ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الثمانون
تاريخ الإصدار: 2 – حزيران – 2025م
www.ajsp.net

"Cyber financial crimes effects on civilians and the best ways to protect the cyber space from the human rights violations"

Dr. Ziad Zouheiry

International relation, CEDS (centre d'etudes diplomatiques et strategiques), Paris, France.

Oricd No: 0009-0004-1011-8931

https://doi.org/10.36571/ajsp802

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الثمانون
تاريخ الإصدار: 2 – حزيران – 2025م
www.ajsp.net

Abstract:

The cyber space is witnessing many kinds of crimes and cyber financial crime is one of them which is one of the most dangerous online crimes, as Each year thousands of people lose their money and sometime their life because of cyber financial crimes.

There are many genres of cyber financial crime as like Money laundering, online fraud auction, selling drugs and illegal substances, and the digital intellectual property theft and each type is a catastrophe by itself, for instance the money launderers are buying and selling in billions of dollars the cryptocurrencies to whitening their money, also people are defrauded yearly because of their participation in online fraud auction , as well the number of addicted teenagers are becoming larger because of the online websites in dark web which sell drugs and illegal issues, besides theft of online intellectual property is a major loss for the economy of the world.

Those cyber financial crimes are harming the people a lot and they are causing many human rights violations as a result of the complexity of applying the AML activities which are ineffective in reducing the number of cyber financial crimes, also the absence of legal frame work in cyber space makes the criminals more free to do whatever they want in cyber space and our methodology was based on the mixed methods in collecting the data from many reliable resources such as books and websites about cyber financial crimes and those resources were credible based on my criteria of credibility and they helped us a lot to reach that cyber governance with its attributes as the best solution for this problem and there must be an effective role for the UN in applying cyber governance, besides the cyber space must be considered as global common to enhance the legal framework of cyber space with more restrictions.

Keywords: cybercrimes impact, online human rights violations, cyber governance, cyber space, global common

A-Introduction:

cyber war is a new kind of war which is happening in cyberspace, and this space is supposed to be used for peaceful purposes such as exchanging information, communication, e-commerce and other useful things, according to Louise Shelley:" the spread of the internet was originally interpreted almost entirely as a force of good. The assumption that greater connectivity and greater access to information would lead to more prosperity and greater intercultural understanding was rarely questioned and is still implicit in the way we continue to think about digital transformation. Not enough serious attention is given to dark sides of the globalized digital economy." (Louise, 2018) also many countries consider now the cyber-attacks as a front-line force in their wars against each other and they can do their attacks anonymously with a great possibility to achieve their target, besides criminals found the cyber space an ideal location to make their crimes since there will be a great possibility to escape the punishment.

The cyber financial crime is the act of having financial gains through improper and criminal actions, and the number of cyber financial crimes are growing gradually because of the e-commerce which is booming and it is always in continuous growth as USA alone in 2024 has an e-commerce market with the amount of 1.2 Trillion US dollars followed by China with the amount of 1.1 Trillion US dollars (Statista Research Department, 2025).

The e-commerce is about online buying and selling process to all kinds of products including cryptocurrencies trading between business to consumer (B2C), consumer to business(C2B) and others, also the e-commerce provides the people with all the required financial services to complete the buying or selling transactions and those services are the online fund transfer, e-shopping cards, cryptocurrency payment and many other forms of payments.

All those financial services are exposing on daily basis to cyber-attacks because the hackers find them very profitable and according to the UK finance over $1.5 billion was the financial loss in 2022 equivalent to $ 2,300 per day (UK Finance, n.d.) as a result of cyber financial crimes.

Cyber criminals are using advanced tools in their cyber-attacks such as malwares which are very effective weapons in stealing money and personal information: "Malware attacks are any types of malicious software designed to cause harm or damage to a computer, server and clients." (Cyberark, n.d.)

There are two kinds of malwares which are used excessively in cyber financial crimes which are ransomware and spyware and the two have different uses, for instance the ransomware is sent to computers to encrypt their files and the criminals hold

the decryption key until a ransom is paid by the victims, Besides The ransomware attacks increase globally to 5,414 in 2024 and this is 11% increase compare to the 2023. (The Hindu Bureau, 2025)

furthermore, cyber criminals use a lot of the spywares in their attacks in order to collect credentials and passwords of the people and with this kind of malware the hackers can steal credit cards numbers, and in 2024 more than 1 billion records were stolen by spywares. (Krysinska, 2024)

The cyber financial crimes are becoming more sophisticated and the cybercriminals are expanding in their online fraud operations and meanwhile the cybercrimes are beyond the e-commerce and they reached the stage of manipulation to gain more money for that reason we found a variety of cyber financial crimes as like : money laundering, fraud auctions, Tax Misapplication, selling illegal stuffs, theft of intellectual property, and hacking the e-banking systems.

Internet has always been an attractive field for criminals to launder money or to practice illegal activities in order to make money and according to Fausto Martin De Sanctis:" The globalization of financial markets and the rapid development of information technology have gradually steered the underworld economy towards new possibilities for the commission of the crime." (Sanctris, 2019)

Every year millions of dollars are laundered in the world and referring to the United Nations report:" laundered funds globally are estimated to be between US 800 billion and US 2 trillion per year." (United Nations, n.d.)

Most of the digital money laundering are coming from cryptocurrency trading and the amount of laundered money is $ 8.6 Billion of cryptocurrency in 2021 (BBC, n.d.), the cryptocurrency is digital currency and you can easily buy it without any restrictions, besides the cyber criminals found the cryptocurrency as a great opportunity to legalize their dirty money by buying and selling their e-wallets of cryptocurrency without knowing their names and the source of money and " Much of these transactions happen via blockchains away from scrutiny of any national and international regulatory authority." (Uwem Essia and Kester Ehiwario, 2022, p. 2)

Right now, many countries are trying to illegitimate the trade of cryptocurrency, but there is no state capable of completely forbids the practice of blockchains.

Additionally, the office of foreign assets control OFAC (Office of foreign assets control, n.d.) has described the cryptocurrency system as corrupted sector in sanctioned nations in which the cryptocurrencies are used heavily to buy services and goods.

Moreover, the Online gambling is another form of money laundry because it is easy in gambling to transfer money to others as most of the gambling houses permit the transfer or deposit of money through money changers or through online untraceable means, also the gambling games have many easy options like buy in and cash out in this process the money launderers can easily cash in the dirty money and cash out later which means legalizing the money by hiding the source of funds, for example Brazil has a popular gambling game called Bingo and in 2007 the Brazilian federal police conducted an operation called "Hurricane" against gangs which contained politicians who laundered money through Bingo games (Mendes., 2007),besides The documentary titled "24 h chrono" made by Herve Martin Delpierre which released on May 8,2013 declared that there are 85% of the sports betting websites are illegal and those websites gain more money than the sport itself, and illegal deals as money laundry can smoothly be made in these websites.

For instance, President George W. Bush signed the law of Unlawful Internet Gambling Enforcement Act (UIGEA) on October 13, 2006 " the UIGEA bans internet gambling by forcing financial institutions to prevent financial payments of wagers from bank accounts and other financial instruments." (M, 2008) But till now there are many countries which have little experience in controlling this line of business and the lack of experience may lead to money laundering operations in gambling industry.

It is true that most of the financial institutions are practicing activities related to anti money laundering (AML) in order to observe and to state any doubtful activity but according to Uwem Essia:" AML may just make things difficult to financial institutions without reducing financial crimes in the medium and the long term because the digitized criminals will sooner find their way around any regulations and defeat its purpose" (Uwem Essia and Kester Ehiwario, 2022, p. 4).

Another form of digital financial crime is the online fraud auction, and the number of users who become victims for this fake auction are increasing gradually each year and according to Dara Clevin: " it should be permitted to govern themselves, claiming that their mechanisms are most effective to prevent fraud, the statistics clearly show that their efforts are ineffective in stemming the growing problem of online auction fraud" (Clevin, 2005).

Likewise, The hackers are abusing their anonymities in the internet and it is always for their advantages in the fraud action and referring to social market foundation: "just over 1 in 5 of adults across UK and in other 14 countries around the world were defrauded between 2021 and 2023." (SMF, n.d.)

The Tax Misapplication is a new mean of escaping the taxes payment , normally the sale taxes are collected and delivered by the retailers who sell the products to the customers but this is not happening, because right now most of the end users or consumers are paying the taxes directly to the taxing state and this method called use tax and according to Eric Menhart: " enforcing use tax is a problem and needs education of consumers, because most of them have no idea how to do the calculation and very few even know that any such tax is due." (E, 2007)

Similarly, The online retailers are still adopting the old methods of taxation fraud as like underreporting sales and False invoicing, and the problem is that there is no united taxation system that can prevent these illegal actions in cyber space as each state or country deploys its own regulations about taxation and this is also applicable on the online businesses , besides this gives the choice for the cybercriminals to establish their shell e-companies in countries with least taxation rate to escape tax payment.

Moreover, selling illegal stuff online is another kind of cybercrime which is happening in dark web where the users will be untraceable, because of that the criminals use the dark web to sell drugs and other things.

For example, P Ross Ulbricht, a criminal who owned a website called the silk road in dark web which sold drugs and caused the death of more than 6 people, had been arrested in Manhattan in 2015 and he was sentenced for life time prison, additionally The silk road was used by thousands of drug dealers and the site made millions of dollars yearly. (US immigration and customs enforcement, n.d.)

Furthermore, the dark web also sells stolen personal data yearly in millions of dollars:" Recent research by NordVPN , through their dark web case study, reveals a staggering $ 17.3 million in income from the sale of stolen data." (Greening, n.d.)

Another financial crime in cyber space is The digital intellectual property theft which is also stated as cyber financial crime since the hackers are stealing idea, trademarks and patents from individuals and companies and the cyber criminals are making illegal money from selling and trading those properties. for instance, USA loses each year between $ 225 billion to $600 billion from the theft of intellectual property. (CRI group, n.d.)

Unfortunately, cyber financial crimes are not only made by individuals but also by countries and the Russian cyber-attack against Estonia in 2007 is one of the biggest financial crimes that had happened in cyber space.

The Russian hackers attacked all the Estonian e-organizations specifically the e-banking systems with the cash machines which were out of order for a plenty of time. (Mcguinness, n.d.)

Likewise, It is important to mention that after the Russian cyber-attack a manual had been created between 2009 and 2012 by the NATO cooperative defense center with the help of international group of experts (N.Schmitt, 2013, p. 1), and the manual called Tallinn which is a name of place in Estonia.

The Tallinn manual is a combination of international law and human rights that protects the civilians only in cyberwarfare and this is the weak point in the manual as for example the manual does not cover the victims of the cyber financial crimes during our normal time apart from cyberwarfare: "cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace are not addressed in the manual because application of international law on uses of force and armed conflict plays little or no roles in doing so." (N.Schmitt, 2013, p. 4)

All the cyber financial crimes that we had mentioned above are causing a human rights violation, first the digital money laundering in cryptocurrency is harming a lot the e-economy, because sometimes the money launderers can manipulate the

price of the cryptocurrency specially if they buy and sell the cryptocurrencies with large amount of money and in short period of time in order to legalize their money , and this kind of transaction may result the bankruptcies of many innocent traders and this is forbidden in the article 17 of human rights declaration:" no one shall arbitrarily deprived of his property."

Moreover, the fraud auction and ransomware attacks are stealing people's money and this is a criminal act and a human rights violation since we are depriving people from their wealth, Also Selling digitally the bad substances such as drugs caused a lot of damages for the buyers and many people died because of their addictions like the victims of Ulbricht case and this is a violation to human rights which is mentioned in the article 3 of the human rights declaration:" everyone has the right to life, liberty and the security of the person." (Amnesty International , n.d.)

Furthermore, selling private personal data in dark web and spyware attacks are another break of human rights which is article 12:" no one shall be subjected to arbitrary interference with his privacy".

Another point to discuss is the failure of regulatory system in controlling the cyberspace which led to the increasing number of cyber financial crimes.

Even the AML practices did not work in cyberspace despite all the global attempts: "despite all the international and national AML laws regulations most money laundering crimes are only discovered after the criminals had succeeded. The reality is that AML efforts are largely unsuccessful globally." (Financial Crimes, n.d.)

Most of the developing countries are suffering from the cyber money laundering because of the lack of policy and regulatory in their states which can prevent those crimes, for instance Brazil till now doesn't classify money laundering as crime in its criminal law code, besides countries such as Mexico and Columbia are having a lot of drug organizations that are counting heavily on the digital wire transfers to launder the drug money. (Linn, 2007)

Most of the big countries as USA, European union, Russia and China and others established their own regulations and restrictions to limit the cyber financial crimes and most of the cybercrimes, also USA founded the internet corporation for assigned names and numbers ICANN as regulator to cyber space.

ICANN is an international multistakeholder group which represents many countries in the world but it is located in USA and many countries did not participate in this organization because they afraid of the American's influence on the organization, besides the ICANN is nonprofit organization with a board of directors from both public and private sectors but it does not contain foreign governments (ICANN, 2014), and the first mission of the ICANN was managing the internet's address system, besides the organization was active in resolving cybersquatting like " more than 10,000 cases in which domain names were either confusingly similar to or illegitimately misused trademarks were solved" (Zalnierute, 2020), also ICANN played an important role in the development of e-commerce and these achievements qualified the ICANN to take more responsibilities in international legal, political, economic, and security issues, however the legitimacy of the ICANN started to be doubtful after the election of October 2000 which produced new five members in the board of the directors and the voters community refused the current board and its policies, but instead of retreating, the board passed its power to an executive community which weakened the legitimacy of ICANN.

Besides, there is another American organization which is collaborative forum of volunteers called the Internet Engineering Task Force(IETF) and its mission had started in 1986 in engineering new protocol and updating old protocol, also the IETF is the governor of the communication system in internet and it contains network designers, operators, vendors, and researchers concerning the internet architecture. The IETF is responsible for the protocol of the global TCP/IP network besides the difference between ICANN and IETF is the technical issue as IETF has a technical communities which deal with particular problems and this gives the IETF more legitimacy than ICANN, nonetheless IETF is only setting standards and it doesn't have interest in resolving disputes and this is a basic thing in cyber governance for that reason the IETF is not consider as the governor of cyber space because its role is partial in cyber governance.

Moreover, there is the information Security Operation Center (ISOC) which is nonprofit organization and its mission is: " empowering the people to keep the internet a force for good: open, globally connected, secure and trustworthy." (Internet Society, n.d.) Besides The organization has its authority and influence but it always acts with members.

Likewise, there is the internet research task force (IRTF) and the main purpose of this American organization is to promote research of importance to the evolution of internet also IRTF identifies area for future research and development but there is a criticism that IRTF competes with other bodies for policy influence.

Furthermore, The European union EU declared cybersecurity Act:" the cybersecurity act strengthens the EU agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services." (European Commission, n.d.)

In Russia there is the critical data infrastructure (CDI) law for cyber security, and in China it calls the cybersecurity law of the people's Republic of China, also There is shanghai cooperation organization which was established in 2009 to ensure an international information security and there are six members in this committee (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) (UNIDIR, 2009), besides there is The Asia Pacific Economic cooperation which is the APEC that was founded in 2002 for the cyber security strategy in this region, as well there is The association of southeast Asian nations and it consists of 10 members (Brunei, Cambodia, Indonesia, Laos, Malysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam), also the association was made for the cyber security of those nations, and there is The commonwealth of the nations that contains more than 53 countries and its mission is to provide those countries with legal framework for cybersecurity.

All those associations and committees are working on the national and regional level in securing the cyberspace from the cyber-attacks but sadly their works are still not enough because the cybercrimes are spreading Fastly in all the world.

The UN is trying to be the guardian and the custodian of cyber space and many agencies were created in UN for this purpose as like international communication union ITU, UNESCO, and UN conference on trade and development UNCTAD and the UN agency which is specialized in cyber governance is the Internet Governance Forum IGF which does not have real authority in managing the governance in cyber space. All of those agencies are working separately but each one has a specific issue to accomplish in cyber space and this is a weak point in UN strategy toward the cyber governance, since sometimes they will be conflicts of interests among those agencies for the reason that they work independently without cooperation with each other.

The question is How we can unify the policy and regulation of the limitless cyber space and the answer for this question is by applying the global cyber governance with respect to global common which has direct relation with cyber governance.

The idea of internet governance is not new and the first summit about this issue was the world summit on the information society or WSIS(2003-2005) and an important statement declared from the conference concerning the internet governance:" the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures that shape the evolution and use of internet, this working decision reinforces the concept of inclusiveness of governments, the private sector and civil society in the mechanism of internet governance." (Chateau de Bossey, 2005)

But in 2013 the internet governance became more popular subject specially after Edward Snowden disclosed information related to illegal forms of mass online surveillance commanded by the US and the UK authorities, this incidence was the impetus that led to the consideration of human rights as an essential issue in cyber governance.

Furthermore, there were two serious attempts to produce officially the cyber governance, but sadly they failed to address the cyber governance as official legal frame work for cyber space for many reasons.

the first one was the UN human rights Council Resolution of 2012 (Chateau de Bossey, 2005), the decisions of this resolution were mainly based on human rights such as respecting the freedom of expression and obliging all the countries to facilitate access to the internet but the problem was that there were signatories in the resolution which supposed to be custodians of human rights under UN systems but those signatories were in the same time perpetrators of human rights abuses, and this made a conflict of interests which led to the failure of this resolution.

A second attempt was the inaugural NETmundial (Internet Society, n.d.),cohosted by the Brazilian government and ICANN in 2014, the meeting produced stronger terms than the UN 2012 resolution specifically the terms related to human rights and norms also a place was given for the nonstate actors in the conference which had an equal role in decision making of internet

governance, unfortunately agencies which consider the referee of cyber governance as the internet governance forum and UN agencies were not presented in the meeting and they did not adopt the outcome of this meeting.

Moreover, identifying the cyber space as global common is necessary in cyber governance and the term common means: "a resource shared by a group of people." (Ostrom, 2006), the common is not privilege for specific state or private person but it belongs to all , also the notion of the global common suggests that there are limits to national sovereignty in specific places in the world should: " open to use by the international community but closed to exclusive appropriation ." (Calster, n.d.)

The global common is about 75% of the earth's surface containing high seas, Antarctica, outer space and the atmosphere and some people said the cyber space is also including (W.Franzese)These areas should be controlled by the international community since the global common considered as common Heritage of mankind, but what is happening right now is the reverse because those areas are controlled by individual coastal nations instead of international community, also the same thing can be happening in cyberspace where countries are trying to have superior control online.

Each area of global common has a unique identity and they are not under the national jurisdiction because they lack the requirements of statehood for that reason the global commons are governed by a mixture of regulation including treaties, regional agreements and national regulations.

There are opposing thoughts as to whether cyberspace is a part of the global commons. for instance, the 2005 US Strategy for Homeland Defense and Civil support states: "the global commons consist of International Water and airspace, space, and cyberspace." (US Department for defense, n.d.) But the 2008 National Defense strategy did not identify the cyberspace as global common. The shared global infrastructure for cyberspace is considered as global common because it is owned by private and public sector and it is subjected to national and international regulations.

The cyber space as global common is also a shared resource among people in all around the world and The cyber financial crimes, which are becoming very successful against e-commerce as we mentioned previously, are shaking the consumers' confidence which degrades the cyberspace as a common resource, also the illegal espionage is a degradation of the resource.

Furthermore, the national regulation in cyberspace is augmenting and it is dangerous aspect on cyber space standing as global common, and the censorship is an activity which is practiced by many countries around the world for good and bad purposes.

The censorship is a filtering mechanism that can block website easily by authorities, some countries as USA is using the censorship to protect the children by blocking the website of children pornography, but many nations are using this option to control the people in cyber space in order to stay in power and this is affecting the freedom of speech and other human rights and most of those countries are contributing in cyber insecurity: " authoritarian regimes are working to censor their web, even countries in sub-Saharan Africa." (Bhala, 2024), also the Syrian and the Egyptian authorities ordered to shut down the internet during the Arab spring period because the internet played a major role in social mobilization, also the Chinese government ordered to block 18,931 websites for the reason that the Chinese authority wants to control what the people watch, all of those actions are human rights violation precisely the article 19 of UDHR which includes the protection of freedom of speech, communication and access to information.

This research has been conducted because the number of victims in cyber space are increasing daily and the problem is that most of the criminals are escaping without judgment because of the existing gaps and holes in cyberspace and only with cyber governance we can reach a solution to the cyber attacks.

B- **Methodology**:

The research article discusses the cyber financial attacks effects on human rights and proposes solutions to this problem, in the research you find many examples about the types of cyber financial crimes as like the money laundering, malwares attacks , selling illegal products, stealing intellectual properties, fraud auctions, misplacement taxes, and attacks on the e-banking system, also many data had been mentioned in the article about national and non-state organizations in the domain of cyber governance such as ICANN,IETF,ISOC, IRTF and others, besides there was information about global common and some examples about the factors which affected negatively the global common as like censorship and national regulation, and we used the mixed method in collecting the data which is a combination between qualitative and quantitative, for instance we can find a lot of numbers which showed the amount of economic losses from the cyber-attacks such as $ 1.5 billion from malware attacks and $ 8.6 Billion from the laundered money in cryptocurrency and we used here the quantitative method,

but most of the data in the research were collected on qualitative method and I utilized the secondary research which was a collection of data based on credible books such as Anti money laundering (AML): governance, Risk management and compliance book , Schemes and scams: auction fraud and the culpability of host auction web book, Tallinn Manual on the international law applicable to cyber warfare book, Dark commerce: How a new illicit economy is threatening our future book and managing cyber-attacks in international law, Business and relations book, likewise there were many websites such as BBC, united Nations, UNESCO, Financial crimes, also most of those books and websites are credible source of information which is based on my criteria of credibility in showing the readers believable information about the cyber financial attacks effects on human rights and convincing the audience with accurate results as cyber governance.

Moreover, I consulted a wide variety of sources in collecting the data and it was my first research strategy as I used the google search engine to find reliable websites and online articles about cyber financial crimes and cyber governance treaties, also I utilized the google scholar to find specialized journal articles related to my topic, for example, I accessed many information from indexed journals. Besides I depended mainly on kindle in searching and downloading the e-books since all the used books in the research were e-books, likewise I used a lot of the existing citations in the e-books to find information and references about my topic.

My second research strategy was the critical thinking since I critically evaluated every piece of data I found before I put it in the research and my evaluation criterium was based on the reliability of information and its relevance to my objectivities in the research.

The third research strategy that I utilized was keeping track to my information sources in order to avoid plagiarism, and I used the reference technique option in Microsoft word to insert the citation and to create the bibliography.

Moreover, I wrote many examples about cyber financial crimes, human rights violations, and the cybersecurity's organizations in order to draw a theory about cyber governance and its attributes and this is an inductive reasoning which is my analytical framework in the research, as most of the financial problems in cyber space that were mentioned in the research accompanied with examples on organizations which failed in protecting the human rights in cyber space and this conducted us to the conclusion of the necessity to apply international cyber governance, and this is the inductive strategy which starts from the specific to reach the general.

C- Results:

First, Cyber governance must be the international law in cyber space which cannot be crossed by the cyber criminals because there will be punishment for each attempt to attack people online, cyber governance is the legal frame work to the cyber space.

Second, the cyber space must be considered as a global common because the global common is additional legal framework to cyber space and it will eliminate the cyber financial crime.

Third, the UN must be more active in cyber space despite its last attempt to create many departments related to cyberspace but this is not enough as the decision making must be centralized in one department, besides the UN must be the official sponsor of cyber governance.

Forth, there must be an international cyber financial court specialized in making new laws against the cyber-attacks since the cyber-attacks are developing gradually with the advanced technology in cyber space, likewise the international financial court must always be ready to update the laws because the cyber financial attacks are changing momently in this era.

D- Discussion:

1-The cyber governance:

cyber governance is the official international law of cyber space that can prevent the human rights violations for that reason cyber governance must be created by both authorities and the private sectors with the support of civil society.

In this process the private sector is fundamental in the creation of governance specially their IT experts who have a huge knowledge in cyber space and they can share their ideas with the authorities toward the formation of laws of governance,

because the IT experts have a complete understanding to the cyber space and the weakness points of cyber security, also they can know what kinds of policies and procedures that are suitable to protect the users from the cyber-attacks and crimes.

The creators of governance must be careful about their restrictions in the space as sometimes too much rules may bother and harm the cyber users, which means that there must be a balance between the limits of restriction in cyber space as governors should not affect negatively the liberty of practicing in cyber space by applying strict regulations, but in the same time the governors must assure the protection of the users online which means that the governors should always take care of human rights.

The rules in governance must be transparent and clear to all the people in cyber space because people must know what should they do and what they should not do.

Moreover, the laws must be effective and always updated since the cyber criminality is always in advance parallelly with the unstoppable development of cyber space.

Furthermore, the laws of governance must be punishable and credible and each criminal must know that there is a punishment available to every violation inside cyber space.

The collaboration between the authorities and the IT experts in private sectors also must take care of the technical issue in cyber space which is a source of cybercrimes for example the weak coding and the easy penetration to the firewalls are big problem in cyber space and the IT experts must fortify the coding system with the firewalls.

There must a collaboration between the legislators of cyber governance and the compliance and fraud prevention teams because there is gap between cybersecurity and financial crimes teams as they work independently which results fragmented team management and missed connections between threats, also there must be alignment between cyber governance and global financial standards as like FATF and AML, besides there must be in the cyber governance body a joint task forces to direct responses to dangerous threats.

2-Global common:

considering cyberspace as global common is still a debate among the countries around the world because many countries afraid of the concept of global common which can interfere in their arbitrary controls to their cyber space, but the nature of cyber space as global shared resource of information is the characteristic of global common, besides the cyber space is similar to the outer space which was considered as global common in 1966 and this classifies the cyber space to be a global common, for that reason some of the international space law can be applicable in cyber space and it can resolve many problems as the following:

First, the global common is controlled by international law which is based on human rights and this idea is a source of fear for dictatorial regimes which are misusing the cyber space by applying censorship option to control their people and this is prohibited in the global common because by censorship we are depriving people from the freedom of choice and from accessing information and the global common is a space for all the people who can benefit from it freely without restrictions and according to the international space law "the space shall be carried out for the benefits and in the interests of all countries and shall the province of all mankind." (United Nations Office of Outer Space, n.d.)

Second, the cyber wars including the cyber-attacks are crimes which are harming the cyber users a lot and global common policy avoids the use of cyber common space for wars' objectives and it should only be used for peaceful purpose and one of the principles in international space law does not allow the states to place nuclear weapons and other weapons or mass destruction in the orbit which means that the wars are forbidden in outer space for that reason all kinds of cyberattacks are against global common regulations.

Third, there are many countries which have their own cyber governance as like Russia and China, and as we mentioned previously that the national regulation is risky on cyber space status as global common, and it is the responsibility of the global cyber governance to create centralized governance and forbid the national governance , and this is clear in the international space law which clarifies that outer space is not subject to national appropriation by claim of sovereignty.

At the end, cyber governance plays a major role in protecting the cyber global common specifically the human rights issue since most of the tragedies in cyber global common are causing a human rights violations. For instance, many countries are illegally surveilling their citizens by using cyberspace like Snowden case, also countries as China and Russia have millions of surveillance cameras with facial recognition technique (FRT) which are connected in the network of cyberspace and the citizens are the main target of these cameras because those regimes afraid of the political demonstration which can be threat to their authorities and cameras can help them to identify the participants in the demonstration.

the cyber governance must forbid the illegal surveillance because it is breaching the privacy and the freedom of expression in cyber space and it is a human rights violation and opposing the global common regulations.

3-**The Role of United Nation:**

We had already mentioned that the UN is trying to play a major role in cyber space, and the UN has many divisions related to cyber space as like international communication union ITU, UNESCO, UN conference on trade and development UNCTAD, and IGF.

The problem is that too many divisions for the cyber space will not be very useful in solving the cybercrimes because there will be a conflict of interests between the divisions and this is not good for cyber security since the UN is the sponsor of human rights and it must play a major role in avoiding human rights violations in cyber space, for that reason the UN must be solid in decision making toward cyber criminalities and there must be only one division specialized in cyber space, with one department as the decision making will be more centralized and more accurate in solving cyber-attacks problems.

The UN must be the coordinator in applying the cyber governance because the UN represents the majority of the nations in all around the globe, so the implementation of cyber governance will be easier with the efforts of the UN as most of the international treaties that had happened lately are considered UN's achievements.

The UN can participate in the creation of legal framework of cyber governance for the reason that the UN has many international legal experts who can contribute positively in making the rules and procedures in cyber space.

Moreover, the most important thing that the UN can do is legalizing the cyber governance globally, also the UN has the privilege and authority to oblige all the countries to follow the policies and procedures of the new cyber governance in cyber space.

Historically, the UN announced many agreements and treaties linked to global common as like the Antarctic treaties, oceans treaties and outer space agreements, which means that the UN can be very supportive for the idea of considering the cyber space as global common and this will facilitate the process of identifying the cyber space as global common.

4- The creation of international tribune for cyber financial crimes:

The quality and quantity of cyber financial crimes are increasing remarkably in cyber space and it is always related directly to the fast technological development in cyber space, so as more as advanced we become in technology as more as cybercrimes we will witness.

The high number of quantities and the different qualities of financial crimes that we have now in cyber space propose a challenge to the legislators of the cyber legal framework system because the legal system should always be updated with the new kinds of cybercrimes that are appearing, for that reason the international cyber financial court is necessary to fix this problem since this court will be formed specifically to penalize the cyber criminals and to update all the laws related to cybercrimes.

This tribune may help the developing countries which are suffering from the financial crimes as like cyber money laundering and others because of their weak financial legal systems, for example the international court can suggest new and updated laws for those developing countries.

The international financial tribune can develop one financial jurisdictional system for all countries around the globe, since most of the financial crimes that were committed online took a lot of time in the investigation process because the crimes had existed in many different countries, and each country has its own financial jurisdiction system as a result of the

multijurisdictional systems the investigations in cyber financial crimes absorb a plenty of time and the investigators face a lot of legal obstacles, so the international court can finalize these problems by implementing one financial jurisdictional system.

The international financial tribune should always take into consideration the human rights violations as most of the financial crimes are violating the human rights like cyber money laundering, fake cyber auctions and selling online drugs and illegal goods, also Many people lose their wealth and privacies, and sometimes people lose their life because of these financial crimes, for that reason the human rights must be the base in creating the laws in cyber space, and there must be cooperation between the International financial tribune and the international human rights court because the Judgment of the international financial tribune in the cases of cyber financial crimes Must be based on human rights treaties and regulations which is the responsibilities of international human rights court.

F- Conclusion:

As a conclusion, the role of UN in cyber financial crimes is fundamental as UN represents most of the countries in all around the world so any decision adopted by the UN will be approved internationally, but there must be only one division in the UN which is specifically for cyber space, also the UN can play a major role in creating the cyber governance and in considering the cyber space as global common,also The international financial tribune can make and update the laws linked to cyber financial crimes because the number and the quality of crimes vary increasingly with the advanced technological development in cyber space, for that reason there will always be new kind of cyber financial crime that needs new updated laws and this is the mission of the international financial tribune.

Moreover, identifying the cyber space as global common will help a lot in fighting the cybercrimes because global common is an additional regulation to the cyber space which will be very supportive to cyber governance.

Furthermore, cyber governance will decrease the cyber financial crimes since there will be a framed restrictions laws in cyber space that respect the human rights and avoid the cyber-attacks against the people, as well cyber governance will be approved by most of the countries because it will be sponsored by UN.

We can find many researches about cybercrimes which share with our research the same idee about the riskiness of cybercrimes in twenty-one century, for instance there is journal article called cybercrimes and their impacts in which the writers mentioned:" organized crime groups are using the internet for major fraud and theft activities, as criminals move away from traditional methods, internet based crime becomes more prevalent." (hemraj Saini, yerra Shankar Rao,T.C.Panda, 2012) , also the researcher claimed that the cyber financial criminal activities reached $ 32 Billion and these information was mentioned in the beginning of our research as the criminals are using badly the cyber space for money laundering and other criminal activities also the financial losses are in billions which makes our information identical with the data of this research, but the research did not propose a solution for cybercrime and it was only a review.

Another research which I found similar to our research is cybercrime and cyber law in Nigeria, in this article the writer declared that the criminal code in Nigeria doesn't cover cybercrime which needs amendment or update:" The national assembly is the legislative body which must as matter of urgency modify and amend certain section of criminal code to deal with cybercrime." (Maitanmi Olusola , Ogunlere Samson , Ayide Semiu, Adekunle yinka, 2013).

Moreover, new creation and renewal of cybercrimes laws are what we suggested previously as one of the solutions in the developing countries to fight the cyber-attacks, also the writers of the Nigerian research paper recommended that there must a collaboration between the government and the civil society to strengthen the legal system in cyber security and this is what we recommended in the formation of cyber governance as we insisted on the collaboration between the governments and the private sectors with the help of the civil society in the creation process of governance, but the research missed the solution for the problem of Nigerian cybercrimes.

There will be a great challenge during the creation of cyber governance and the first challenge will be in having environments with low formalization and we mean here the developing countries which have poor cyber infrastructure and weak jurisdiction systems that can't help in implementing cyber governance globally.

The second challenge is the heterogenous organizational form of cyber governance as we said previously that many organizations will participate in cyber governance such as governments, private companies and social communities and each member will have specific role to accomplish in cyber governance but there is a great possibility of losing transparency of cyber governance in this heterogenous structure. for instance, cyber governmental investigators cannot give information about a suspect to a partner in the governance body until the investigation is done and this is a lack of transparency between the partners of cyber governance.

The third challenge is the large number of actors in cyber governance which will affect the decision-making process.

The fourth challenge is the possibility of human rights violations during cyber security operation, since the main goal of cyber governance is to fight the cyber-attacks and sometimes for security reason cyber governors suggest censorship to avoid certain suspicious websites and this can have negative effect on the freedom of choice also practicing espionage on emails for the purpose of identifying malicious emails is a breaking of the privacy and this is human rights violation.

There are many opinions contradict the idea of cyber governance because it is: "stratified…structure underscores a particularly complex regulatory environment, making…mapping or forecasting, the effects of regulations especially difficult." (Powell, 2023), also there are Dr. David post and David Jhonson suggested the abstract models in mapping cyberspace as like the " the astronomical number of different configurations" and this is very complex model but required to cyber space matrix because a one change in regulatory framework can have bad consequences elsewhere and the doctors described the process of creating the legal framework of cyberspace as: " an exponentially complex system." (R.Jhonson, 1998)

Furthermore, Scott J. Shackelford claimed that: "national control of cyberspace is one of the classical solutions to the tragedy of the commons" (Scott J.Shackelford, 2014) which opposes the centralization of cyber governance in decision making , besides China is a great example of the national control of cyberspace which has a strict control over the internet: " an estimated 30,000 personnel spread across twelve government agencies enforce more than sixty internet regulations and censorship systems implemented by state owned Chinese ISPs, business and organizations." (Zhao, 2008)

The Chinese experience in the domestic cyber regulations and identifying China in cyber space as the great firewall proved that China is prioritizing the national regulation over global cyber governance.

The strength of this research is our suggestion to classify the cyber financial crimes law under cyber governance umbrella and it is new idea which can enlarge and strengthen the cyber governance s' legal frame work, also cyber financial crimes can be eliminated with the help of international cyber financial court which is another suggested original solution, besides considering cyber space as global common is another point of strength to our research because cyber governance will be more wanted globally and more effective since cyber governance will be responsible for any human rights violation in cyber global common also the global common will be a strong legal shield to cyber space.

In the opposite side, the unstoppable development of cybercrime will must probably lead to new kinds of cybercrimes which are difficult to be predicted and that required a daily investigation by cyber governors in order to invent and update regulations and this is point of weakness in our research as what we suggested today as solutions may be not useful for the future cyber financial crimes.

Another point of weakness in our research is the difficulty to apply cyber governance in the real world since most of the attempts that had happened in the past failed to create the cyber governance because of the complexity of the creation process so our proposal about cyber governance could be more theoretical and difficult to apply in reality.

References

(n.d.). Retrieved from CRI group: http://crigroup.com/intellectual-property-what-do-the-statistics-indicate/

(n.d.). Retrieved from European Commission: http://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

(2009). Retrieved from UNIDIR: http://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIxMiJ9

Amnesty International . (n.d.). Retrieved from http://www.amnesty.org

BBC. (n.d.). Retrieved January 26, 2002, from https://www.bbc.com/news/technology-60072195

Bhala, N. (2024, March 4). *Reuters* . Retrieved from https://www.reuters.com/article/world/digital-authoritarianism-threatening-basic-rights-in-africa-study-says-idUSKBN2AW0YR/

Calster, G. V. (n.d.). *INTLL*. Retrieved from https://www.eolss.net/sample-chapters/c14/E1-36-01-04.pdf

Chateau de Bossey. (2005, June). Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wgig.org/docs/WGIGREPORT.pdf.

Clevin, D. (2005). *Schemes and Scams: auction fraud and the culpability of host auction websites.* Loyola consumer law review .

Cyberark. (n.d.). Retrieved from https://www.cyberark.com/what-is/malware/#:~:text=Malware%20attacks%20are%20any%20type,infrastructure%20without%20end%2Duser%20knowledge.

E, M. (2007). *Taxing the internet: Analyzing the states 'plan to drive online sales revenue.* Journal of state Taxation.

Financial Crimes. (n.d.). Retrieved from http://www.elucidate.co/blog/5-reasons-why-the-global-anti-money-laundering-system-is-failing-financial-institutions

Greening, J. (n.d.). Retrieved February 18, 2025, from http://www.gosa.org

hemraj Saini, yerra Shankar Rao,T.C.Panda. (2012). Cybercrimes and their impact: a review . *International Journal of engineering* , 202.

ICANN. (2014, july 29). Retrieved from https://www.icann.org/en/governance/documents/bylaws-for-internet-corporation-for-assigned-names-and-numbers-a-california-nonprofit-public-benefit-corporation-30-07-2014-en

Internet Society. (n.d.). Retrieved from https://www.internetsociety.org/about-internet-society/#:~:text=We%20are%20a%20global%20charitable,the%20heart%20of%20our%20mission.

Internet Society. (n.d.). Retrieved from https://www.internetsociety.org/events/netmundial/2014/

Krysinska, J. (2024, December 2024). *Nordlayer* . Retrieved from https://nordlayer.com/blog/data-breaches-in-2024/

Linn, C. (2007). One hour money laundering: prosecuting unlicensed money transmitting business using section 1960. *USA attorney'sbulletin* , 5-55.

Louise, S. (2018). *Dark Commerce. How a new Illicit economy is threatning our future* . New Jersey : Princeton University Press .

M, B. (2008). *The unlawful Internet Gambling enforcement act: a bad gambling act? You Betcha!* Rutgers Law Review.

Maitanmi Olusola , Ogunlere Samson , Ayide Semiu, Adekunle yinka. (2013). cybercrimes and cyber laws in Nigeria. *International journal of engineering and science* , 19-25.

Mcguinness, D. (n.d.). *BBC*. Retrieved April 27, 2017, from https://www.bbc.com/news/39655415

Mendes., S. S. (2007, September 1). *International Enforcement Law Reporter*.

N.Schmitt, M. (2013). *Tallinn Manual on the international law applicable to cyberwarfare* . Cambridge : Cambridge University Press .

Office of foreign assets control. (n.d.). Retrieved October 2005, from http://ofac.treasury.gov/media/913571/download?inline

Ostrom, C. H. (2006). *Introduction: an overiew of the knowledge Common in Understanding knowledge as Common Theory To practice* .

Powell, D. E. (2023). *Fordham Law School*. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2271&context=faculty_scholarship

R.Jhonson, D. G. (1998). *Chaos in Prevailing on Every continent: Toward new Theory of Decentralize the Decision Making in Complex system.*

Sanctris, F. M. (2019). *Technology Enhanced Methods of Money Laundering* . Switzerland : Springer .

Scott J.Shackelford. (2014). *Managing Cyber Attacks in International Law, Business and Relations.* New York: Cambridge University Press .

SMF. (n.d.). Retrieved March 12, 2024, from https://www.smf.co.uk/1-in-5-people-have-been-a-victim-of-fraud-in-the-last-couple-of-years-international-survey-finds/

Statista Research Department. (2025, April 1). Retrieved from https://www.statista.com/forecasts/1283912/global-revenue-of-the-e-commerce-market-

The Hindu Bureau. (2025, March 18). Retrieved from https://www.thehindu.com/sci-tech/technology/as-ransomware-attacks-surge-india-accounts-for-over-half-the-hits-in-2024-report/article69343710.ece

UK Finance. (n.d.). Retrieved from https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app

United Nations. (n.d.). Retrieved from http://www.unodc.org/roca/en/NEWS/news_2024

United Nations Office of Outer Space. (n.d.). Retrieved from https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

US Department for defense. (n.d.). Retrieved from https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/Homeland-Defense-Integration-and-DSCA/References/Strategies/

US immigration and customs enforcement. (n.d.). Retrieved May 29, 2015, from https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating

Uwem Essia and Kester Ehiwario. (2022). *Anti money laundering (AML): governance, Risk management and compliance* . Mauritus: Lab Lambert Academic publishing .

W.Franzese, P. (n.d.). *Soveignity Of Cyber Space Can Exist.*

Zalnierute, M. (2020). *University of New South Wales Research Series*. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www5.austlii.edu.au/au/journals/UNSWLRS/2020/6.pdf

Zhao, J. (2008). A Snapshot of internet Regulation in contemporary China: Censorship, Profitability and responsibility. *China Media Research*, 37.

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار الثامن – العدد الثمانون
تاريخ الإصدار: 2 – حزيران – 2025م
www.ajsp.net

"آثار الجرائم المالية الإلكترونية على المدنيين وأفضل الطرق لحماية الفضاء السيبراني من انتهاكات حقوق الإنسان."

د. زياد زهيري

الملخص:

الفضاء السيبراني يشهد أنواع عديدة من الجرائم، والجرائم المالية الإلكترونية هي واحدة منها، وهي من أخطر الجرائم على الإنترنت، حيث يفقد الآلاف من الناس أموالهم وأحيانًا حياتهم بسبب هذه الجرائم.

توجد أنواع عديدة من الجرائم المالية الإلكترونية مثل غسيل الأموال، الاحتيال عبر المزادات على الإنترنت، بيع المخدرات والمواد غير القانونية، وسرقة الملكية الفكرية الرقمية، وكل نوع منها كارثة بحد ذاته. على سبيل المثال، يقوم غاسلو الأموال بشراء وبيع عملات مشفرة بمليارات الدولارات لتبييض أموالهم، كما يتعرض الناس للاحتيال سنويًا بسبب مشاركتهم في المزادات الاحتيالية على الإنترنت، بالإضافة إلى أن عدد المراهقين المدمنين يتزايد بسبب المواقع الإلكترونية في الشبكة المظلمة التي تبيع المخدرات والقضايا غير القانونية، بالإضافة إلى أن سرقة الملكية الفكرية على الإنترنت تمثل خسارة كبيرة للاقتصاد العالمي.