STRATEGIC SUPPORT
- KNOWLEDGE MANAGEMENT
- GLOBAL AND REGIONAL NETWORKS
- OPERATIONAL COORDINATION - SUPPORT
- ANALYTICAL SUPPORT AND INTELLIGENCE
- CAPACITY BUILDING
- INFORMATION SHARING AND KNOWLEDGE NETWORK
- PARTNERSHIPS
- GUIDELINES AND FRAMEWORKS

7. Difference between Dark web and Deep web

“Deep web” and “dark web” are not interchangeable terms. Although the entire dark web is part of the deep web, the deep web is not a part of the dark web. Simply put, the deep web is any part of the internet that is not indexed by search engines. This includes websites that gate their content behind paywalls, password-protected websites, and even the contents of your email. The dark web, on the other hand, uses encryption software to provide even greater security.

Millions of regular internet users access private databases such as email inboxes and credit card accounts daily. These pages are not indexed by search engines and are protected behind security walls, authentication forms, and passwords on the deep web.
Approximately 90% of all websites are on the deep web, and many are used by entities such as corporations, government agencies, and nonprofits. What's known as the dark web exists within the deep web; it's an area of the internet that is only accessible by users who have a Tor browser installed. In general, most average internet users will never need to access content on the dark web, although it is perfectly legal to use Tor.

The Internet is a complicated information network; the overwhelming majority of that is simply not available to any average user. The part that we are most familiar with is really just what we might think of as the surface web. This includes sites we regularly visit, be it our social media networks, news outlets, or e-commerce sites – indexed by traditional search engines like Google or Bing. This very well-known territory hides a lot more – a giant called the deep web and an even smaller part called the dark web.

Hence, the deep web literally comprises all those parts of the internet that are not indexed by search engines. The kinds of content present in this region include private databases, medical records, academic journals, and other sensitive information that requires special permission to access. For example, every academic institution holds valuable resources within its online libraries that are important to its students and researchers who have legitimate access but not for public consumption.

The dark web is the portion of the deep web that has specifically been hidden from users and, only with specific programs like Tor, it can be accessed. It is associated with illegal activities such as drug dealing and hacking, although for some, especially privacy advocates, it is a safe haven. The deep web vs dark web can together be said to make up the inner layers of the internet,

which sometimes do meet some of the needs for accessibility, privacy, and security

It is estimated that around 96% of the internet is part of the deep web, compared to only 4% of the surface web. Understanding the distinction between the deep and dark web can make it possible for activists and journalists working in repressive regimes to safely share information without governments monitoring them. This article aims to clarify these concepts, explore the differences between them and highlight the associated goals and risks.

Deep Web Use Cases	Dark Web Use Cases
Routine Use: Users logging into routine websites such as bank accounts or social media using personal credentials do so on the deep web without realizing it.	**Uncensored Journalism**: Journalists use the dark web frequently (usually via the Tor Project), especially when they are working on sensitive stories or traveling to foreign countries.
Secure Payments: Every time consumers pay for a product or service online, they enter payment information through the deep web.	**Free Speech**: Citizens of oppressive regimes (such as North Korea) use the dark web to safely organize and speak freely. The dark web was critical for protesters **avoiding Net censorship during the Arab Spring** after governments shut down access to social media.
Campaigns: Website Developers can have certain part of their websites or pages on the deep web to track campaigns, such as displaying specific homepage designs for users on specific locations	**Safety**: Many corporate and government whistleblowers rely on the dark web to ensure their safety. Notably, WikiLeaks has a counterpart on the dark web for exactly this reason.

Paid Subscriptions: Paywalls prevent search engine crawlers from accessing certain content that only users who paid for or subscribed to can access. This content, by definition, is on the deep web.

Privacy: Victims of stalking and similar online threats may use the dark web to cover their tracks as they find their way out of their situation.

i.Deep Web

The deep web refers to parts of the internet not fully accessible through standard search engines like Google, Yahoo!, and Bing.
The deep web includes pages that were not indexed, fee-for-service (FFS) sites, private databases, intranets, and sites found on the dark web. Also called the hidden web or invisible web, the deep web is different from the surface web, where contents can be accessed through search engines. Information on sites like Investopedia is part of the surface web, as it can be reached through search engines. Most experts estimate that the deep web is much bigger than the surface web. Many web pages are dynamically generated or do not have links from other sites. Without links from previously indexed sites, the search engines cannot find them. That is why getting links from other pages is a basic principle of search engine optimization (SEO).

Fee-for-service sites are another major source of deep web content. Although fee-for-service sites, such as Netflix, are visible on the web, most of their content is not. Customers must pay a fee, create a user id, and set up a password to get most of the material offered by these sites. Only those willing and able to pay the fees for these sites can get access to their content. This restriction of information to paying customers goes against the egalitarian spirit of the early internet. While access to movies might seem trivial, serious research tools like JSTOR and Statista also charge fees.

Private databases are also a crucial component of the deep web. Private databases can be as simple as a few photos shared between friends on Dropbox. They also include financial transactions made on major sites like PayPal. The key feature of private databases is that people wish to share it with just certain people or preserve this information without having it publicly accessible to everyone. That makes it part of the deep web rather than the surface web.

Finally, dark websites are part of the deep web. Silk Road was perhaps the most infamous site on the dark web. Many dark websites can be reached by specialized search engines designed for that purpose, but not by standard search engines. In order to access these search engines and sites, it is necessary to use specific browsers, such as the Tor Browser. The dark web allows legitimate users to avoid censorship, but it also creates opportunities for cybercrime.

The deep web gives users access to far more information than the surface web. This information may simply be pages that aren't important enough to be listed. However, it also includes the latest TV shows, databases that are essential for managing your personal finances, and stories that are censored on the surface web. Much of the content on the deep web would not be available at all if only the surface web existed. Privacy, which is usually provided by encryption, is another benefit of the deep web. Encryption on the deep web allows fees for service sites to keep their content away from nonpaying Internet users while serving it to their customers. The encryption of databases is absolutely necessary for all forms of fintech to function properly. Without this security, neither firms nor individuals could safely conduct financial transactions over the Internet. The dark web was designed mainly to provide users with more privacy.

Perhaps the most serious criticism of the deep web is that it undermines the openness and equality of the internet. In the 1990s, there were hopes that the Internet would give everyone an equal chance to access everything. Instead, fee-for-service sites give access to premium productivity tools only to those who can afford them. In many cases, crucial tools cost hundreds and even thousands of dollars, creating barriers to entry.

The dark web creates another set of issues for the deep web. Those with advantages in knowledge rather than money can use it to commit crimes. In some cases, people hiding behind the dark web attack legitimate users on the surface web, reducing the quality of the Internet for everyone.

8. Access to the Dark web

The dark web is a subsection of the deep web that conventional search engines cannot index. As an encrypted network of websites, the dark web can only be accessed using special browsers such as Tor. Tor, formerly an acronym for “The Onion Router,” is a free and open-source software intended to protect the personal privacy of its users and keep their internet activities unmonitored.

While the dark web is known for both legitimate and illegitimate purposes, it remains notorious for facilitating illegal and deviant activities ranging from drug dealing to human trafficking, arms dealing, and extremist recruitment. Accordingly, researching and understanding the dark web is a critical and essential step in fighting and preventing cybercrime. However, studying the dark web poses unique challenges.

However, users can also use the Tor network to conceal illegal activities, making it a primary target for law enforcement and hackers. To access the dark web, you need to download a dark web browser such as Tor Browser or Tails. You then need to configure the browser to connect to the Tor network.

9. The Crimes committed on the Dark web and Deep web

Crimes Associated With the "Dark Web"

The Dark Web is the center of criminal attacks because it provides anonymity and serves as a doorway into the criminal world. The following are some of the most well-known crimes committed on the Dark Web:

Drug Trafficking

The dark web is an unlawful marketplace for the sale of illegal and dangerous substances in exchange for crypto currency. Bitcoin, Ethereum, and Ripple are just a few examples.

Silk Road was also a well-known marketplace for unlicensed medications and illegal drugs. The FBI took down this website in 2013. Agora is a website that was shut down as well. There are a number of such websites that operate on the Dark Web for the sale and distribution of illegal drugs. Visually pleasing, these sites resemble any other shopping website, with a brief description of the items and a photograph to accompany them.

Human Trafficking

Human trafficking takes place at Black Death, a dark web site. The British model Chloe Ayling is one of the victims of human trafficking on the Dark Web. According to a 2017 survey, the majority of human trafficking survivors were recruited for sex and labor trafficking.

Other reports have demonstrated that the Dark Web has aided in the concealment of this crime. Black Death is a dark web organization that operates by often changing URLs.

Information Leaks and Theft

Many anonymity-supporting platforms, such as TOR, are helpful resources for whistleblowers, activists, and law enforcement. So, it is reasonable to believe that specialized sites make it easier for individuals to exchange physical and private information, such as passwords and access to passwords for the surface Web, paid pornography sites, and PayPal credentials.

Hackers use the Dark Web to spread sensitive information. On the dark web, a hacker gang once exposed the credit card accounts and login information for around 32 million Ashley Madison customers as a 9.7GB data dump. Employees are even paid by dark web hubs to expose corporate information.

Murder and Contract Killers

The Assassination Market website is a prediction market where a party can gamble on a person's death date and receive a payout if the date is "guessed" correctly. This encourages assassination since the assassin, knowing when the event will take place, can benefit by placing a precise bet on the time the subject will die. It is much more difficult to assign criminal guilt for the assassination because the payment is for knowing the date rather than doing the assassination itself.

On the dark web, there are even websites where you may hire professional assassins. Once, a hacker known as 'bRpsd' gained access to BesaMafia's website and leaked its information online. User accounts, personal conversations, eight hit-orders, and a folder containing nearly 200 victim photos were all exposed.

Terrorism

Terrorists and the dark Web appear to be made for one other; the latter requires an anonymous network that is both accessible and inaccessible. Terrorists would struggle to maintain a presence on the surface Web because their sites might be easily shut down and, more crucially, traced back to the original poster.

While the dark Web may not have the same broad appeal as the surface Web, the hidden ecology is ideal for propaganda, recruitment, finance, and planning,

which is in line with our first perception of the dark Web as an unregulated cyberspace.

Exploit Markets

Exploits are malware that takes advantage of software defects before they are fixed. Zero-day exploits target zero-day vulnerabilities, which are those for which the vendor has yet to release an official patch. The term “zero-day” refers to the fact that the programmer had no time to fix the vulnerability.

Exploit markets are marketplaces for buying and selling zero-day exploits, and the price of an exploit is determined by the popularity of the target software as well as the difficulty of cracking it.

Proxying and Onion-Cloning

Users of Tor-like platforms are vulnerable to attack because of their anonymity. The normal ‘HTTPS’ in the URL of such a site which indicates that it is secure does not appear. They must bookmark the TOR page to ensure they are on the legitimate site.

When a fraudster uses website proxying, the user is tricked into believing he is on the original page, and the scammer then re-edits the link to send the user to his scam URL. When a user pays in crypto-currency, the money is transferred to the scammer instead.

Onion Cloning is comparable to proxying. In order to steal money from the user, the scammer builds a replica of the original site or page and modifies the links so that the user is referred to their scammed site.

Illegal Financial Transactions

Theft and sale of a user’s credit card credentials and personal information are referred to as carding frauds. On the Dark Web, it is the most popular sort of criminal activity.

Credit and debit cards are sold on darknet markets. Multiple URLs redirect the user to the same page on these sites. Vendors from other forums submit advertisements describing what they have. Vendors sell cards at a lesser cost.

Carding frauds are also possible on some money transfer services. This service is available through a website called Atlantic Carding, and the more you spend, the more you get. Business credit card accounts and even infinite credit

card accounts linked to ultra-high-net-worth individuals are up for grabs. The user's personal information, such as name, address, and so on, are available at a price.

Arms Trafficking

It serves as a conduit for illegal arms trafficking. According to a RAND Corporation study, the dark web is expanding the availability of firearms at similar prices to those seen on black market streets. Europe is also discovered to be the main supply of firearms. The Dark Web has become a forum for criminal groups and terrorists, with Germany coming in third with 5.31 percent.

Euroarms is a website that sells a variety of firearms that may be delivered to your door in any European country. The ammunition for these weapons is sold separately, and that website should be discovered on the dark Web.

The Dark Web and Malware

The dark web market is a place where illegal materials can be bought and sold. It is a home for a variety of malicious software and services and malware is a critical component of many cyber-attacks occurring through the Dark web.

Cryptominers deploy a variety of malwares to carry out their unlawful cyber activities and these are some of the most common malwares:

Data Stealing Trojans

They can also collect passwords from the clipboard, intercept keystrokes, bypass or disable antivirus software, and transfer files to the attacker's email address.

Ransomware

Ransomware encrypts your computer or files and demands a ransom payment before they may be decrypted. Ransomware is a type of malicious assault that takes control of a user's system and prevents that user from accessing it. There are various methods through which ransomware criminals select the organizations they attack. Some businesses are attractive targets because they appear to be more willing to pay a ransom quickly.

Medical facilities and government entities, for example, frequently require fast access to their files. Law firms and other sensitive data organizations may be

ready to pay to keep news of a hack hidden, and these organizations may be particularly vulnerable to leakware attacks.

Remote Access Trojans (RATs)

Remote Access Trojans allow an attacker to monitor user activity, take screenshots, run files and commands, activate the webcam and microphone, and download files from the internet. DarkComet, CyberGate, ProRAT, Turkojan, Back Orifice, Cerberus Rat, and Spy-Net are examples of popular RATs.

Botnet Malware

It's a multipurpose malware that demonstrates how fraudsters are broadening their attack methods. The ransomware, keylogger, and botnet capabilities are all included in the virus. Botnet Ransomware is an example of Virobot. When Virobot infects a computer, it joins a spam botnet that spreads the malware to new people. The ransomware uses RSA encryption to encrypt the data on the targeted system. Meanwhile, the botnet's keylogger captures logged data from victims and sends it to the C2 server. Virobot's botnet function leverages Microsoft Outlook on an infected machine to send spam emails to everyone on the user's contact list.

ATM Malware

These Trojans are used to steal money from ATM machines. ATM hacking is profitable due to the fact that a single ATM might contain up to $100,000 in cash. ATM malware is the most expensive of all malwares and a single piece of malware can be used to attack multiple ATMs. Exploits look for flaws in a system or software and take advantage of them. The exploits available on the dark web are designed to work on a variety of platforms. Due to the large market size, Windows-based exploits are the most popular.

Monitoring the Dark Web

The dark Web in general, and the Tor network in particular, provide a secure platform for cybercriminals to support a wide range of illegal activities, from anonymous marketplaces to secure means of communication to an untraceable and difficult-to-shutdown infrastructure for deploying malware and botnets.

As a result, it has become increasingly vital for security agencies to track and monitor activities on the dark Web, which is currently focused on Tor networks but may expand to other technologies in the near future.

Customers' Web data could be analyzed by security agencies to detect connections to non-standard sites. Depending on the customer's level of Web activity, this may not aid in tracking down links to the dark Web, but it may reveal insights about activities hosted with rogue top-level domains. This can be accomplished without invading the user's privacy because only the destinations of Web requests need to be monitored, not who is connecting to them.

Pastebin and other similar sites are frequently used to distribute contact information and addresses for new hidden services. These sites would have to be constantly monitored in order to detect message exchanges containing new dark Web domains.

Most hidden services are highly volatile and frequently go offline, only to reappear later under a new domain name. It is critical to capture a picture of each new site as soon as it is discovered, for further study or monitoring its online activities.

Once the data for a hidden service (any of the websites on the dark Web) has been collected, creating a semantic database including crucial information about the hidden site can assist in tracking future illegal activity on the site and associating them with malicious actors.

Finally, it would be beneficial to concentrate on profiling transactions on dark Web marketplaces in order to collect information on vendors, users, and the types of commodities transacted.

In Conclusion

The dark web is a part of the Internet where people go to accomplish things in secret and leave no trace. It has become a center for illegal activities such as child pornography, arms trafficking, drug trafficking, and onion cloning, among others. The anonymity provided by this platform is the driving force behind these activities.

Other trends are beginning to emerge as a result of recent discoveries regarding widespread Internet surveillance by nation-states and recent arrests of cybercriminals operating dark Web sites. It wouldn't be shocking if the criminal underworld became more divided into various dark nets or private networks, making investigators' jobs even more difficult.

The dark Web has the capability to host an escalating number of malicious services and activities, and new major marketplaces will inevitably arise. To cope with future occurrences as promptly as possible, security professionals

and law enforcement agencies must remain watchful to develop new approaches for detecting emerging malicious activities

10. Current global impacts of Dark web crimes

ECONOMIC

The global cost of cybercrime will increase to $11.9 trillion USD in 2026, going all the way up to $19.7 trillion USD in 2030 - surpassing the current GDP of China.

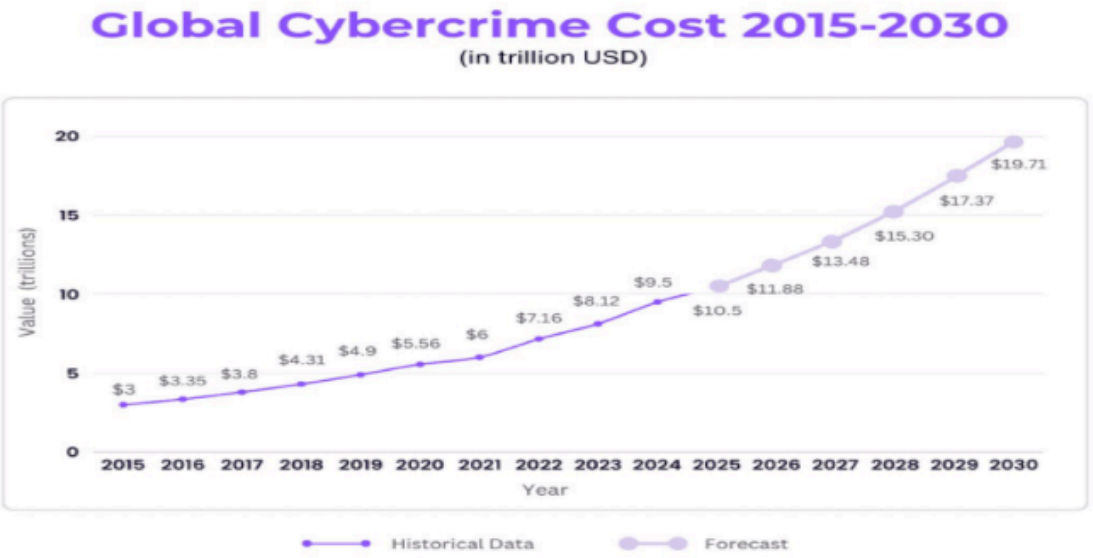
The 10 countries at highest and lowest risk: European and North American countries are among the safest, while Latin America and the Middle East are at high risk.

Ransomware, phishing, and social engineering attacks continue to be the most popular ways of committing cybercrime, while some of the biggest rises in attacks have been in cryptojacking (136%) and software supply chain attacks (300%).

The US (3.8%) is the country with most users rejected via the KYC process, followed by Vietnam (3.2%) and Indonesia (1.9%), according to Proxyrack internal data. They are also the three countries with most accounts suspended or locked due to potential malicious use.

Global Cybercrime Cost Forecast

Cybercrime continues to grow, posing one of the most severe threats to global security and economies. However, it’s not growing linearly—our research shows that it’s increasing exponentially.



Using global data from 2015 to 2024 to create a forecasting model, we predict that the cost of cybercrime around the world will go up to $11.9 trillion USD in 2026. By 2030, cybercrime will cost $19.7 trillion USD, eclipsing the current nominal GDP of China.
Katy Salgado, Operations Manager at Proxyrack and head of this cybercrime research, comments on what this means for businesses looking at cybersecurity measures to protect themselves:

The exponential rise in the cost of cybercrime signals a growing global threat that will likely demand more advanced strategies and investments in cybersecurity. This trend emphasizes the need to stay proactive with preventative measures, enhance threat detection, and refine internal systems to address this escalating risk. It also highlights an increasing focus on resilience and adaptation to stay ahead of cybercriminal activities.

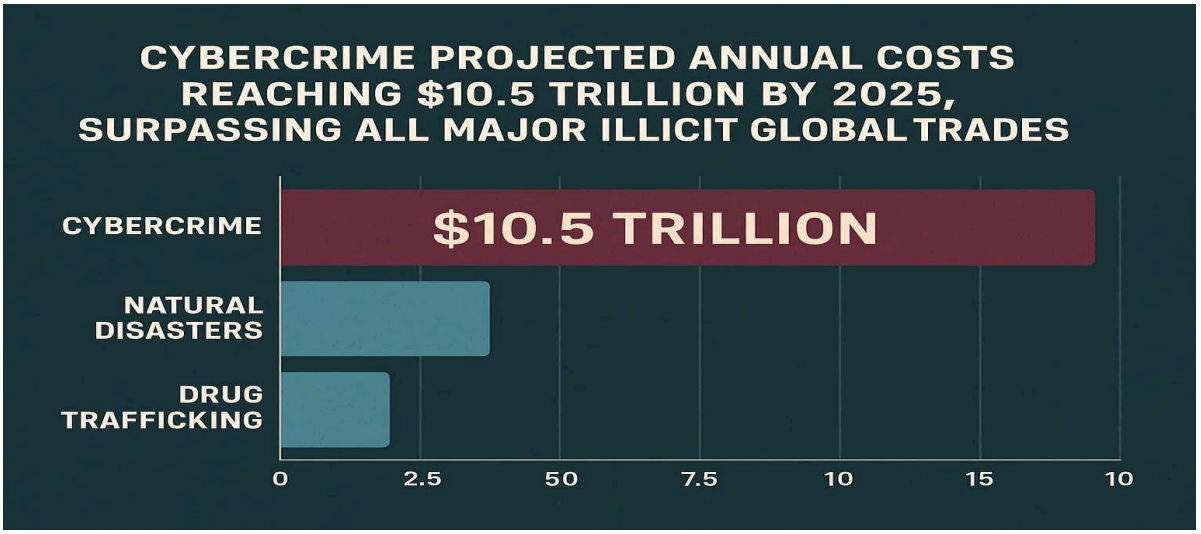
Cybercrime by Country
To assess the risk of cybercrime across countries, we looked at several factors. These include measures and indexes for cybercrime exposure, cybersecurity capabilities/preparedness, digital development, and legislation.
With four countries on this list (Panama, Chile, Costa Rica, Uruguay), Latin America seems to have some of the biggest problems with cybersecurity. The Middle East also seems to have some issues; though both the UAE and Saudi Arabia got perfect GCI scores, showing their commitment to cybersecurity development, there is still a lot of work to be done to reduce their exposure

and increase their readiness for cybercrime.

Top 10 countries most at risk from cybercrime

RANK	COUNTRY	BASEL AML INDEX	CYBERSECURITY EXPOSURE INDEX	NCSI	DIGITAL DEVELOPMENT LEVEL	GCI	CYBERCRIME RISK SCORE
1	Panama	5.81	5.69	4.32	5.16	3.35	4.86
2	Belarus	5.21	6.14	3.51	4.34	3.86	4.61
3	Chile	4.03	4.69	5.07	4.11	2.98	4.18
4	Costa Rica	4.58	4.38	4.68	3.77	2.49	3.98
5	Georgia	4.64	3.83	5.58	4.64	0.81	3.90
6	United Arab Emirates	5.70	3.59	5.97	3.11	0.00	3.68
7	Thailand	5.80	4.45	4.00	3.08	0.08	3.48
8	Saudi Arabia	5.28	3.90	4.08	2.92	0.00	3.24
9	Uruguay	4.07	3.48	3.92	3.15	0.53	3.03
10	Mauritius	5.03	2.00	3.75	3.99	0.00	2.95

Meanwhile, Europe leads the way in cybersecurity, with Nordic countries scoring especially well. France, the UK, Spain and Germany are also among the lowest-risk countries, with the US (notwithstanding its list of cybercrime hot spots) and Canada rounding off the list.



The global cost of cybercrime is on track to hit $10.5 trillion annually by 2025. This isn't just a big number; it's an economy. If cybercrime were a country, its GDP would be the third largest in the world, trailing only the United States and China. This figure represents what Cybersecurity Ventures calls the greatest transfer of economic wealth in history, a sum that eclipses the

damage from natural disasters and the global trade of all major illegal drugs combined.
When you connect this staggering financial projection with the rise of professionalized Cybercrime as a Service (CaaS) platforms, a clear picture emerges. Cybercrime is no longer a scattered collection of individual acts but a mature, globalized shadow economy. It has its own research and development, sophisticated supply chains, and market forces that commoditize attack tools, making them available to anyone with a credit card and a grudge. This article breaks down the essential cybercrime statistics for 2025. We'll explore the real world costs behind the headlines, dissect the AI driven attack vectors that define the modern threat landscape, and provide a no nonsense playbook for building resilience. The rising costs are forcing a strategic shift in how businesses approach security, moving beyond simple compliance. This requires a deep understanding of your organization's unique risks, which can be uncovered through robust security assessments like internal vs external penetration testing.

The Global Cybersecurity Outlook 2024 revealed significant cyber inequity, exposing stark disparities in resilience between small and large organizations. The World Economic Forum’s Global Risks Report 2024 found that cyber insecurity is a global risk over multiple time horizons, with cyber risks such as malware, deepfakes and misinformation threatening supply chains, financial stability and democratic systems. Additionally, the Chief Risk Officers Outlook from October 2024 ranked cyber risk among the top three threats severely affecting organizations.
A striking 71% of chief risk officers anticipated severe organizational disruptions due to cyber risks and criminal activity.
In 2024 the world witnessed the largest IT outage in history, disrupting airlines, banks, broadcasters, healthcare providers, retail payment systems and ATMs globally and causing an estimated $5 billion in losses.
This incident underscored the vulnerabilities stemming from dependence on a limited number of critical providers. Cyberthreats continued to escalate, with 72% of respondents to the Global Cybersecurity Outlook (GCO) survey (see Appendix: Methodology) reporting a rise in cyber risks. The survey further revealed that cybercrime grew in both frequency and sophistication, marked by ransomware attacks, AI-enhanced tactics – such as phishing, vishing and deepfakes – and a notable increase in supply chain attacks.

The challenge for the year ahead

The 2025 report finds that a series of compounding factors are driving an escalating complexity in the cyber landscape:

- Geopolitical tensions are contributing to a more uncertain environment.
- Increased integration and dependence on more complex supply chains are leading to a more opaque and unpredictable risk landscape.
- The rapid adoption of emerging technologies is contributing to new vulnerabilities and new threats.

Meanwhile, the proliferation of international regulatory requirements adds an additional compliance burden for organizations. All of these challenges are compounded by a widening skills gap, further complicating the ability to manage cyber risks effectively.

Together, these factors drive increasing complexity and unpredictability in the cyber landscape, which affects organizations in many ways. First, it drives inequity throughout the cyber ecosystem, undermining resilience by creating a divide between those organizations that have the resources to adapt and those that do not and subsequently fall behind. This affects the resilience of the ecosystem, because many larger and more mature organizations typically depend on extensive networks of smaller, often less-mature suppliers, and any incident affecting them could also impact the entire supply chain. Second, it drives greater demand for more specialist skills in cybersecurity, further exacerbating the skills gap. Keeping up with technological advances requires more specific skills that are in greater demand in the cyber skills market. At the same time, complexity puts increasing pressure on often already stretched cybersecurity teams.

These challenges demand a comprehensive reevaluation of cyber strategies at the organizational and ecosystem level to address the complexity that has become inherent in the cyber landscape.7 A broader understanding of cyber risk is necessary that goes beyond mere “IT” and considers cyber from an overall business risk perspective.

11. Questions to be addressed

1. How to prevent people accessing the dark web?
2. What steps can INTERPOL take to prevent illegal sales on the dark web?

3. How can countries improve international cooperation against dark web crimes?
4. In which ways Interpol can develop its strategies and goals?
5. How to reduce the global impacts of crime on the Dark Web?

12. Bibliography

https://www.britannica.com/topic/Interpol
https://byjus.com/free-ias-prep/interpol/#:~:text=Interpol%20–%20Introduction,prevent%20or%20combat%20international%20crime

https://sopa-tulane-edu.translate.goog/blog/everything-you-should-know-about-dark-web?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc
https://cyberjustice.blog/2023/03/08/enhancing-law-enforcements-cybercrime-response-through-interpols-dark-web-training
https://www.egattorneys.com/common-federal-dark-web-crimes
https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure
https://www.pandasecurity.com/en/mediacenter/dark-web-statistics

https://cyberjustice.blog/2023/03/08/enhancing-law-enforcements-cybercrime-response-through-interpols-dark-web-training
https://www.ibtimes.co.uk/interpol-cryptocurrency-fight-bitcoin-crimes-dark-web-1518264
https://www.ondarknet.com/news/othertornews/interpol-announces-a-new-unit-to-investigate-crimes-related-to-cryptocurrencies-and-the-dark-web
https://www.interpol.int/en/Crimes/Cybercrime
https://www.interpol.int/content/download/19815/file/Cybercrime%20Short%20strategy%20EN.pdf
https://www.darkreading.com/cyberattacks-data-breaches/5-facts-about-how-interpol-fights-cybercrime

https://www.techtarget.com/whatis/definition/deep-Web
https://www.investopedia.com/terms/d/deep-web.asp
https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web
https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-vs-deep-web/

https://www.researchgate.net/publication/369176693_The_Dark_Web_What_Is_It_How_to_Access_It_and_Why_We_Need_to_Study_It
https://www.trendmicro.com/en_no/what-is/dark-web.html

https://oal.law/dark-web-crimes-addressing-the-cyber-threats-and-crimes-associated-with-the-dark-web

https://www.proxyrack.com/blog/global-cybercrime-report-2025
https://deepstrike.io/blog/cybercrime-statistics-2025
https://www.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/1-understanding-complexity-in-cyberspace-587e8c5eba