CYBERCRIME AND CYBER LAWS: INTERNATIONAL DIMENSION

[**Issue Number 104 - April 2018**](https://www.lebarmy.gov.lb/en/content/104-d)

**Cybercrime and cyber laws: International Dimension**
Prepared By: Tania Nehme
ABD global studies.

**Introduction**

Cybercrime is evolving, and new trends are emerging all the time. According to a study made by an Intel company called McAfee, the likely annual cost to the global economy from cybercrime is estimated to be more than $400 billion, where the minimum estimate would be $375 billion in losses, while the maximum could reach as much as $575 billion([[1]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn1%22%20%5Co%20%22)) .In the past, cybercrime was mainly committed by individuals or small groups. However, today, we are seeing exceedingly multifaceted cybercriminal networks that collaborate from across the globe and are able to commit crimes on an astonishing scale.

Some of the cybercrimes are not necessarily new such as theft, fraud, trafficking…but they are evolving in a way where criminals can hide behind a screen and acquire opportunities that land on their laps in a matter of seconds, thus becoming more widespread and damaging. However, new types of crimes have emerged that don’t and can’t exist without the presence of information and communication technologies (ICT’s), and this is where the law encounters an untouched territory.

Looking at the evolution of the internet, we notice that it grew in a completely unpremeditated and unregulated manner causing a nuisance in both the online and offline worlds. The growth rate of cyberspace has been enormous, doubling their population every 100 days. With the spontaneous and almost phenomenal growth of cyberspace, new and delicate issues relating to various legal aspects of cyberspace started emerging. Even the inventors of the Internet could not have really projected and predicted the scope and far reaching consequences of cyberspace. We can thus state that the quicker technology evolves the more legal issues are presented by these innovations. The swift growth of the information and communication technology (ICTs) networks in cyberspace has produced new opportunities that allow criminals to perpetrate crimes, and to exploit online vulnerabilities and assail countries’ crucial and significant information infrastructure.

In order to come up with the most suitable verdict, the law must look into both the criminals and their behavioral analysis, and the victims and the roles they play in the crime. Every crime may be unique, however these elements in a crime usually have a pattern that can be studied and analyzed in order to understand the crime and the outcomes, and further deduce the most rational and reasonable verdict.

Similar to the air one breathes, the internet today has become a necessity in humans’ daily lives. One may not be aware of the immense dependency they have towards it, but inevitably, it is present in every aspects of the human’s lives. The internet is used for various purposes such as work, education, entertainment, research, shopping, banking transactions and several more. Due to its enigmatic entity one begins to wonder how it has become this vast phenomenon that brings the world together.

Since one can hide behind a screen when using the internet, a butterfly effect is very likely to happen, for one click of a button could lead to disastrous consequences and repercussions, especially when an individual purposely seeks to commit the “perfect crime”.

On a domestic level, the numbers of countries that are tackling this issue and have established cybercrime departments are very few. Many countries have unspecialized agents dealing with the issue, making them unfit to tame the situation domestically.

On an international level, no international laws have been established for the cyber space that holds criminals liable to their actions. Judging from the outcomes of cybercrimes threats, there is a great need to develop a strategy preventing future international catastrophes. In July 2005, the first step towards developing an international cyber law was taken because by then, the need for cyber laws started to gain its recognition and importance due to the increase in cybercrimes that came with this new territory and jurisdiction.

Hence why do cyber criminals do what they do? What are their motives? According to sociologist Paul Taylor, cyber criminals are motivated by a variety of reasons, including addiction, curiosity, boredom, power, recognition, politics/ political activism, fame, intellectual challenge, financial gain, and revenge([[2]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn2%22%20%5Co%20%22)). This shows that their crimes are stemmed from the same rationale, any criminal would attest to justify themselves and their crimes. The objectives are the same but the means are different. The critical point for law enforcement, when punishing a cybercriminal, is the ability to measure the actions that take place in the online world and compare them to the tangible and corporeal world. The results of the crime are not new, however the means are new to law enforcements. Can the law compare a murder where the victim was strangled through the murder’s bare hands, to another murder that occurs as a result of cyber bullying or endorsement of suicide through brainwash? Here, the victim was murdered, and it was the criminal’s intention to hurt the victim in both cases, therefore, should the criminal’s punishment be the same?

**Cybercrimes: Delimitations**

Cybercrime is a new subject the world is dealing with, thus the information found on the subject manner is highly generalized and shallow. Many individuals are trying to contribute to this subject, but are failing to organize their points of view, due to the complex and enigmatic elements the cyber world possess. Moreover, the statistics gathered to study cyber-attacks are inaccurate. In the case of personal cyber-attacks, victims rarely speak up because they feel indignant as citizens when their state does not take their cases seriously and prioritizes them. And, when it comes to the statistics of global cyber-attacks, not all companies, global websites and government agencies admit to being victims of cyber-attacks to avoid public humiliation and bad reputation. Moreover, there are many deliberations on the definition of cybercrimes and what is and isn’t considered as such. Therefore trying to understand the subject without having a clear definition and clear organized prospective on how to explain these crimes can complicate the research process. This paper however contributes to allowing readers to understand cybercrimes and learn about the different approaches one can take in order to explain a complex crime, and analyze it in order to deduce a fair verdict.

**Cybercrimes in Perspective**

Albert Einstein once said: “If you can't explain it simply, you don't understand it well enough.” Thus three approaches were used in order to simplify the complexity of cybercrimes; first by defining cybercrimes, then by mentioning the types of cybercrimes that occur in the cyber world, and finally by categorizing cybercrimes from different prospectives and points of view.

In general, cybercrime is a term for any illegal activity that employs a computer as its primary resource. The U.S. Department of Justice goes furthermore and incorporates in the definition “any illegal activity that utilizes a computer for the storage of evidence”([[3]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn3%22%20%5Co%20%22)).

However, there are a number of controversial issues surrounding the definition of cybercrime. One of the problems is the different opinions the majority of the law enforcers have on whether certain cyber activities should be considered as cybercrimes or even crimes in general. The ability to draw a line between what is acceptable and what isn’t is the dilemma they deal with. For example should catfishing (the act of baiting individual/s into a relationship of some through the creation of a fictional online persona) someone online be considered as a crime? In the offline world, giving someone a fake name isn’t considered as a national crime. However in the online world, due to lack of physical contact, it could be considered as pedophilia and child pornography for example, when the cat fisher is a 40 year old male who infiltrates himself in a conversation with an 11 year old girl by posing as her peer in order to freely converse with her and eventually obtain unethical photos of her after gaining her trust. Moreover, whose fault is it? The 40 years old male who is taking advantage of the anonymity of the internet, or the vulnerable girl who at some point willingly gives her “peer” photos of herself?

Another controversial example is the dilemma of being put under the position to choose which human right/law is more important to stand behind when dealing with the internet. For example, we take the issue of digital surveillance and its impact on civil liberties. Ever since the terrorist attacks on the World Trade Center of 9/11, many citizens have stood behind the idea of curtailing some individual rights to privacy of information for better security in return. Government surveillance networks monitor massive volumes of personal and confidential communications and exert artificial intelligence applications to strain and “clean” out relevant data([[4]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn4%22%20%5Co%20%22)). Even though these types of extensive surveillance could significantly decrease the possibility of cybercrime, it is nearly unfeasible to do without violating individual privacy. Furthermore, due to the fact that these surveillance organizations are activated in secret, they are not open to scrutiny.

**Diversity: Types of Cybercrimes**

**A: Hacking:**

This is a type of crime where a person’s computer is broken into (similar to breaking into a person’s house in the real world) in order to access that person’s personal, sensitive, and private information. In hacking, the criminal can use a variety of programs called “malicious software” or “malware” to enter a person’s computer. These programs can even allow the person’s computer to be accessed from a remote location. Hacking also has sub-divisions that include the intention of hacking such as:

• Identity Theft: This is where a criminal accesses personal data such as a person’s bank account, credit cards, Social Security, debit card and other sensitive information, and take on that person’s life while using their name and account. Moreover the criminal can steal the victim’s identity by creating social media profiles or emails in the victims’ names to purposely harm them or to pretend to be them.

• Electronic Funds Transfer Fraud: This is when valid credit card numbers are captured either through hacking or by physically stealing the card, and the digital information stored on a card is then recreated. For example, in 1994, Vladimir Levin who is a Russian hacker was able to hack into the computers of Citibank's central wire transfer department, and then transferred funds from large corporate accounts to other accounts that had been opened by his “subordinates” in The United States.

• Cyber-extortion: When a website, e-mail server, or computer system is hacked and denied of service by shutting down their system. These hackers sometimes request money in return for promising to stop the attacks, or sometimes just want to cause chaos or impairment in operation. An example of cyber-extortion was the attack on Sony Pictures of 2014. On November 24, 2014 a group of hackers who named themselves “Guardians of Peace” hacked into classified data that belonged to the film studio of Sony Picture Entertainment in order to get their attention. The data included all personal information of the employees and their families, the executives’ salaries and unreleased films. After leaking the data, the hackers then demanded that the movie “The Interview” cease to be release in theaters. The movie talks about the North Korean leader Kim Jong-un; this is why the hackers even threatened to carry out terrorist attacks in the movie theaters if the movie was to be released. After tracking the source of the hack, the US government was able to detect the source coming from North Korea. After informing the North Korean government of the source of the hack, the Korean government denied any accusations, thus leaving the company no choice but to stream the movie online to avoid any attacks.([[5]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn5%22%20%5Co%20%22))

•Dissemination of Offensive Materials and Cyber Blackmail: When someone hacks into the private files of their victims and posts their private information such as pictures, phone numbers, emails, bank account numbers…online, or threaten to post them in exchange for what they desire. In one case, a man allegedly stole nude photographs of his former girlfriend and her new boyfriend and posted them on the Internet, along with her name, address and telephone number. The woman was later harassed by people from all over the world and wasn’t able to do anything because the information had already been posted online. In England, the CEO of a financial institution was reported to have paid between 1993 and 1995 a total of $85,000,000, who was threatened by the extortionists to release a video of him having sexual relations with a minor.

• Theft of Services: Theft of service takes place when the hacker gains access to an organization’s services such as telecommunication services, either by hacking into the switchboard or by impersonating an employee or recreating a fake employee ID card, and abusing their access to gain free services.  This could also include violation of copyrights and uploading pirated material online. In United States; computer hackers had illegally obtained access to Scotland Yard's telephone network and made $1,240,000,000 worth of international calls for which Scotland Yard was responsible.

• Feed Hacking: When someone hacks into the camera of their victim’s computers, phones, security systems… to spy or obtain information.

• Command Hacking: Command hacking is the act of hacking into electronic devices such as microwaves, electronic dolls, electric ovens and so on, and controls them, to cause fear, manipulation, and in some cases fire. The problem here is that modern appliances are increasingly connected to the Internet, causing a new pool of devices hackers can choose from.

• Cyber terrorism: Cyber terrorism is stemmed from political motives and triggers individuals to use computers and information technology to cause severe disruption or widespread fear. Even a simple video like the one ISIS sends about their executions, can be considered as cyber-terrorism. The criminals usually hack government websites, military websites or circulate propaganda.

These hackers can be terrorist outfits or enemy governments of other nations. Cyber terrorism can also include hacking activities directed towards individuals, families, and organized by groups within networks, to cause them fear, demonstrate power, collect information, robberies, blackmailing and so on…

**B: Child soliciting and Abuse:**

This occurs when criminals solicit and manipulate minors via chat rooms for the purpose of obtaining media files used later on for pornographic purposes. Sometimes criminals gain the trust of these children and ask to meet them in real life, and once they do, they end up abducting them.

**C: Trafficking:**

While browsing the dark web, one can find markets for many illegal offline “products” that can be obtained through the click of a button without the risk of getting caught. Even though the delivery of the products can be tricky, since the process shifts from online to offline, the whole operation’s risk has been reduced by 50%. Trafficking includes:

• Drug Trafficking

• Human Trafficking:

• Organ Trafficking

Sometimes people meet the traffickers online and are asked to meet offline. Once offline meeting occurs, the victims are abducted and sold, either for the organ black market, or for prostitution.

**D: Cyber Stalking:**

Cyber-stalking is the use of the Internet or other electronic means to stalk an individual, a group of individuals, or an organization. It may include false accusations, making threats, damage to data or equipment, or gathering information in order to harass the targeted victim. The definition of "harassment" must meet the criterion that a reasonable person, in possession of similar information, would regard it as sufficient to cause another reasonable person distress. Cyber stalking is different from physical stalking. However, it sometimes leads to it, or is accompanied by it. In extreme cases cyber stalking could lead to murder.

**E**: **Cyber**-**bullying**:

Cyber-bullying is when all kinds of media devices are used post certain content online for the sole purpose of hurting or embarrassing another person. Cyber-bullying can be as simple as constant contact with a person (ex: send an e-mail) who has said they want no further contact with the sender, or it may also include sexual remarks, threats, harassment, pejorative labels , making someone the subject of ridicule in forums, and posting false statements that aims to humiliate an individual. In extreme cases cyber bullying could lead to suicide.

**F: Copyright Theft and Piracy:**

This crime occurs when a person infringes on copyrights and downloads music, movies, games and software, either for personal purpose, for sale at a lower price, or for free distribution. Due to this, piracy has caused substantial concern to owners of copyrighted material, and billions of dollars are being. For example: certain movies are being released online before their official release causing a strain on the directors and producers who have invested time and money on the production. However, today, the justice system provides laws that prevent people from illegal downloading.

According to the most common reports or complaints to Inter-GOV of computer crime, here are the types of computer crime that seem to occur most often: ([[6]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn6%22%20%5Co%20%22))

|  |  |  |
| --- | --- | --- |
| **1** | Child pornography | 35% |
| **2** | Fraud (scams) | 33% |
| **3** | e-mail abuse | 12% |
| **4** | Missing Children | 9% |
| **5 - 10** | Stalking,Copyright Violations,Harassment/Threats,Children (Abused),Hacking/Viruses,Other" | (Remaining 11%) |

**Categorization of Cyber Crimes**

Due to the many controversies that follow defining the term cyber law, the better approach to understanding this concept is if one categorizes the types of crimes. Despite the fact that computer crimes encompass a broad range of activities, it can still be categorized in a structuralized manner. Even though each category can use a variety of methods and the methods used vary from one criminal to another, and many scholars have categorized the crimes in different ways and have approached this concept from various prospectives, the best way to start is with the general categorization and then move to the more specified ones.

When one looks at the emerging list of cybercrimes they notice that it comprises of crimes that have been made possible by computers, such as the interference in a network and the distribution and dispersal of computer viruses, and it also includes crimes that are computer-based variations of preexisting crimes, such as identity theft, stalking, bullying and terrorism. All these crimes can be committed through hacking, personal contact in communication-enabled applications or a combination of online and offline contact.

Cybercrimes can also be categorized as offences committed against individuals with the intention to harm them directly or indirectly. The computer itself may have been used for the crime, or the computer may have been the target. When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The dealt damage is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims that makes him harder to trace and arrest.

In Crimes where the computer is the target, usually these crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have, which explains how society and the world, in general, are unprepared to combat these crimes. There are numerous crimes of this nature committed daily on the internet. Crimes that primarily target computer networks or devices include:

• Denial-of-service attacks

• Computer viruses

• Malware

The third way to categorize these crimes is to label them according to motives such as:

• Crimes committed for financial purposes (ex: hacking into a bank account)

• Crimes committed that stem from emotional reasons (ex: cyber-stalking)

• Crimes motivated by sexual impulses (ex: pedophilia)

•Politically motivated crimes (ex: cyber-terrorists)

• Crimes which are less dangerous in nature such as sharing copyrighted movies, software by individuals and others…([[7]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn7%22%20%5Co%20%22))

The crimes, according to the targeted victims, can be also categorized, where targeting involves:

•An Individual ( Ex: Cyber Stalking)

•Property i.e. individual, organization, and society/nation. (Hacking into a company’s data base)

•The Government (Ex: Cyber terrorism)

**Cybercrimes and International Organizations**

From a legal perspective, the following conventions have tackled the issue of cybercrime, where the UN has a draft a treaty on an International Court or Tribunal for cyber space. The convention will take place in Mumbai in November 2016.  In the draft the treaty mentions who has jurisdiction over internet crimes, and who is considered a cybercriminal and thus must be liable to punishment. The Council of Europe Convention on Cybercrime (2001) states types of cybercrimes, and declares that any person liable to these actions is sanctioned through deprivation of liberty, however to what extent, is not mentioned. The CECC has met every year since and added more definitions to what is considered as cybercrimes. The League of Arab States Convention on Combating Information Technology Offences states that each member state of the convention should be committed to fulfill its obligations arising from the convention, however without the interference of other states’ interior affairs. The convention also clearly stated that no state judicial is entitled to jurisdiction on other states, and that every state should respect the sovereignty of other states. Moreover, the Convention also endows with the imposition of sanctions on the following crimes: entry i.e. hacking, interference with the private lives, withholding some information, amendment, mail fraud, or posting obscene material. The Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information (2007) define the type of criminal acts, who are the competent authorities, forms of cooperation to combat cybercrime, and how to request their assistance in case of being victimized. The Shanghai Cooperation Organization Agreement in the Field of International Information Security (2008-2012) states that the members are: “firmly convinced that terrorism, separatism and extremism, as defined in this Convention, regardless of their motives, cannot be justified under any circumstances, and that the perpetrators of such acts should be prosecuted under the law.([[8]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn8%22%20%5Co%20%22))” The African Union Convention on Cyber Security and Personal Data Protection (June 27, 2014) states the online activities should be exercised freely except:

a) Gambling, even in the form of legally authorized betting and lotteries;

b) Legal representation and assistance activities;

c) Activities exercised by notaries or equivalent authorities in application of extant texts.([[9]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn9%22%20%5Co%20%22))

**Scholars and Cybercrimes**

Many Scholars have written about cybercrimes, but have approached the problem in many ways. Due to the different types of cybercrimes, some scholars focused on categorizing them and others focused on specific types of crimes. Burden, Kit stated that there are two types of cybercrimes, the ones that are “e-enabled”, meaning crimes that were known to the world before the internet, but are facilitated through the World Wide Web, and “true” cybercrimes, meaning crimes that would not exist outside the online environment. ([[10]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn10%22%20%5Co%20%22))

**The** **Cyber-Criminal**

Understanding the behavioral analysis of the criminal:

For some time now, forensic psychologists and behavioral scientists have been working in collaboration with law enforcement agencies to incorporate psychological science into criminal profiling. But what is criminal profiling?

Criminal profiling seeks to identify criminals by analyzing their behavior after they have engaged in a crime. The fundamental rational is simple: If certain behavior and evidence in a crime are found to be in common with other crimes, then there is a big probability that it is the same criminal activity because behavior is related to the psycho-socio characteristics of an offender.

Behavior is shaped by the choices criminals make while committing a crime. This could include the method of the crime, the location of the crime, and the choice of the targeted victims i.e. victimology, and so on... This data is then combined with physical evidence collected from the scene of the crime. Once the data has been collected, it is then compared with the characteristics of recognized personality types and mental abnormalities. This process later develops a practical working description of an offender, for example when a baby is kidnapped, but a body has not been found, it usually signifies that the kidnapper may be a female between the age of 30 and 40 who had recently lost a child of her own. The lack of body signifies that the baby will substituted for the “lost baby” of the kidnapper. If the baby was a child or if the baby was murdered then the whole profile would be completely different.

Criminal profiling emerged as a new tool for investigation at the beginning of the 20th century, starting with the case of the infamous Jack, the Ripper killings in England. However it has only been recent that this science has caught the eye of the public, after TV shows such as CSI, Criminals minds, the Mentalist, Lie to me and so on included studying the mind of the killer in their plot.

However, what can profiling contribute to when dealing with cybercrimes? Research has proved that criminal profiling is estimated to have a success rate of 83 percent when assisting traditional investigations. Moreover, due to the fact that cybercrime is a new unpaved addition to the “new world”, officials would seek all the help they can get in order to catch the invisible criminal, especially when physical evidence is lacking in a cybercrime. The world of cybercrime restructures the rules of criminal investigation. Unlike traditional crime scenes, the evidence found mostly exists only in the cyber-world; in a network, computer, or the Internet. Moreover, it is this faceless aspect of cybercrime that compiles its challenge. However, if cyber criminals depend on the pseudo-anonymous nature of the Internet and need this technology to camouflage their true identities, then it is up to security leaders to use this to their advantage. Fortunately, a cyber criminal's facelessness is considered as a signature behavior, a motivation, and an MO (modus operandi). Criminal profiling relies heavily on such clues because not all cyber criminals have the same maturity in technique, behavior, characteristics and motives, making every cybercrime unique. This means that hackers are not the same as traffickers, furthermore hackers also aren’t all the same.

The following figure represents a 4 step process of induction of evidence investigators must follow in order to deduce the profile of the criminal.([[11]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn11%22%20%5Co%20%22))



It is important to remember that cyber criminals are highly stereotyped, and one must not fall into this trap when profiling. Some of those stereotypes propose that cyber criminals have an above average IQ, possess advanced technical and problem solving skills; they feel dissatisfied and de-motivated by unchallenging surroundings at school or work. They are introverts suffering from social cues and relationships, and are scared of personal confrontation especially with the authority.

Part of the reason in finding such stereotypes is because most of the research on that subject has been done on hackers. This is the case because most behavior analysts think that hacking is a “true” cybercrime while other crimes are regular crimes facilitated by computer technology. Therefore, cyber criminals who do not fall in the hacking category have similar traits to criminals who do similar crimes in the “real world”; however, they only found a new and easier way to commit these crimes making them “developed” 21st century criminals.

Many reports on cyber hackers suggest that these hackers favor the structure of computer technology and its predictability to the dynamics and complexity of social relationships. This is why they spend excessive time online, losing sense of time to the point that their on-line activities interfere extensively with their personal lives. They are more likely to be independent, self-motivated, antagonistic loners, who can’t work in teams. Other reports go as far as linking cybercrime behavior to psychological disorders. For example, the infamous hackers Adrian Lamo and Ryan Cleary were reported to have suffered from Asperger's ([[12]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn12%22%20%5Co%20%22)), which is a form of autism and development disorder characterized by notable difficulties in social interaction. In addition to these psychological disorders most cyber criminals have mixed senses of loyalty and entitlement, as well as lack of empathy.

Nonetheless, even hackers don’t all have the same profile; one must look into their crimes, and base the profile according to the hacking expertise. Marcus Rogers is a cyber-forensics researcher and an associate professor at Purdue University in West Lafayette, Indiana. He believes that the hacking community is a diverse and complex universe, consisting of various skill layers and motivations.([[13]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn13%22%20%5Co%20%22)) By understanding the diverse types of hackers and what motivates their behavior, it is possible to profile the hacker, making it easier to forecast and calculate future activity. Thus, Rogers identified eight types of hackers, classifying them by their skill levels and motivations.([[14]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn14%22%20%5Co%20%22))

The categories range from script kiddies (diminutively skilled hackers, who use pre-fabricated and pre-coded software and depend on “how to” documents and videos downloaded from the Internet, aren’t motivated by any meticulous factor, but rather seek out easy targets in order to get recognition, and tend to seek attention or recognition for their hacks often by telling the Elite (hackers who have the knowledge, proficiency and skill of the highest level while still maintaining ethical integrity. It is agreed upon that elite hackers do not take on any criminal activity or enclose malicious intent; but rather alert systems administrators and expose their security flaws and other coding problems to allow them to enhance the system and avoid problems).Cyber terrorists, in contrast, master the state of the art gear and are capable of writing very complex and sometimes untraceable codes.([[15]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn15%22%20%5Co%20%22))

**Understanding the difference between the diverse Types of Hackers**

If one wants to include other scholar’s categorization of hackers and their skill levels, the list would go on. That is why MacAfee labels two main categories for hackers: the Black Hats and the White Hats. Since then a new category has been added called the Gray Hats for those hackers, in between. The main aspect that separates the Black Hats from the White Hats and Gray Hats is the intent.([[16]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn16%22%20%5Co%20%22))

**White Hat Hackers:**

A white hat hacker, also known as an ethical hacker is, in the computer world, a person who is ethically opposed to the exploitation of computer systems. A white hat mainly focuses on securing IT systems and fixing them.

The term white hat hacker is usually used to illustrate those who aim to break into systems or networks in order to alert the owners of the system of their security flaws, or to execute some other altruistic action. White hat hackers as a result, are sometimes called “sneakers or tiger teams” when found in teams.

**Grey Hat Hackers**:

A Grey Hat in the online community describes someone's activities that cross between black and white making them hybrids. One reason, grey hats might identify themselves as such to disaffiliate from the other two extremes: black and white. Some people use the term brown hat; however grey hat is a more popular one. These hackers usually do not have malevolent intentions, but may or may not sporadically commit crimes during the course of their technological development. It might be a little delusive to say that grey hat hackers do not hack for personal gain, for all hackers have their reasons. Their intent might not be malicious however they aren’t for the greater good either. Moreover, a grey hat will not notify the system admin of a glitch in their system due to the fact that such a hacker usually prefers anonymity at almost all cost, carrying out their hack with minimal damages.

“War-gaming” is also classified as grey hat hacking, which is a cyber-security challenge and mental sport where the competitors must have several tasks and are asked to either protect or abuse a computer system, similar to the “catch the flag” game in real life.

**Black Hat Hackers:**

A black hat is a person who jeopardizes the security of a computer system without consent from an authorized authority, usually having malicious intent. Generally, a black hat is a person who uses the knowledge of vulnerabilities and takes advantage of the skills for private gain, rather than informing either the general public or the manufacturer for rectification. Many black hats hack networks and web pages solely for financial gain, and in extreme cases they hack for blackmail, threats, extortion, or political and military purposes.

**Understanding the Role of the Victim in the Crime**

In cybercrimes, one wonders what role the victim plays during the crime. Does the victim take full precautions or are they unconsciously helping the criminal through irresponsibility, recklessness or lack of awareness. For example, many receive, or have received emails that claim a distant relative had passed away and left major funds of millions of dollars without any one to inherit this fortune. All what the intended victim is required to do is send their bank’s name and account information. At some point they even ask to send a certain fee for the “barrister” who would legalize all documents. While many are aware of never sending these kinds of information to an unknown entity, and that such emails sound sketchy and most probably scams, other people might fall into this trap.

In this case, the victim played a huge role in the crime, where in the real world this would be similar to handing out, to a stranger in a dark alley who claims wanting to give some  money,  the key to a safe. The law does not protect the ignorant and the duped. However, there are certain steps and precautions one must take in order to avoid falling into traps. Also, there are other things that are just out of people’s hands for example buying a product that had been hacked during manufacturing.

This is a list of examples when something most likely constitutes a scam:

• It looks or sounds too good to be true.

• You receive an email claiming you won or are inheriting money.

• You are asked for your account information to wire money instead of sending a check to an “offline” address or using a certified online payment method.

• The person you are dealing with is out of the country and needs some sort of donation or form of payment.

• You are purchasing an item from a seller who claims to be in a different location from the item they are selling.

• When you are selling something online and a buyer wants to send you a check for more than the asked price of the item; then you cash the check and wire the extra money back.

• Any job that claims you can become rich where you have to cash checks or “reship” items.

• You receive an email from your bank, university, finance department of your job… asking for any login info, bank account info, or personal info.

• When you receive unsolicited offers.

• When you put in your credit card information on a website that isn’t verified (the URL would generally be green and a lock would appear if the website is verified)

• When using free Wi-Fi in a public place and do not take security measures.

• When they offer you a highly paying job as CEO or general Manager, and others

In general, people should be as cautious online with their information as they are offline. Not only should the individuals take safety measures for themselves, but also monitor the children’s (if any), online activities and make sure they aren’t talking to strangers or making any online payments and transactions. Moreover, schools should educate the children on the dangers of chatting with strangers and the general dangers of the internet that could lead to kidnapping, suicide, and all forms of trafficking to name a few.

Ignorance is not bliss when it comes to the internet, and nothing should be taken lightly. Just because the activities are occurring behind the screen does not mean it won’t hurt offline in the real world.  One ought to avoid posting unnecessary amount of personal photos and information; privacy is a fundamental human right ([[17]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn17%22%20%5Co%20%22)). Abusing this right will bring up unwanted attention and end up turning the individual into an easy and predictable target.

**Understanding the rights of the victim**

Committing crimes online facilitates anonymity of identity and location. Moreover, as mentioned above, due to lack of territory and ease of access, one can commit a cybercrime thousands of miles away. This makes it easier for the criminal to commit crimes but harder for police and other law enforcement organizations to bring them to justice.

What makes cybercrime an even bigger opportunity for a criminal is the fact that law enforcement agencies seldom have qualified agents that can deal with the issue, consequently considering cybercrime the least of their priorities.

Furthermore, if, by any chance the offender was identified and arrested, then the criminal will be taken to court. Compensation and justice however, will depend on the role the victim played in the crime and how ignorant they were.

**International Laws and Cybercrimes**

When one looks at existing international laws that could contribute to the international affairs of cyber law we can take Article 1 of the United Nations Code of Conduct for Law Enforcement Officials([[18]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn18%22%20%5Co%20%22)) that clarifies that the responsibility of law enforcement is to execute the duty forced upon them by law, “by serving the community” and “by defending all persons from illicit acts.”

This duty is extended to the complete range of prohibitions under penal statutes([[19]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn19%22%20%5Co%20%22)). However, as cybercrime acts grow to be more common and widespread, law-enforcement agencies progressively face the question of what “serving” and “protecting” in the perspective of a crime within global dimensions really means.

A study done by the United Nations Office of Drugs and Crimes reported that more than half of the world’s countries testified that between fifty and one-hundred percent of cybercrime acts faced by the police involve an international element.([[20]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn20%22%20%5Co%20%22))

Thus, responding countries pointed out that the majority of cybercrime acts are discovered by the police through individual victim reports.

Therefore, the UNODC came to the conclusion that cybercrimes generally transpire globally, but are reported locally. Here, one finds the need for collaboration between nation states in order to avoid jurisdiction problems. Cyberattacks are becoming highly developed and more difficult to discover especially when new techniques promptly find their way to a broader audience. There are certain International Organizations that have started to tackle the issue of cybercrimes. Starting from 2005 when the “Electronic Transaction and Information Law” was presented to the Law House in Indonesia in July, and when the “Council of Europe Convention on Cybercrime” was ratified in Norway on the 4th of November, when the State Senate in the Netherlands formed a committee that introduced a proposal for legislation on Computer crime on the 20th of December, and when the “Computer security and Critical information  in Infrastructure Protection Bill 2005 (Sb254)” was introduced to the National Assembly in Nigeria on the 22nd of December. Up to this day when in November 2016 an International Convention on Cyber Crimes will take place in Mumbai India that will try to establish an international unified cyber law.

When one looks at the International Organizations and their significance, one must look at whether they are binding on states or none-binding. Almost half are non-binding.([[21]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn21%22%20%5Co%20%22))

For binding mechanisms, the geographic scope is usually determined by the nature and framework of the organization. Hence, for instance, the League of Arab States Convention‘s main principle is “to strengthen and improve cooperation between the Arab States.” ([[22]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn22%22%20%5Co%20%22))

Likewise, the “Commonwealth of Independent States Agreement” that abolished the USSR, labels “the members” as “Independent States,”([[23]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn23%22%20%5Co%20%22)) and the Draft African Union Convention is foreseen to be open to “Member States of the African Union.”([[24]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn24%22%20%5Co%20%22))

However, not all members of the organization may be participants to the original agreement([[25]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn25%22%20%5Co%20%22)) and –where the agreement is prone to ratification, approval, or acceptance([[26]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn26%22%20%5Co%20%22))– not all participants may have accepted such changes or agreements([[27]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn27%22%20%5Co%20%22)). Some ratifications, additions and changes are opened for signature external of the membership of the organization where this “additional belief” was developed. For example, The Council of Europe Cybercrime Convention was open for membership by states of the Council of Europe AND by “non-member States which have contributed in its expansion.” Founding states become the current states that have power over the entry of new states applying for membership, usually with accordance to the rules that were set in the “original” treaty agreement. ([[28]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn28%22%20%5Co%20%22))

Treaties may be one of three things when it comes to its recruitment policies. It is “open” when any state may become a member by simply articulating their intent to join and follow the presented treaty terms. It is “semi-open” when membership is approved by a majority vote from the contracting states. And finally it is considered as “closed” when membership requires a unanimous vote from the contracting states.([[29]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn29%22%20%5Co%20%22))

An example of a closed membership is the Council of Europe Cybercrime Convention, where after the Committee of Ministers of the Council of Europe consult with the contracting states of the Convention and obtain their unanimous consent, may they “invite any State that is not a member of the Council and has not participated in its foundation and expansion.([[30]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn30%22%20%5Co%20%22))” Similarly, the Common wealth of Independent States Agreement is “open for membership by any other State prepared to be bound by the requirements, only after all Parties agree. ([[31]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn31%22%20%5Co%20%22))” On the other hand, The Shanghai Cooperation Organization Agreement is said to be “open to membership by any State that believes in the same principles and goals of the Agreement.” ([[32]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn32%22%20%5Co%20%22))

Organizations and Treaties developed under the “sponsorship” of the United Nations usually have the broadest geographical scope. The Convention on Law of the Sea is open for “membership by any State.” ([[33]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn33%22%20%5Co%20%22))

Globally, 82 countries have ratified and/or signed 1 of the binding cybercrime organizations,([[34]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn34%22%20%5Co%20%22)) and some countries have signed and became members of more than one organization.

Even though there is a possibility of joining more than one international organization that contributes to dealing with cybercrimes, facts point out that even till this day no single IO has a global geographic reach of membership. The Council of Europe([[35]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn35%22%20%5Co%20%22)) Cybercrime Convention has the leading number of signatures/ memberships with 43 member-states, and 5 Non-member States of the Council of Europe.The League of Arab States Convention has 18 countries/members, the Commonwealth of Independent States Agreement has10 countries/members, and the Shanghai Cooperation Organization Agreement has 6 countries/members.

If the Draft African Union Convention were to be signed by all member states of the African Union, it could have up to 54 countries/members. The main question would remain: Once a unified law is fully established will the member states implement it? What is de-motivating from past events is that none of the international organizations that have already been established have taken full effect. The cyber world is witnessing an increase in cybercrimes over the past years instead of solutions for them. What attributes to these results is the fact that the majority of states haven’t made cybercrimes a priority in their crime departments.  Moreover, trying to catch a cybercriminal can sometimes feel like chasing after a ghost. What good do any rights and laws do for the individual if they can’t be exercised properly when another individual oversteps on them.

**Human Rights and Cyber Crimes**

Human Rights in the digital age has posed many controversial issues and the dilemma of being put under the position of choosing which human right/law is more appropriate to apply when dealing with the internet. Considering both article 3 and article 12 from the Universal Declaration of Human Rights, as they respectively declare: “Everyone has the right to life, liberty and security of person”([[36]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn36%22%20%5Co%20%22)), and “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”([[37]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn37%22%20%5Co%20%22))

One notices that the progress in information communication technology is facilitating access to information altering these technologies in the process of becoming very susceptible for interception. What is even more frightening are the new recent discoveries that have exposed how new technologies are being secretly developed to facilitate these practices, with high efficiency.

Using this as an excuse, it is no longer a secret that the government has been keeping tabs on citizens’ private information whether it is from phone calls or search history from explored engines such as Yahoo and Google, to “protect”.

This is why in December 2013, the United Nations General Assembly executed resolution 68/167, which articulates deep concern at the negative impact the interception and surveillance of the citizen’s communication and online activities may have on human rights. The General Assembly came to the imperative realization that the rights people practice offline must also be protected online; and it is the States’ responsibility to impose the respect and protection of the right to privacy in digital communication. That is why the General Assembly called on all States to inspect their procedures, legislation and practices related to communications inception, collection, and surveillance. It stressed the need for States to guarantee the complete and effective implementation of their obligations to adopt and implement the international human rights law. A year later, on the 13th of November 2014, at its 27th session, the Human Rights Council assembled a panel to discuss the right to privacy in the “digital age” tackling the subject of surveillance. ([[38]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn38%22%20%5Co%20%22))

The report was then presented to the General Assembly at its sixty-ninth session. One month later, in December 2014, Resolution 69/166([[39]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn39%22%20%5Co%20%22)) was adopted, and the General Assembly encouraged the Human Rights Council to deem the possibility of establishing a special procedure to promote this aim.

In April 2015, the Human Rights Council executed resolution 28/16 at its twenty-eighth session, and decided to assign a Special Reporter, for a period of three years, on the right to privacy ([[40]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_edn40%22%20%5Co%20%22)). The resolution assigned the Special Reporter, along with other responsibilities, to report on suspected violations of the right to privacy that are connected to the challenges cropping up from new technologies. States were obliged to fully cooperate and support the Special Reporter.

**Economic Impact of Cybercrimes**

Putting a number on the cost of cybercrime, and cyber is the tip of the iceberg, but the body of that iceberg is the effect on competitiveness, technology, trade, and trust.

While the cost of cybercrime to the global economy is an average of 400 billion dollars every year, the dollar amount, as much as it may seem, may not fully reveal the real damage done to the global economy. Cybercrime also slows the rate of innovation, disrupt trade, and create social costs from job loss. This larger effect could be more significant than any actual number.

**Conclusion**

First one needs to acknowledge the weakness in the definition of cybercrimes, due to the fact that there still does not exist a uniform understanding of the act. The best definition would be the one that factors in not only the crime, but the criminal’s intention and the victim. Therefore, cybercrime can be best described as the act of intentionally harming an individual without their consent through the means of information and communication technologies.

As the world evolves, so will all its aspects: the good and the bad. That being said, one must not forget to “modify” the definition of crime, meaning that the face of crime has evolved. Megabytes are substituting for bullets and the scary part is that no weapon can fight this ongoing battle except for the weapon of knowledge and cooperation.

How can one combat the threat of cybercrime? Before tackling the issue on an international level and point out the importance of establishing a conventional relationship between states, there are critical elements every state should adopt in itself first, that will improve domestic law enforcement response to reported acts of cybercrime.

These elements include:

• Establishing a successful legal framework that allows investigative measures to reach the proper balance between  the respect for personal privacy and investigative authority;

• Sufficient access to un-intrusive investigative tools and inquiry methods during investigation, such as obtaining electronic evidence from third parties like internet service providers, to trace activity and not content.

• Adequate training and technical capability for both specialized and non-specialized law enforcement agents.

• Providing training workshops in schools, universities, banks, companies, and relevant work fields that raise awareness on cybercrimes.

• Introduce the “Hack for Good Program”, in which law enforcement agencies hire the hackers they arrest in exchange for exemption of imprisonment to help them catch cybercriminals. In other words, using “criminals to catch criminals”.

However, implementing these security measures and elements is difficult and could take time to master. This is why governments need to use what they have as domestic criminal laws as a base to build upon new laws for cybercrimes. Moreover, definitions for certain criminal acts must be ratified and updated in order to fit the new reality.

[[1]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref1%22%20%5Co%20%22) Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies - June 2015 McAfee.

[[2]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref2%22%20%5Co%20%22) Campbell, Q., & Kennedy, D.M. (2009). Chapter 12: The psychology of computer criminals. In Bosworth, et al (Eds.), Computer security handbook. New York, NY: John Wiley &Sons, Inc.

[[3]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref3%22%20%5Co%20%22) https://www.justice.gov/criminal-ccips

[[4]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref4%22%20%5Co%20%22) See American Civil Liberties Union (ACLU) report of 2008

[[5]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref5%22%20%5Co%20%22) Hacking” page 7 By Walter Spivak  (2012)

[[6]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref6%22%20%5Co%20%22) -"The National Information Infrastructure Protection Act of 1996 Legislative Analysis. “Department of Justice Computer Crime and Intellectual Property Section. Internet. URL: http://www.usdoj.gov/criminal/cybercrime/1030\_anal.html.

[[7]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref7%22%20%5Co%20%22) Shinder, D. (2010) Profiling and categorizing cybercriminals. [online] http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069

[[8]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref8%22%20%5Co%20%22) The Shanghai Cooperation Organization Agreement in the Field of International Information Security (2008-2012) – Also see http://www.cybercrimelaw.net/SCO.html

[[9]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref9%22%20%5Co%20%22) See “The African Union Convention on Cyber Security and Personal Data Protection (June 27, 2014)”

[[10]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref10%22%20%5Co%20%22) Computer Law and Security Report May 2003

[[11]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref11%22%20%5Co%20%22) FBI records in the Vault: Criminal Profiling

[[12]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref12%22%20%5Co%20%22) American Computer Criminals: Adrian Lamo, Kevin Mitnick, Mark Abene, Bradley Willman, Larry Mendte, Ytcracker, Robert Soloway, Chad Davis, Author: Books Llc, Editor: Books Llc Publisher: General Books, 2010

[[13]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref13%22%20%5Co%20%22) xiii- Conflict and Cooperation in Cyberspace: The Challenge to National Security page 46

[[14]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref14%22%20%5Co%20%22) Global Information Assurance Certification Paper, Crime and Punishment: The Psychology of Hacking in the New Millennium

[[15]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref15%22%20%5Co%20%22) Crime and Punishment: The Psychology of Hacking in the New Millennium, Global Information Assurance Certification Paper, page 6

[[16]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref16%22%20%5Co%20%22) “Duelling Unicorns: Crowd Strike vs. Cylance in Brutal Battle to Knock Hackers Out.” Forbes Magazine, July 26, 2016 issue.

[[17]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref17%22%20%5Co%20%22) See Universal Declaration of Human Rights

[[18]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref18%22%20%5Co%20%22) See Article 1 of the United Nations Code of Conduct for Law Enforcement Officials

[[19]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref19%22%20%5Co%20%22) See Penal Statues of the United Nations Code of Conduct for Law Enforcement Officials Ibid, Commentary to Art 1(d).

[[20]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref20%22%20%5Co%20%22) Study cybercrime questionnaire. Comprehensive Study on Cybercrime Draft—February 2015 by UNODC (United Nations Office on Drugs and Crimes)

[[21]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref21%22%20%5Co%20%22) Study cybercrime questionnaire. Page 145 Comprehensive Study on Cybercrime Draft—February 2015 by UNODC (United Nations Office on Drugs and Crimes)

[[22]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref22%22%20%5Co%20%22) League of Arab States Convention, Article 1.

[[23]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref23%22%20%5Co%20%22) Commonwealth of Independent States Agreement. Preamble

[[24]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref24%22%20%5Co%20%22) Draft African Union Convention. Part IV, Section 2, Art. IV-2.

[[25]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref25%22%20%5Co%20%22) League of Arab States members Comoros, Djibouti, Lebanon, and Somalia have not signed the League of Arab States Convention. Council of Europe member states Andorra, Monaco, the Russian Federation, and San Marino have not signed the Council of Europe Cybercrime Convention.

[[26]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref26%22%20%5Co%20%22) For a review of international law of treaties in general see Shaw, M.N., 2007. International Law. 6th ed. Cambridge: Cambridge University Press.

[[27]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref27%22%20%5Co%20%22) Council of Europe Cybercrime Convention signatories Czech Republic, Greece, Ireland, Liechtenstein, Luxembourg, Poland,

Sweden and Turkey have not yet deposited instruments of ratification, acceptance or approval.

[[28]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref28%22%20%5Co%20%22) See Article 15 of the Vienna Convention on the Law of Treaties

[[29]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref29%22%20%5Co%20%22) Malone, L.A., 2008. “International Law”, New York: Aspen

[[30]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref30%22%20%5Co%20%22) “Council of Europe Cybercrime Convention”, Article 37(1). Proposals for amendment of the procedure followed under Article 37(1) have been made by the Council of Europe Cybercrime Convention Committee (T-CY) and the European Committee on Crime Problems (CDPC). Both proposals are currently under review by the Council of Europe Rapporteur Group on Legal Co-operation (GR-J). See Council of Europe Cybercrime Convention Committee 2012. Criteria and Procedures for Accession to the Budapest Convention on Cybercrime – Update. T-CY (2012)12 E. 28 May 2012.

[[31]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref31%22%20%5Co%20%22) Commonwealth of Independent States Agreement, Art. 17.

[[32]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref32%22%20%5Co%20%22) Shanghai Cooperation Organization Agreement, Art. 12.

[[33]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref33%22%20%5Co%20%22) “United Nations Convention on Law of the Sea”, Article 48; and United Nations OP-CRC-SC, Art. 13. ‘State’ has a broad meaning in this content and is not limited to Member States of the United Nations.

[[34]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref34%22%20%5Co%20%22) Signature or ratification of: Council of Europe Cybercrime Convention, League of Arab States Convention, Commonwealth of Independent States Agreement, and Shanghai Cooperation Organization Agreement.

[[35]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref35%22%20%5Co%20%22) In addition, a further eight countries (Argentina, Chile, Costa Rica, Dominican Republic, Mexico, Panama, Philippines, and Senegal) have been invited to accede to the Council of Europe Convention in accordance with the provisions of Article 37. Accession of these countries to the Convention would significantly expand its geographic scope.

[[36]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref36%22%20%5Co%20%22) See Article 3 in the Universal Declaration of Human Rights

[[37]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref37%22%20%5Co%20%22) - See Article 12 in the Universal Declaration of Human Rights

[[38]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref38%22%20%5Co%20%22) See GE.14 Human Rights Council Twenty seventh session Agenda items 2 and 3Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary General Promotion and protection of all human rights, civil,  political, economic, social and cultural rights, including the right to development- The right to privacy in the digital age

[[39]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref39%22%20%5Co%20%22) See A/RES/69/166 C.3 68 (b) A/69/PV.73 18 December 2014 GA/11604 without a vote A/69/488/Add.2 DR I “The right to privacy in the digital age”

Also see http://www.un.org/en/ga/69/resolutions.shtml

[[40]](https://www.lebarmy.gov.lb/en/content/cybercrime-and-cyber-laws-international-dimension%22%20%5Cl%20%22_ednref40%22%20%5Co%20%22) See United Nations Humans Rights Council Resolutions 28/16 The right to privacy in the digital age 3 A/HRC/28/L.27 Adopted without a vote, 56th meeting, 26 March 2015

Also see http://www.un.org/en/ga/69/resolutions.shtml

**الجرائم والقوانين السيبرانية: البُعد الدولي**

ليست الجرائم السيبرانية بالضرورة جديدةً مثل السرقة، والاحتيال، والإتجار، ولكنّها تتطوّر بطريقة يمكن فيها للمجرمين أن يختبئوا وراء الشاشة ويحصلوا على الفرص التي تستقرّ بين أحضانهم في غضون ثوانٍ، وبالتالي تصبح أكثر انتشارًا وتسبّبًا بالضرر. مع ذلك، ظهرت أنواع جديدة من الجرائم لا يمكن تواجدها من دون تكنولوجيا المعلومات والاتصالات، وهذا هو المكان الذي يواجه فيه القانون أرضًا لا تُمسّ.
وتُقدّر التكلفة السنوية المحتملة التي يتحمّلها الاقتصاد العالمي بسبب الجريمة السيبرانية بأكثر من 400 مليار دولار، حيث قد يبلغ أدنى تقدير 375 مليار دولار من الخسائر، بينما قد يصل الحدّ الأقصى إلى حدود 575 مليار دولار. في الماضي، كانت الجرائم السيبرانية تُرتكب بشكلٍ رئيسٍ على أيدي أفراد أو مجموعات صغيرة. مع ذلك، إنّنا نشهد اليوم بشكل مفرط شبكات مختلفة الجوانب من الجريمة الإلكترونية التي تتعاون في أنحاء العالم جميعًا، وهي قادرة على ارتكاب جرائم واسعة النطاق. وبالنظر إلى تطوّر شبكة الإنترنت، نلحظ أنّها تنمو بطريقة غير مبرّرة وغير منظّمة تمامًا، ما يسبّب المتاعب في عالم الانترنت وخارجه.
بالنسبة إلى معدّل نمو الفضاء السيبراني فقد أصبح هائلًا، وعدد سكّانه يتضاعف كل 100 يوم. ومع النمو العفوي وغير العادي تقريبًا للفضاء السيبراني، بدأت تظهر قضايا جديدة وحسّاسة تتعلّق بالجوانب القانونية المختلفة للفضاء الإلكتروني. وبالتالي، فبقدر سرعة تطوّر التكنولوجيا تقوم هذه الابتكارات بطرح المزيد من القضايا القانونية. وقد ولّد النمو السريع لشبكات تكنولوجيا المعلومات والاتصالات في الفضاء السيبراني فرصًا جديدةً تسمح للمجرمين بارتكاب الجرائم، واستغلال أوجه الضعف على الإنترنت، ومهاجمة الهياكل الأساسية للمعلومات البالغة الأهميّة في مختلف البلدان.