International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cyber Attacks on Human Rights and the Role of Cyber Governance

Ziad Zouheiry

Ceds Centre Detudes Diplomatiques Et Strategiques, Paris, France

Abstract: ***The paper is about cyber-attacks and their consequences on human rights and the effective role of cyber governance in protecting the users from human rights violations, besides the mixed method approach and deductive reasoning were used in the paper to collect information from different resources as like books, articles form the internet, and we used some research studies which are similar to our subject and we used also record keeping which represented articles from different sources. Cyber-attacks have caused many human rights violations because the attacks disclosed the privacies of cyber users which is human right violation, also the cyber-attacks had badly affected the freedom of expression and freedom of opinion and the intellectual property in many incidents which are also human rights violations, and the question is how we can prevent the human rights violations in cyber space. The research findings lead us to cyber governance which is the best way to protect the users in cyber space, and the number of human rights violations will definitely decrease if the governance is applicable in cyber space because cyber governance will be based on high ethical standards and the governance will represent the international law in cyber space which will be the guard of human rights.***

Keywords: cyber-attacks, human rights, cyber governance, freedom of expression, ethical standards

1. Introduction

Cyber attack is the kind of crime which is happening daily in all parts of the world , and cyber attack can be made against all kinds of users in cyber space from individuals to reach the biggest e-organizations and e-businesses, as the statistics showed that more than 422 million users were attacked in cyber space[1], also cyber-attacks in 2023 cost the world about $5.9 trillion[2] and there is expectation that the losses will continue to grow till it will reach $ 10.5 trillion in 2025[3], cyber attacks have not only bad effects on the e-economy but also cyber attacks are badly affecting the ethics and societies, for example many cyber attacks are happening against children and women in the world, in 2020 cyber attacks against children increased by 144% compared to 2019 with the average of 8 children per day who were being attacked in cyber space[4], likewise the number of women who were being attacked in cyber space in 2021 was about 20.2% of the overall cyber-attacks incidents that had happened in 2021[5].

Cyber attack is not only the weapon of the hackers and predators but it is also the new weapon of the armies, meanwhile most of the armies are classifying the cyber-attack as fatal weapon because of its high accuracy in accomplishing any tactical mission, for example the cyber-attack on Iranian nuclear facilities Natanz was attacked by Stuxnet worm which were developed jointly between US and Israeli intelligence services in 2010.

The Stuxnet worm had caused a breaking to the uranium enriching centrifuges and this is considered dangerous as it is physical damage made by worm attack[6], besides the Russian cyber-attack against Estonia in 2007, the Russian had made the cyber-attack on Estonia because of political reason, and the Russian hackers sent the DDOS (distributed denial of service) to the Estonian organizations like banks, ministries, parliaments and newspapers.

The banking system in Estonia had been critically damaged by the Russian cyber-attack, specifically the online banking system which was paralyzed for 22 days after the attack.

This attack had led to the creation of the official Tallinn manual which is the first official transcript about protecting the civilians in cyber warfare which was accredited by NATO in 2008[7].

It is illegal in Tallinn manual to attack any civilian during warfare which is rule 32in the manual[8],also it is illegal to attack any object related to the civilians during the warfare which is rule 37[9], but the problem in Tallinn manual that it is only inspecting the international law during cyberwarfare

[1] Nivedita James,"90's cybercrime statistics 2023, cost, industries and trend", Getastra, October 24,2023, https://www.getastra.com/blog/security-audit/cyber-crime-statistics/.

[2] Douglas Bonderud, "cost of a data breach 2023: Financial industry impacts", Security Intelligence, August 20,2023, https://securityintelligence.com/articles/cost-of-a-data-breach-2023-financial-industry/

[3] Steve Morgan, "Cybercrime to cost the world $10.5 Trillion annually by 2025", Cyber Security Ventures,November 13,2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[4] "Children and online risk: global statistics", November 20,2023,https://surfshark.com/research/cybersecurity-for-kids/statistics

[5] "Cybercrime against women",January 8,2023,https://www.clearias.com

[6] Michael Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities", July 16, 2015, https://surfshark.com/research/cybersecurity-for-kids/statistics

[7] Micheal N.Schmitt," Tallinn Manual of the International Law Applicable To Cyber Warfare", (USA: Cambridge University Press,2013),page 1.

[8] Micheal N. Schmitt," Tallinn Manual of the International Law Applicable To Cyber Warfare", (USA: Cambridge University Press,2013), page 113.

[9] Micheal N. Schmitt," Tallinn Manual of the International Law Applicable To Cyber Warfare", (USA: Cambridge University Press,2013), page 124.

and the manual is only about cyber actions under the term of use of force, besides there is no covering for international human rights which is an important part in international law concerning cyber-attacks and cybercrimes that are happening daily in cyber space against civilians, and here we can ask the question about the effects of cyber-attacks and cyber-crimes on human rights and what kind of violation we are facing in cyber space.

Cybercrimes and human rights violations:

Meanwhile People are becoming very reliant on cyber space because cyber space is containing all the humans needs like entertainment, communication, e-businesses, e-banking, e-shopping, working from distance, e-learning and others.

Furthermore, Cyber-attacks are becoming very critical to the users in cyber space and unfortunately cyber-attacks are violating the human rights and the international laws, and in this paper, we are going to discuss some of those violations.

1) Cyber-attacks and cyber connection:

Connecting to Cyber space is a necessity to every human, and any attempt to interrupt the connection between the user and cyber space is a human right violation, and the UN declared in 2016 That the internet is a human right according toarticle 19:" Everyone has the right to freedom of opinion and expression, these rights includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers, the promotion, protection, and enjoyment of human rights on the internet".[10]

For example, During the Egyptian revolution in 2011 the authority had cut off the access to the internet because of the effects of social media on the revolution.[11]

Moreover, in the Iranian presidential election of 2009 and throughout the protests against the government after the accusation to the government in interfering the election process, what the government did is disrupting the internet application as like Google's YouTube sites.

Furthermore, in 2005 the Nepalese government had stopped the internet connection during the king 's declaration of martial laws.

All those examples that we mentioned considered as human rights violation.

2) Cyber-attack against Privacy: most of the cyber-attacks are disclosing the privacies of cyber users because attackers are stealing the personal information from the users and they instantly misuse the information and this is banned in article 12 of the universal declaration of human rights in 1948:" no one shall be subjected to arbitrary interference with his privacy", similar to the north Korean cyber-attack on Sony Media Company in USA.

In 2014 Sony produced a movie called the "interview" which is a black comedy and it was about the assassination of North Korean president.

The North Korean regime considered the movie as threat to their president, for that reason the North Korean's hackers had made a cyber-attack on Sony media which is the media company that produced this movie, and the cyber-attack was massive as more than 3000 personal computers were hacked[12],and most of the personal information and emails were published lately in Wikileaks.

This is the biggest cyber-attack that ever happened in USA and it is considered as human right violation since thousands of personal information had been stolen.

Another cyber-attack incident concerning the privacy had been happened in the 2016's US presidential election between the two candidates the republican Donald Trump and the democrat Hillary Clinton.

More than 150,000 emails for the democrats had been stolen by the Russian hackers according to Guccifer 2.0 ,WikiLeaks and DC leaks, [13] the attack disturbed Hillary Clinton's staff because the cyber-attack disclosed many important information about the democrat 's election campaign which affected the final result of the election and this is another human right violation related to privacy.

There is also the case of Edward Snowden which is linked to privacy in cyber space, and the case considered as human rights violation because Snowden declared that there is an intelligence surveillance program controlled by US national security agency (NSA) and the UK's intelligence organization[14], and this program can observe the users on all the smart devices as smart phones, laptops and others.

3) Cyber-attacks against Freedom of expression and freedom of choice: people should express their opinions openly without interference in cyber space specially in social media and this is clear in article 19 of universal declaration of human rights in 1948:" everyone has the right of freedom of opinion and expression".

Freedom of expression is also mentioned in article 10 of ECHR (European convention on human rights) which

[10] Catherine Howell & Darrell M. West," the internet as a human right",Brookings, November 7,2016, https://www.brookings.edu

[11] "Arab spring anniversary: when Egypt cut the internet", Aljazeera, January 25, 2016,https://www.aljazeera.com/features/2016/1/25/arab-spring-anniversary-when-egypt-cut-the-internet

[12] Richard Stengel," The Untold Story of Sony Hack: How North Korea's Battle With Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016",Vanityfair, October 6,2019, https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack

[13] Satter,R.,Donn,j.,&Day,C.,"inside story: how Russians hacked the democrats emails", Associated press, November 3,2017, https://www.bloomberg.com/news/articles/

[14] Nick Younger," the Case of Edward Snowden",Whistleblowers, November 19,2020, https://www.whistleblowers.org/news/the-case-of-edward-snowden/

forbidden any intrusion from authority in any process of freedom of expression.[15]

Lately, People had used actively the social media platform to express their opinion freely and they had used the social media to protest against their corrupted regimes like what happened in Arab spring.

The social media played a major role in the revolutions of Tunisia, Egypt and other countries. Moreover, the social media activists had used the social media for instructing and leading the rebels in the manifestations.

The social media was very important way of communication in the 2011 Egyptian revolution and there is an Egyptian activist claimed that:" this is becoming the region's first telecommunication civil war. Our internet and smartphones are weapons, the government won't allow us to have "[16].

Furthermore, The US presidential election of 2016 between Donald Trump and Hillary Clinton had witnessed Russian's cyber interference for the benefit to Donald Trump as per social media 's accounts evidences.

The Russian hackers had made thousands of twitter accounts which supported Trump's election campaign, and twitter had identified more than 50,000 automated accounts related to Russians which mainly tweeted during the US presidential elections[17]of 2016.

The Russian Hackers were accused ofinterfering in theUS presidential election of 2016, besides the democrat 's candidate Hillary Clinton declared that the Russian's cyber-attacks were commended directly from the highest level of kremlin and the reason behind the attacks were to influence the election for the benefit of the republican candidate Trump.

Using thousands of twitter accounts by the Russians hackers to support the republican 's candidate against the democrat's candidate is a human rights violation as the Russian hackers are affecting American people's choices by the hackers' manipulation in the election process, and this is badly disturbing the freedom of choicewhich is a human right violation.

People should express their opinions freely in order to choose freely their next president,and the Russian cyber attackers tried their best to misuse the social media accounts to publish rumors and lies on the democrats which deeply affected the electors 'opinions toward their democrats' candidate Hillary Clinton, besides it was one of the reasons that led to the loss of Hillary Clinton.

Another incident related to freedom of expression had happened in Thailand, when a normal citizen sent messages in cyber space to government officials complaining about Thailand royal family, and the citizen was penalized for 20 years in the prison because of sending those messages.[18]

4) Cyber-attacks against Intellectual property: the cyber space is containing a huge volume of e-businesses, and the revenue from the e-businesses is in billions of dollars yearly, also there are many types of e-business as like e-retail stores, e-books stores, online hotel reservation and many other types of e-businesses.

It is not easy to steal those kinds of e-businesses but it is easy to copy them and this is called intellectual property theft, besides this is a human rights violation and it is mentioned in article 17 of the universal human rights declaration in 1948:" no one shall arbitrary deprived of his property".

The intellectual property(IP) has long been a point of conflict between USA and China, as China had imitated a lot of American products since 1970 because USA has been an open economy since 1970with the nothing to hide concept, as well in 2001, a new punishment laws related to IP theft were adopted by the world trade organization, but unfortunately there was no commitment from the Chinese government because many hacking accidents had been happened recently, as like when the New York times announced in 2013 that the Chinese people's liberation army (PLA) had hacked its network systems and stole data which considered as IP theft [19] , after while another news organizations claimed that the PLA also hacked their computer systems and stole data, although the wall street had long been alert of the Chinese hackers signified to intellectual property rights[20].

After the Chinese cyber-attacks on the news and media organization, a press conference had been held in the white house by the house spokesman Jay Carney who described the Chinese attacks as cyber espionage against the US economy and he considered China as a criminal when he declared that cyber-attacks are being made:" at the highest levels about cyber theft with senior Chinese officials, including in the military[21]".

Copy right is a part from the intellectual property and copyrights is a set of rights granted to the inventor of authentic work such as software, movies, photographs, music, books and others.

[15] "European convention on human rights",ECHR, https://www.echr.coe.int/european-convention-on-human-rights

[16] Maryam Ishani," Foreign policy: scramble to silence partner process ",NPR, January 28,2011, https://www.npr.org/2020/01/09/794864423/journalist-details-dangerously-unstable-relationship-between-the-u-s-and-china.

[17] Kathleen Hall Jamieson, "cyberwar: How Russian Hackers and Trolls Helped Elect a President",(USA: Oxford university press,2020)p.150.

[18] "An inconvenient Death: A Sad Story of a bad law, Absurd sentences and political expediency", May 12,2012, https://www.economist.com

[19] Nicole Perlroth," Hackers in China Attacked the Times for last 4 months", New York times, January 30,2013,Http://www.nytimes.com

[20] Joana Kulesza& Roy Balleste," Cyber security And Human Rights In The Age of Cyberviolence",(USA:Rowman&littlefield,2016)p.208.

[21] Ken Dilanian& Christi Parsons," white house Adopts New Strategy to Safeguard intellectual Property", Los Angeles Times, February 20,2013, Https://articles.latimes.com

Most of the e-entertainments are exposing to cyber-attacks and for example the music industry had lost billions of dollars because of file sharing site called Napster emerged which allowed people to download free music illegally without respecting the copyright issue:" the music sales declined roughly 50% in 1999 from $ 14.6 Billion to $ 7.7 Billion in decade because of Napster site[22]."

The companies in USA lose annually billions of dollars:" US companies alone loose around a quarter to half a trillion dollars annually through intellectual property theft".[23]

The human rights violations are a lot in cyber space and unfortunately there is no international law that protects the human rights in cyber which makes the situation worse in cyber space, and the violations might increase in the near future because people are becoming more and more dependable on cyber space specially in their jobs, because meanwhile most of the jobs can be done remotely, and we cannot forget Corona epidemic when people obliged to do their jobs from distance to avoid direct contact with people, also there are scientific researches 'expectations about the infectious diseases which are going to increase in the future, for that reason most of the businesses will let their employees to work from distance.

The best solution to protect people in cyber space is by providing the cyber with governance which is clearly missing in the space, and by the implementation of governance, human rights will automatically be protected in the space because cyber governance will be as the international law in cyber space.

Cyber space and governance:

Protection the cyber space is not an easy job because the used cyber protection systems proved their ineffectiveness in securing cyber space, for that reason the cyber needs new methods of cyber security, and the methods must be practical and dynamic and the methods must be experienced at the national and global level.

The cyber space was described by many experts as:" environment without borders and free from state control"[24], this description is very meaningful and it explains the problem that we are facing in cyber space which is the absence of control which means governance, so the governance is missing in cyber space.

Moreover, the environment without borders means that there are no borders in cyber space, which isalso considered a problem because until now cyber space is not identified as global common place in where we can find norms and rules that are globally approved.

Global Common place normally is a place with norms and rules and for example The global common contains about 75% of the earth's surface including the high seas and Antarctica as well as the atmosphere and some argue the outer space.

Each country is obliged by those rules and norms in global common place, which cannot be crossed them and those global norms and rules must be applied in cyber space, because cyber space does not have norms and rules based on the international standards that protect the user form any attack, and cyber governance is the only mean that can provide the space with international norms and rules.

One of the organizations that was created to govern cyber space was the nonprofit organization ICANN (Internet Corporation for Assigned Names and Numbers) which founded in USA in 1998.

ICANN has a board of directors from the private and public sector but with insignificant role for the foreign countries in the organization which actually weakened the effectiveness of ICANN in cyber space governance.

ICANN had a great leverage on cyberpolicy making, besides ICANN solved more than 10,000 disputes among cyber users, and the disputes were related to domains names and trademarks[25].

ICANN was a major player in e-commerce development but despite all those achievements that had been made by ICANN many countries around the world were against ICANN because they considered it as an American privilege, because the board of directors in ICANN does not represent all the countries in the world, even some countries wanted UN to take the responsibilities of cyber space which means that governance problem still exist.

There is another organization considered also as cyber governor which is IETF (Internet Engineering Task Force) which is responsible for architect the internet communication system.

IETF is an open and flat organization that contains the designers, operators and vendors; IETF develops and designs the architecture of the internet's communication system.

IETF is more in coding as the engineers in IETF write codes which is fundamental in cyber space and cyber security, for that reason coding is law in cyber space according to Professor Lawrence Lessig in Harvard[26], because those codes can be very critical to the cyberusers if the codes were written without moral standards, for example in USA the WLAN 'codes were written based on the concept of anonymity and anarchy of the U.S standard[27].

[22]" (RIAA 2011) (Cyfirma 2023) Recording Industry Association of America", June 9,2011, https:// www.riaa.com

[23] "China IP Theft Report", Cyfirma, June 6,2023, https://www.cyfirma.com/

[24] Andrew Murray, "the regulation of cyberspace: control in the online environment", Routledge,October 10 ,2006, http://www.routledge.com/The-Regulation-of-Cyberspace-Control-in-the-Online-Environment/Murray/p/book/9780415420013

[25] Murray, "ICANN bylaws", ICANN, October 15,2013,http://www.icann.org/en/about/governance/bylaws.

[26]Tian Ma," Is code Law", Legal Tech Blog, November 9,2021, https://legal-tech.blog/

[27] Scott J.Shackelford," Managing Cyber Attacks in International Law, Businesses and Relations In Search of Cyber peace",(USA: Cambridge University Press,2014)P.40.

There is a partnership between ICANN and IETF in inter organizational communication and cooperation in cyber space, and both organizations had an official discussion on cyber governance [28], but the implementation of internet governance crosses beyond standards of institutions as ICANN and IETF because we need to include in internet governance:" private industry policy, national policies, international treaties and the design of technical architect."[29]

There was also an attempt from the UN to take the custody of internet governance which is the best solution and this led to the creation of many departments inside UN such as international telecommunicating union (ITU) UNESCO, the UN conference on trade and development (UNCTAD), and the newest one the internet governance forum (IGF), but there was a tension over the authority of internet governance between the UN, the USA and other internet governance stakeholders.

A general conference in November 2015 for UNESCO with the presence of 195 members states mentioned the importance of internet universality[30], but many members in the conference expressed their worries about internet governance, unitary regime may in fact be an impossibility[31],both the world summit on the information society (WSIS) and working group on internet governance (WGIG) concluded that there might be disagreement about the internet governance with the American's government which is controlling the domain names and critical internet resources through ICANN.[32]

The cyber space is a huge place without control and there is no international law that can protect the user from any human rights violation, and with only the good governance to the cyber space we can guarantee the safety of the space, also the implementation of governance will contain steps and processes to maintain the best version of cyber governance which we will reach it in the findings.

2. Methodology

In the research we used mixed method approach which are the quantitative method and the qualitative method.

We used the quantitative method to show some statistics numbers about the cyber-attacks , but qualitative method was mainly used in the paper, and we used also the deductive reasoning.

1) The deductive reasoning

Cybercrimes are causing human rights violations in cyber space and it is a global problem and most of the countries are suffering from it, and as long as there is no cyber governance that can provide the space with international rules and procedures which can protect the users from any human right violation as more as cyber-attacks we will have in cyber space.

The cyber governance will provide the space with norms and rules which will represent the international law in cyber space and the international law will put restriction on any human right violation.

The implementation of cyber governance will definitely decrease the number of cybercrimes because the space will be highly secured technically and legally.

2) The qualitative record keeping:

It is obvious in the paper as most of the examples were already existing reliable resources and there were many online articles which were taken from New York Times, Aljazeera, NPR and others.

3) The qualitative case study method:

We used in the paper many references from books like "Managing cyber-attack" book for Scott J. Shackelford, also "what if we all governed the internet" for Anri Van Der Spuy and other kinds of books which all considered as case study method as the references were specifically made for missing cyber governance case.

3. Findings

The absence of global cyber governance increased the number of cyber-attacks because the role of governance in cyber security is basic, besides the role of governance in cyber space could be divided into two parts which are technical governance and ethical governance as internet governance decisions includes both scientific perceptive and social studies of power and authority.

Technical governance role:

It is related to the coding and the design of the cyber space as the hackers were cracking the cyber space because of the bumps found in coding, which meant that the weakness was in writing the coding, and there were many types of errors in coding as like missing brackets and entering incorrect variable names, and these kinds of errors were very useful for the hackers and they could penetrate easily the systems.

Governance could protect the cyber space technically because coding cybersecurity was the responsibility of cyber governor and any written code in cyber security should be grounded on rules and standards that protect the users from any harm, so cyber governors could assure to provide written code in cyber security with high level of inspection to any possible attack.

[28] Steve Crocker," ICANN's relationship with the IETF", ICANN, February 19,2014, https://www.icann.org/en/blogs/details/icanns-relationship-with-the-ietf-19-2-2014-en

[29] Laura, Denardis," the Global War For Internet Governance",(USA: Yale University Press,2014)p.19.

[30] Anri Van Der Spuy," what if we all governed the internet",(France: United Nations Educational ,Scientific and cultural organization,2017)p12.

[31] Mueller, M. & Wagner, B." Finding a Formula for Brazil: Representation and Legitimacy in Internet governance",Internet governance, November 1,2014, https://www.internetgovernance.org/pdf/MiltonBenWPdraft_Final.pdf

[32] Anri Van Der Spuy," what if we all governed the internet",(France: United Nations Educational ,Scientific and cultural organization,2017)p17.

Safeguarding the addressing system in cyber space as well as DNS is one of the priorities in cybersecurity governance.

Cybersecurity governance techniques should verify the users, guard the credibility of the content and defend the cyber space from any attack as like DOS, worms and other security threats.

The ethical governance

It meant policymaking in cyber space which produced the rules and laws that would definitely eliminate cyber-attacks because there is no international law that could protect the users in cyber space from the attackers and each country followed its local law regarding any cybercrime , and this made confusion in any case related to cyber-attacks specially in international level , sometime there would be a cyberattacks to many different users in many countries and if the harmed users in those different countries wanted to complain to the courts , each court might have a different preview about the attack and the judgment would be different from court to court :" governance is traditionally understood as the efforts of the sovereign nation states to regulate activities within or through national boundaries"[33], and as we said previously the only international law or official treaties that could protect users in cyber space is Tallinn but it is only valid during the cyberwarfare.

The main responsibility of cyber governance was to produce an international norms and rules in cyber space, and all the states of the world should follow those rules and procedures because it would be obligatory, and any cyber-attack should be investigated it, and it should be regulated it depending on those international norms and rules, also the governors should assure for the alignment between the applicable international norms and the human rights.

Cyber governor should be classified cyber space as common space and that would enrich the cyber space with more international rules and it would help the countries to know their legal responsibilities toward any cyber-attack which was happening in their territories.

UN should lead the governance in cyber space and UN should produce the norms and rules concerning cyber space , and there should be only one department that is responsible for cyber space and governance ,thus right now there are many departments in UN as we mentioned previously which were specialized in cyber governance, and always the various number of departments with multi decisions would take their time to make any decision and sometime decisions would interfere with each other and this made a confusion in decision making, and this would ruin the process of any mission related to governance , also cyber governance is sensitive process requires a quick and one time decision because cyber-attacks are developing quickly and there must be one department with only one decision that could deal with any attack situation.

4. Discussion and Conclusion

The absence of cyber governance is the main reason of why cyber-attacks are happening against millions of users, because the Hackers are misusing cyber space, thus it is an empty space without rules and limits and only the cyber governance can protect the cyber from the hackers.

Cyber governance must be created based on rules and moral standards, also cyber governors must protect the space with high and unpenetrated coding systems in cybersecurity, besides classifying cyber space as common space is a part of internet governance which will help a lot in the countries and the states in all the world to know precisely their responsibilities toward any attack will be made in their territories of authorities , and the governance must be like the international law that protects the users from any human rights violations as like privacy, freedom of expression and intellectual properties ,and unfortunately those violations are caused by both individuals hackers and soldiers hackers who represent officially their nations and states.

The result that we reached in the paper is similar in some points to the declaration of principles in the WSIS (World Summit on the information society) of Geneva 2003-Tunnis 2005.

It is mentioned in the WSIS principles that the role of UN is necessary in the development of anything related to internet governance, and in the paper we can found that the UN must be the governor of cyber space and UN must be the guard of internet governance , furthermore in WSIS declaration there is a statement which is about UN role in preventing the use of cyber space for criminal and terrorists purposes and the human rights must be respected[34], also we mentioned this in the research about the important role OF UN in producing norms and rules which can protect the cyber space from cyber-attacks, and the norms and rules must be the international law that is responsible for human rights protection.

There is difference between the declaration and the paper which is obvious in the principle number 10 of the declaration which is:" we are also fully aware that the benefits of the information technology revolution are today unevenly distributed between the developed and the developing countries and within society[35]".

In the paper we mentioned the important role of classifying the cyber space as common place, which will fairly distribute the benefits of information technology among the developing and the developed countries.

Furthermore, the internet governance was only given few principles in the declaration which are not enough, because the value of internet governance in protecting the cyber

[33] Laura, Denardis," the Global War For Internet Governance",(USA: Yale University Press,2014)p.8.

[34] "Declaration of Principles Building the information society: a Global Challenge in the new Millenium", World Summit on The Information Society, December 12,2003, https://www.itu.int/net/wsis/docs/geneva/official/dop.html

[35] "WSIS outcome Documents December 2005",(Geneva: International Communication Union (ITU),2005)P.11.

space is considerable, and in the paper, we can find more details about the internet governance that prove the credibility of internet governance in protecting the cyber space from the hackers.

The only limitation that we have in the paper is that internet governance needs to be discussed by details , because it is a huge process needs a lot of efforts from private and the public sectors, also it needs people with high proficiencies in law and coding who can figure out all the weaknesses in cyber space, so the research needs a work group of professionals in coding and international law firms in order to get an accurate transcript of internet governance , and this is difficult to happen thus the research will be very costly and it will take a lot of time.

The results in the paper are very simple and all the people can understand them easily and you do not need to be expert in cyber space to understand the results.

The researchers in the field of cyber governance can understand that there must be an alliance between the public and the private sectors to produce a proper cyber governance, as there will be a conflict of interests if there is nocooperation between the two sectors.

Cyber space considered as public place and it is the right for all the people in all around the world whether they are poor or rich to use the space freely, and the human rights activists should emphasize on the authorities and the UN to classify the cyber space as common space.

Furthermore, Cyber security and the safety of users in cyber space were discussed briefly in Tallinn manual, and the manual prevents the cyber-attacks against the civilians during warfare, but there are points of weaknesses in the manual which degrade the power of Tallinn manual in cyber space. For instance, the manual did not cover many important crimes that are happening daily in cyber space which are related to human rights as like theft of intellectual properties and cyber espionage.

In the paper it was clear that cyber espionage is a form of cyber-attacks and it is considered as human rights violation because it is related to the human's privacy, also we mentioned cyber-attacks against the intellectual properties in cyber space and it is a human rights violation, besides both crimes can be eliminated by applying the cyber governance which will be based on international law and human rights.

Cyber governance is a necessity in cyber space to reduce the volume of cyber-attacks, besides cyber governance must be created and approved by all the nations in all around the globe.

Cyber governance is norms and rules that are similar to international law, and the norms and rules must be made on high standard of morality and all the nations should follow them typically because any inaction from the nations in applying the rules and norms will cause many problems in cyber space as human rights violations.
Human rights violations are happening in cyber space because of the continuous cyber-attacks that do not respect human's privacy and intellectual properties and only with cyber governance we can reach the peace in cyber space.

References

[1] 2016. *Aljazeera* . January 25. www.aljazeera.com.
[2] B, muller M & Wagner. 2014. *Internet Governance* . November 1. www.internetgovernance.com.
[3] Balleste, Joana Kulesza & Roy. 2016. *Cyber Security and Human Rights in The Age of Cyberviolence* . USA : Rowman & littlefield.
[4] Bonderud, Douglas. 2023. *Security Intelligence* . August 20. www.securityintelligence.com.
[5] 2023. *Clearias* . January 8. www.clearias.com.
[6] 2023. *Cyfirma.* June 6. www.cyfirma.com.
[7] Denardis, Laura. 2014. *The Global War For Internet Governance* . USA : Yale University Press.
[8] n.d. *ECHR.* www.echr.coe.
[9] 2012. *Economist* . May 12. www.economist.com.
[10] 2012. *Economist* . May 12. www.economist.com.
[11] Ishani, Maryam. 2011. *NPR.* January 28. www.npr.org.
[12] J.Shackelford, Scott. 2014. *Managing Cyber Attacks in International Law.* USA: Cambridge University Press .
[13] James, Nivedita. 2023. *90's cybercrime statistics 2023,cost,industries and Trend.* October 24. www.getastra.com.
[14] Jamieson, Kathleen Hall. 2020. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President.* USA : Oxford University Press .
[15] —. 2020. *cyberwar: how Russian Hackers and Trolls Helps Elect a Preident.* USA : Oxford University Press .
[16] M.West, Catherine Howell & Darrell. 2016. *Brookings* . November 7. www.brookings.edu.
[17] Ma, Tian. 2021. *Legal Tech Blog.* November 9. www.legal-tech.blog.
[18] Morgan, Steve. 2020. *Cyber Security Ventures* . November 13. www.cybersecurity.com .
[19] Murray. 2013. *ICANN* . October 15. www.icann.org.
[20] Murray, Andrew W. 2006. *Routledge* . October 10. www.routledge.com.
[21] N.Schmitt, Micheal. 2013. *Tallin Manual of The International Law Applicable To Cyber Warfare.* USA: Cambridge University Press .
[22] Parsons, Ken Dilanian & Christi. 2013. *Los Angles Times* . February 20. www.articles.latimes.com.
[23] Perlroth, Nicole. 2013. *New York Times* . January 30. www.nytimes.com .
[24] 2011. *RIAA.* June 9. www.riaa.com.
[25] Satter.R.Donn.J, Day,C. 2017. *Associated Press* . November 3. www.bloomberg.com.
[26] Spuy, Anri Van Der. 2017. *What If We all governed the Internet* . France : United Nations Educational Scientific and Cultural Organization .
[27] Stengel, Richard. 2019. *Vanityfair.* October 6. www.vanityfair.com.
[28] 2023. *Surfshark.* November 20. www.surfshark.com.
[29] 2003. *World Summit on The Information Society* . December 12. www.itu.int.
[30] 2005. *WSIS Outcome Documents December 2005.* Geneva: International Communication Union .
[31] Younger, Nick. 2020. *whistle blowers* . December 09. www.whistleblowers.org.