



THESSISMUN

2008

THESSALONIKI INTERNATIONAL STUDENT
MODEL UNITED NATIONS

United Nations General Assembly 3rd Committee Topic Area A

Cyberspace and Human Rights, regarding:

- a) protection of personal data,*
- b) crime syndicate,*
- c) national sovereignty,*
- d) civil liberties*



UNIVERSITY OF MACEDONIA
THESSALONIKI, GREECE

WWW.UOM.GR/MUN - WWW.THESSISMUN.ORG



Introduction

Cyberspace has rapidly evolved during the last decades. Development has led to a continuously expanding technology, which has a vast field of application. To begin with, cyberspace is a reality that needs to be defined, in order to understand this new notion and the domains that are affected or altered by it. Many of the answers given can only be empirical, for the time being, since the comprehension of cyberspace is ongoing. The procedure of understanding the tools, the modifications, the conditions and the effects of cyberspace are fundamentally connected with natural law and has to be explained under the basic needs of all subjects connected with it, either with tight or with loose bonds. This is the reason why cyberspace needs to be seen most and above all under a humanistic approach. Human rights, individual and collective ones, can easily be violated in a newly-settled environment, where morals, ethics, tradition, legislation and a variety of interests clashing each other create an unsafe 'topos' for its users.¹

Internet's eutopia or dystopia² relies on the attention paid to the circumstances and United Nations is the only institution in full capability of producing the means as to guarantee cyberspace's peaceful uses. The United Nations, while expressing the scopes of international community, can embrace this new dimension and regulate measures trustworthy and liberal simultaneously, for the shake both of its member-states and for individuals.

For this reason, it is necessary that cyberspace's applications are well interpreted, in order to crystallize the customs which follow its functioning and create a proper legal framework. The questions arising are of great significance as every conflict and dispute which already exists in "real world" is transferred to cyberspace. Civil liberties and specifically personal data have to be protected, so as to ensure that individuals are not threatened in any possible way. On the other hand, since education and the army have entered in the reality of cyberspace, nation-states are

¹ Roger Hurwitz, "Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace", Vol. 28, No.6, Contemporary Sociology, (1999), 655-661, at 655.

² Yuan Shu, "Information Technologies, the U.S. Nation-State, and Asian American Subjectivities", No.40, The Futures of American Studies, (1998), 145-166, at 145-147.



deeply involved in cyberspace technology and have to create all the necessary mechanisms for safeguarding their systems and their nationals too.

Cyberspace is just one of the modes to see through globalization's spectrum, thus greatly connected with the reform of societies, the political formulation not only of Western democracies, but also of all kinds of communities. Many believe that, if it weren't for the internet, Western democracies wouldn't have been so successful, since fast reach and rapid response time (time compression) lead to the revitalization and the fluent ventilation of the world community, easing down the hegemonic propensities of the centres of power and promoting a non-hierarchical structure, where institutionalism is enhanced and states are no longer so important factors in the international system, as to dominate upon transnational initiatives and generally individuals' intentions. The internet supports communications which are counter hegemonic, thus enhancing its use by activists (labor, animal-rights) or by organizations (environmental, women's) etc.³

Access to the internet – Equality

Personal rights of the individuals constitute a very crucial topic that has to be thoroughly examined within cyberspace's frame. What comes first is the need to shape the profile of its users. Surprisingly, this is the point where human rights' violation starts. The use of the internet, although not posing any kind of national or territorial borders, is prohibited for some groups of people. Access to the internet has some very strict prerequisites, such as the ability to write and read (the ability to see as well - impairment of vision) and the financial ability to cover the costs of all the hardware and software necessary for networks. Illiteracy and poverty are the two main barriers that deprive some people from their right to access the internet and their right to communicate in general.⁴ After having mentioned the above, it is obvious that cyberspace has

³ Paul Adams, "Network Topologies and Virtual Place", Vol.88, No.1, Annals of the Association of American Geographers, (1998) 88-106, at 100-102.

⁴ *ibid.*, at 101-103.



been created in order to serve the interests of developed countries, where there is a high budget spent on technology and the appropriate infrastructure to support every new finding.

If we were so to characterize this situation, it can be said without any hesitation that internet, from its very starting point, is in clash with the principle of equality. As a matter of fact, people are divided in two categories: the ‘netizens’ and the citizens.⁵ The ‘netizens’ are most times wealthy and educated. In the United States only 5% of Hispanic households have access to the internet and only 14% of African-American households own a personal computer. African-Americans are 5.3% out of the entire American population accessing the internet. There are many who argue that the internet was just an American subculture, with distinct advantages for the white audience.⁶

The statistics are even worse when it comes to developing countries. In Africa, the first place with access to the internet was a cyber cafe with ten terminals, in the capital of Senegal, in 1996.⁷ The so-called ‘white domination’ of cyberspace resulted in the construction of Pan-African sites of resistance. There are portals which promote nationalism both on a cultural and on a political level. The empowerment of the Black community is in the heart of these web-pages. Some times, there are even protests organized via the internet and most specifically through mail lists gathered by these portals. There is a movement aiming to the “liberation” of the black population worldwide, which forms strategic plans, so to improve their position on the internet.⁸

Cyberspace is still not accessible to the Third World. Taking into consideration the exception of some Newly Industrialized Countries (NICs), such as South Korea, Singapore, Hong Kong and Taiwan the rest of the member-states do not have cyber knowledge.⁹ Under the present conditions there is the creation of a bipolar system, where there are the countries where

⁵ Roger Hurwitz, “Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace”, Vol. 28, No.6, *Contemporary Sociology*, (1999), 655-661, at 655.

⁶ “Black Higher Education on the World Wide Web”, No.14, *The Journal of Blacks in Higher Education*, (1996-1997), 72-74, at 73.

⁷ *ibid.*, at 74.

⁸ Colin A. Beckles, “Black Liberation and the Internet: A Strategic Analysis”, Vol.31, No.3, *Journal of Black Studies*, Special Issue: *Africa: New Realities and Hopes*, (2001), 311-324, at 313.

⁹ Gerard Sussman, “Urban Congregations of Capital Communications: Redesigning Social and Spatial Boundaries”, No.60, *Globalization?*, (1999), 35-51, at 43-44.



cyberspace has been introduced and the rest where there is not such an opportunity. Transnationalism is shortened and reaches fewer places. Political writers refer to the classic Marxist notion of class struggle and believe that it has been transferred to cyber-reality.¹⁰

Discriminations

Racial discriminations continue to play a very important role even in cyberspace. It is difficult to find out which are the subject positions that cyberspace allows exist and which are the deprived ones.¹¹ The situation cannot be easily depicted. When the technology of telecommunications began to evolve there was the belief that preconceptions regarding some targeted groups of people, would start to disappear, due to the creation of interaction and the greater availability of information and knowledge provided. The truth is that internet is charged for racist, sexist and homophobic reproductions.¹²

There are nations, or even ghettos, being constructed in the digital world. Since personal interactions are based on self-disclosed facts and stereotypical questions, there are linguistic borders, borders of race, or political standpoint. Discrimination brings to the front matters of access, privilege and power. Proliferations seem to be institutionalized. California's anti-affirmative action on legislation delimiting the rights to access to employment and education is just an example of the already mentioned.¹³

There are undoubtedly links between racism and poverty and discriminations are performed both legally and nationally. The freedom that internet reflexes is given only to already powerful groups, while households that are not wired get marginalized, forming a new

¹⁰ Yuan Shu, "Information Technologies, the U.S. Nation-State, and Asian American Subjectivities", No.40, *The Futures of American Studies*, (1998), 145-166, at 151.

¹¹ Christina Elizabeth Shape, "Racialized Fantasies on the Internet", Vol.24, No.4, *Institutions, Regulations, and Social Control*, (1999), 1089-1096, at 1089.

¹² *ibid.*, at 1093-1094.

¹³ *ibid.*, at 1091.



“electronic ghetto”. Marginal groups are also deprived of their *right to information*, a violation which weakens their position, since power is counted as on the fields of information.¹⁴

Cyberspace is a new factor which leads some historically discriminated groups to be oppressed. Asian-American subjectivities exist through role-playing computer games, which recycle traditional and cultural stereotypes, being frequently offensive to Eastern populations and thus promoting misunderstandings between nations and cultures. Multiculturalism is targeted by cyberspace’s rapid evolvement which has no pointed direction. The inherent *right to diversity* is violated and there is moreover, the creation of non- healthy role-models for the majority of the users.¹⁵

China and civil evolution

The example of China, though, shows the advantages of cyberspace and the positive effects that it brings to societies. Internet is met to be one of the major factors that have helped China to move towards democratization and a productive and well functioning civil society. The field of civil liberties has been on an elaboration process, since cyberspace has offered great chances to the Chinese population.

Internet provided China with direct communication with the other states of the Pacific, as well as with the Western societies. China, being the centre of the production of almost all goods, had to be connected with all its allies so as to satisfy its interests. In this case, cyberspace helped to the organization and better structure of the country’s interior, while offering job positions and employment opportunities to many people who entered the network industry. Furthermore, cyberspace has helped the country on the grounds of production as well, since knowledge regarding communication technologies was better absorbed by the population.

¹⁴ Paul Adams, “Network Topologies and Virtual Place”, Vol.88, No.1, Annals of the Association of American Geographers, (1998) 88-106, at 101.

¹⁵ Yuan Shu, “Information Technologies, the U.S. Nation-State, and Asian American Subjectivities”, No.40, The Futures of American Studies, (1998), 145-166, at 151-155.



In the meantime, cyberspace has greatly helped the population to secure themselves from oppression deriving from governmental decisions and laws, as it gave publicity to mistreatments, abuses and violations that some groups have been suffering from, for a long time.¹⁶

Free market- consumers

The western model though governs cyberspace in almost every aspect. Many concerns have been expressed during the last decades, regarding consumption principles promoted through the internet. Some believe that consumer sovereignty is the main political value in cyberspace.¹⁷ Generally speaking, cyberspace can be defined as the global domination of free-market capitalism.¹⁸ Production, consumption, free market and competitiveness are the groundwork upon which cyberspace lies. It has to be taken under consideration that cyberspace is a modern, thus expensive industry. Advertisements, that almost every user has encountered, are one of capitalism's signs that mark modern societies and as a matter of fact internet too. What matters, is that these advertisements appear most times on the user's screen without its prior permission.

This is a severe *violation of the user's personality*, since he has not the opportunity to choose the information that appears on the screen and most importantly there is lack of response to these advertisements, which tend to surprise the individuals and consequently lead them to purchases governed not by reasonable thinking and objectively established needs. Individuals face an inevitable universalization of humane desires, which on the contrary particularize the culture which dominates cyberspace.

¹⁶ Guobin Yang, "The Co-Evolution of the Internet and Civil Society in China", Vol.43, No.3, Asian Survey, (2003), 405-422, at 408-414.

¹⁷ Roger Hurwitz, "Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace", Vol. 28, No.6, Contemporary Sociology, (1999), 655-661, at 657.

¹⁸ David Leiwei Li, "Introduction: Globalization and the Humanities", Vol.53, No.4, Comparative Literature (2001), 275-282, at 275.



Having mentioned some of the individual human rights that can be easily violated on the grounds of cyberspace, it is time we examined and interpreted some latest behaviors that the users adopt, which pinpoint the dangers of cyberspace.

It is true that the internet offers employment opportunities to many civilians. The *right to employment* seems to be well served and functioning in every possible manner. It has to be underlined though, that the right to employment has a negative meaning as well, functioning alongside with the positive context of it. A right's negative meaning is the individual's ability to either use it or not. In the last years, it has been recorded that many corporations demand from their employees to provide their work through the internet. Telework¹⁹ is a new trend that has great disadvantages as far as it concerns the individual's income. Another practice often used by corporations is the employment of individuals who possess their own hardware. This practice takes away from many people the opportunity to be selected.

Many strange and eccentric behaviors have emerged on cyberspace. The phenomenon of "cycling through" describes a person's ability to adopt many identities in the same time and perform as several different persons,²⁰ just like the story of Dr. Jekyll and Mr. Hide. This conduct is pathogenic as it reflects people's desire to fit into groups and feel accepted. Cyberspace does not obviously activate all human senses.

As a result, virtual reality increases the danger of indeterminacy and loss of the user's identity. Social life through the internet avoids confronting identity and determination of the individual. The *people's right to self-determination*, not on a collective basis but on a personal one, is definitely violated. Unfortunately, this violation cannot be charged or even attributed to someone and therefore it is perceived as a minor effect to the individual, as a real situation that has no further consequences and lacks indeed in terms of meaning.

¹⁹ Barry Wellman; Janet Salaff; Dimitrina Dimitrova; Laura Garton; Milena Gulia; Caroline Haythornthwaite, "Computer Networks as Social Networks: Collaborative Work, Telework and Virtual Community", Vol.22, Annual Review of Sociology, (1996), 213-238, at 218-219.

²⁰ Paul Adams, "Network Topologies and Virtual Place", Vol.88, No.1, Annals of the Association of American Geographers, (1998) 88-106, at 100.



Protection of personal data

Personal data is the hard core of the information which constitutes the identity of every person. Personal data is perceived as the category including the primary, the fundamental human rights which are the precondition to the right to self-determination. Therefore, it is apparent that their protection is of great necessity for every single individual. Regrettably, their violation is the most frequently occurring in cyberspace. Cyberspace, due to lack of legislation and lack of harmonization of the existing legal frameworks, is a field where such violations can be easily carried out without even being understood by the victims, which fall short of receiving protection. What needs to be highlighted, though, is the fact that personal data is threatened not only by the private sector, but also from national governments which attempt to secure their network systems against individuals, who may jeopardize them.

The already existing legal instruments are a compromise between states' interests. The most important ones are the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (adopted by the Organization for Economic Cooperation and Development, OECD, 1980) and the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (adopted by the Council of Europe, 1981). These papers are the foundation of the protection of personal data as they shape up the most essential, the key principles to address the topic. Some of the principles that can be easily extracted from within the text are collection limitation, purpose specification, use limitation, security safeguards, openness and accountability. These rules apply to the collection, storage and processing of personal data. The solidarity of the aforementioned is surpassed by the government's interest in accessing, sharing and storing information.

These interests are legitimized under the principles of national security, good faith and political commitment. The application of the above covers areas such as travel and communications, taxation and terrorism. Personal data is collected when passengers travel abroad (mostly via airplanes), under the pretext of facilitating travel services.²¹ Data collection

²¹ Mary Rundle, "International Personal Data Protection and Digital Identity Management Tools", Identity Mashup Conference, Berkman Center for Internet and Society, (Harvard Law School, 2006), background paper.



has been even more systematic after 11/9. Since then, personal data is used in order to reach terrorists, or their financial supporters. Last but not least, personal data is used so as to impose taxes on activities of international commerce. Personal data's collection is sometimes legitimized on the grounds of combating corruption.

Due to the fact that social relations have been globalized and lifted from the local contexts of interaction, information sharing is another measure of safeguarding national political orders.²² In China and Singapore the governments require from the users to state which are the activities they undertake, when in the internet.²³ Other governments, typically and externally more liberal, have made efforts to police cyberspace and create restrictive legislation.

The private sector, on the other hand, has made it easier to violate individuals' personality by using identity information, since technology companies have invested great amounts of money in the creation of digital identity management tools.

Cyberspace's implications

Cyberspace's social implications can be easily categorized and named, but the acceptance of their existence and their validity is a question that needs to be carefully answered. First of all, there is the *principle of equality*, which has already arisen. Inequality dominates networks in many different aspects (examples of racial and other kinds of discriminations). To continue, there is the notion of a *global community*, which is always connected with *social capital*. Once again, cyberspace technology does not allow the international community to be treated as the same to the cyberspace community, whereas social capital follows neo-liberalistic values. *Political participation* is another social repercussion.

Debate over this point has taken wide publicity during the last few years, especially on democratic states, where mass media are of capital importance. The internet is one of the tools

²² *ibid.*

²³ Roger Hurwitz, "Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace", Vol. 28, No.6, *Contemporary Sociology*, (1999), 655-661, at 656.



used, so to influence the public opinion regarding the electoral results. Cyberspace has undoubtedly, though, favored the rise of *institutionalism and the nation-state's decline*. Ancient regimes are quickly replaced by institutions of different origins, with different scopes and perspectives and various means of interaction. Cyberspace has multiplied the subjects of the international order. Non-governmental organizations are more flexible than states and thus easily adapting to the new reality and better responding to its demands.

Last but not least, *cultural diversity and participation of civilizations* in the internet is an intricate element to establish. Diversity and multiculturalism, although not in the front of the world's interests are of significant value for the global community.²⁴ Cyberspace is once again following western norms, as linguistic barriers and liberal conceptions rule the network.

The procedure of democratization of political communities- participation

Cyberspace also affects the structure of societies and gives a new meaning to many collective human rights. As it has already been mentioned political communities are under a revitalization process, since cyberspace is a new tool to be applied in their forming. Al Gore (1995) and Bill Gates are the first ones that have predicted the democratizing potential of the internet.²⁵ Nowadays, that the nation-state concept is weakened, due to the neoliberalistic economic trends and also due to individuals' disorientation,²⁶ cyberspace may enhance the governments' surveillance capabilities.²⁷ The political culture of cyberspace is on a sprouting point. Political participation of its users is a process developing the last few years.

Participation shows that cyberspace reflects democratic standards. But do the requirements for a digital democratization exist? Democracy might be deliberative, partisan, or monitorial.

²⁴ Paul DiMaggio; Eszter Hargittai; W.Russell Neuman; John P. Robinson, "Social Implications of the Internet", Vol.27, Annual Review of Sociology, (2001), 307-336, at 307.

²⁵ Colin A. Beckles, "Black Liberation and the Internet: A Strategic Analysis", Vol.31, No.3, Journal of Black Studies, Special Issue: *Africa: New Realities and Hopes*, (2001), 311-324, at 311.

²⁶ David Leiwei Li, "Introduction: Globalization and the Humanities", Vol.53, No.4, Comparative Literature (2001), 275-282, at 277.

²⁷ Roger Hurwitz, "Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace", Vol. 28, No.6, Contemporary Sociology, (1999), 655-661, at 655.



The type of deliberative democracy would encourage chat rooms, fora and other places of interaction. It fails to be applied though, as censorship prohibits users from making negative or black comments and the rules of order provided are very strict. Partisan democracy cannot effectively operate too, as candidates have websites where the users cannot interact and actively participate. Thus, individuals become passive consumers of political information.

Monitorial democracy has been functioning more successfully. Although, communities of common political interests, alerts and online protests have been fruitfully organized many times, the monitorial model is threatened by the individuals' little knowledge on the issues of argumentation.²⁸

Cyberspace and National Liberation Movements (NLMs)

As it has already been mentioned, cyberspace encourages institutionalization and it offers freedom of speech to anyone who might be deprived of this right. National Liberation Movements search for a wider acceptance through the internet. The Zapatistas in Chiapas (Mexico) is the most famous example of a national liberation movement which organized its actions through the internet. They tried to webcast messages all over the globe in order to receive financial assistance and substantive support.²⁹ Despite the fact that the revolutionaries were not able to have direct access to the internet, they effectively promoted their local reality and fought for justice.

Globalization was modified into a tool which served this group and, according to many writers, led Mexico to democratization. What has definitely to be mentioned is the fact that the revolutionaries were opposed to the Mexican government because it has applied neoliberalistic policies and it has introduced capitalistic free market reforms, some general ideas also endorsed by cyberspace. Moreover, the Zapatistas struggled for a more democratic government, which would not use force to resolve civil turbulences and to confront its domestic conflicts. Last but

²⁸ *ibid.*, at 658-660.

²⁹ *ibid.*, at 656.



not least, the movement tried to draw awareness regarding the rights of indigenous people and emphasizing the need to be protected.

The movement's demands were expressed by many means, but most importantly through a website, constructed in 1996 and named the "New Aguascalientes", where all the activists were free enough so to blame the government's actions and most specifically the use of force against civilians. Their manifestations were translated and posted in the website. Debates, chat forums, mail lists and other forms of cyber-communication helped the Zapatistas establish their arguments and reach their political goals. As it was successfully pointed out, it was a cyber-'war of positions' against Mexico's leaders and ruling class, with worldwide recognition.³⁰

There are other circumstances as well, where revolutionary groups found a cyber-shelter. For example, the B-92 Serbian radio-group was broadcasting its alternative positions both on the radio and also through the internet. The responsiveness that webcasting received led the Serbian authorities to threaten the crew of the radio station that they would be arrested and to lock them out of the studio.³¹

Institutionalization, though, can work alongside with governmental and national positions, in cases where there is a common target. One of the most typical examples is the one of Saudi Arabia. It is a state which perceives itself as the defendant of the Eastern world against the Western corruption, although under significant American influence in many of its provinces, rich in oil. Just like it has happened with the Zapatistas revolutionary group, groupings opposing to globalization, use one of its more powerful instruments in order to combat it. They fight against globalization, by rejecting localization at the same time. It is of capital importance to state that in this case not only groups of individuals, but also the official governmental sites and its assents declare their grievances as far as it concerns globalization and its consequences.³²

³⁰ Chris Gilbreth; Gerardo Otero, "Democratization in Mexico: The Zapatista Uprising and Civil Society", Vol.28, No.4, Latin American Perspectives, Mexico in the 1990's: Economic Crisis, Social Polarization, and Class Struggle, (2001), 7-29, at 8-14.

³¹ Roger Hurwitz, "Who Need Politics? Who Needs People? The Ironies of Democracy in Cyberspace", Vol. 28, No.6, Contemporary Sociology, (1999), 655-661, at 656.

³² Mamoun Fandy, "CyberResistance: Saudi Opposition between Globalization and Localization", Vol.41, No.1, Comparative Studies in Society and History, (1999), 124-147, at 125-127.



More or less, Kuwait³³ is nation-state which follows the same policy regarding the internet. The common element between these two countries is that they share relative civilizations, which they feel are under a threat that can be understood with difficulty. The official governments act like liberation movements, which try to free themselves from an invisible captivity. Their opposition, though, against globalization and cyber-reality initiates from the fact that there is significant and unavoidable Western influence on their territories.

Cyberspace and the “clash of civilizations”

The “clash of civilizations” is a famous and well-known concept of Samuel Huntington, also applicable when referring to cyberspace. Cyberspace has failed to grant the idea of planetarianism and has become many times an area of discriminations. The protest of groups of peoples who are deprived of either their individual or their collective human rights is often taking place in the internet. Fundamentalists, from the “Front National” in France, to the Christian fundamentalism in the United States and the “Islamic Brothers”, try to find supporters through the internet.

As their activities are most times illegal, they are deprived of access to other forms of communication.³⁴ Fundamentalism, as an expression of authoritarianism is an obstacle to democratization and good governance, which are the basic tools in order to reach a global community, where all people enjoy the primary human rights. Discriminations can be based on religion, race, language or culture.

All of these can be explained under the umbrella of clash of civilizations and they may lead to fundamentalism, unless there is mutual understanding. In several conditions though, where there are long lasting disputes between states or non-state actors, fundamentalism arises and

³³ Paul DiMaggio; Eszter Hargittai; W.Russell Neuman; John P. Robinson, “Social Implications of the Internet”, Vol.27, Annual Review of Sociology, (2001), 307-336, at 310-312.

³⁴ David Leiwei Li, “Introduction: Globalization and the Humanities”, Vol.53, No.4, Comparative Literature (2001), 275-282, at 276-278.



cyberspace is like a shelter to it, since there are not concrete boundaries and a complete legal framework to be implemented. Fundamentalists take the chance to fight against the already existing political systems and they oppose to the traditional political communities, understood only within a given territory.³⁵

The liberty which they most times seek is usually compared to the freedom that the internet provides and therefore fundamentalists create trends by moralizing their ideologies. Cyberspace is used so to confuse users with the final purpose to legitimize the fundamentalists' actions.

Cyberspace and terrorism

Fundamentalism is many times the origin of terrorist attacks. The last few years, terrorist leaders have altered their policies and have modified the way their groups function. For this purpose, the internet is one of the most useful new technologies to be applied. Cyberspace, due to the absence of a legal framework, no legal penalties and austere measures to punish international crimes, can be easily used so as to serve terrorist purposes.

The United Nations has unequivocally condemned every kind of terrorist actions. Under the auspices of the organization, a series of resolutions, which terms and characterizes terrorism as a 'threat to peace', has been adopted. This characterization entails the direct application of Chapter VII of the United Nations Charter. This definition helps the organization to combat terrorist attacks and to directly protect world peace. What has to be done, though, is to recognize that terrorism functions via the internet as well something which also constitutes a threat to peace and in any case it is an international crime, which has the primary purpose to institute terror among people and to lead to the infringement of social life in all possible aspects.

Since we adopt a definition which fits to the purpose of terrorist actions, actions which are carried out through the internet have to be thought up like international crimes, which pose a threat to national security and innocent civilians as well. Terrorist organizations attempt to gain

³⁵ Peter Juviler; Sherill Stroschein, "Missing Boundaries of Comparison: The Political Community", Vol.114, No.3, Political Science Quarterly, (1999), 435-453, at 437-440.



access to governmental confidential information or to national military forces through the internet. It is amazing how national security systems show vulnerability regarding terrorism, a deficiency originating from cyberspace.

Crime in cyberspace – Legislation

Crime follows cyberspace from its birth. Cybercrime derives from a wide range of motivations. It can either be political criteria or weakness of the individual. Dealing with cybercrime is more complex than it really appears to be. It involves many factors, such as national policies, international relations' trends, the clash of perceptions regarding sovereignty and territoriality, institutions and traditions. The international legal system, need to cooperate so to adapt in a condition where the application of national law is almost out of question and harmonization between the already existing legal systems is the one and sole way to deal successfully with cyber crime. Issues of legal treatment and legal enforcement have to be revised on the basis of unanimity and consensus, provided by the United Nations. Otherwise, the punishment of crimes committed on the internet will not be acceptable and in compliance with all national laws, something which will unquestionably create international disputes between states which will aim to the protection of their nationals. Legal harmonization is the hot spot when referring to the internet.

Cyber crime involves three categories of activity. First of all, there are the crimes which are computer-related, such as theft. In this category, the computer is only the instrument used so as to commit the crime. The new element in these crimes, which alters them from the traditional form of the crimes to which they are similar, is that they also incorporate the manipulation of personal data, as a prerequisite for their completion. The second group of crimes is the content-based cyber crimes. These criminal actions focus on the illegal delivery of data, which violates the fundamental right to personality.

For example, child pornography and copyright infringement are only two of these cases, where the crime receives disdain mainly for the content of the data that is distributed and not for



its manipulation because great humiliation is created and financial interests are severely violated. Lastly, there are the crimes which aim to paralyze computer systems, by violating their integrity and the confidentiality supposed to be provided. Hacking and the creation of viruses are the ways to achieve such crimes. This category raises greater need for protection as it applies simultaneously to both individuals, whose rights are violated and to nations as well, which fail to guarantee to their nationals their right to personal security. Additionally, criminals enjoy cyberspace's advantages, such as anonymity and geographical reach which allow them to try crimes which under traditional conceptions would be unapproachable.³⁶

The main problems which occur when it comes to the confrontation of cybercrime are obscurity of data collection, the behavior of cybercrime victims, the widespread notion which dominates national authorities that cyber crime is not of top priority and the difficulty to keep a record of these crimes. Specifically, data collection is not an easy task, because there is not a widely accepted definition of cyber crime conducting to the denial of data sharing.

On the other hand, cyber crime victims do not report the crimes that have been committed against them, or they do not even understand that they have been the victims of a crime. For this reason, there are several national legislations that impose legal obligations to the individuals who do not report the crimes. The user's responsibility is of fundamental importance at this point. Moving on to the role that national authorities play, police officers do not think of cyber crime as an area of interest, when in the same time they have to deal with crimes which fit the traditional crime definition and involve direct violation of human rights. This approach creates a reluctance to move to investigations or even prosecutions of cyber criminals.

There are some situations, though, where individuals or non-state actors effectively managed to punish committed cyber crimes. For example, in France, the 'League Against Racism and Anti-Semitism' has successfully tried 'Yahoo!' which was offering Nazi memorabilia for sale. This action consisted of a crime according to France's national legislation (the French Penal Code) and was brought in front of the courts in 2001 (Reidenburg). In 2000, the American authorities were investigating in the activities of two Russian hackers and by using

³⁶ Stefan Helmreich, "Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism", Vol.25, No.4, *Science, Technology & Human Values*, (2000), 472-491, at 485-487.



their passwords and data they managed to reach Russian computers and information of national interest. The Russian authorities pressed charges on the American officers who have conducted the research. Their investigations were understood as violation of Russia's national sovereignty and territoriality (Brenner and Koops - 2004).

National provisions have been helpful in substitution for an international legal framework which does not exist for the time being. In the United Kingdom, internet service providers along with the 'Internet Watch Foundation' established a law protecting from the distribution of pictures with content related to child pornography. Other examples are those of the United States of America, which adopted in 2003 the "National Strategy to Secure Cyberspace", or, the European Union which has concluded to Directive 95/46/EC, which asks for the implementation of national penal codes or other appropriate measures on those who process personal data, more specifically when the process takes place over many networks. South Africa has adopted the 'Electronic Communications and Transportations Act' of 2002, which poses special requirements to those who try to use important data related to information of national security.

There have to be, though, an international approach regarding cyber crime. Moving on to this direction, there are some initiatives that have taken place under the auspices of several international fora, like the G8 or the European Union. The Council of Europe is by far the institution that has led to essential steps to cyber crime combating. In 1985, a special committee was established with the purpose to provide national legislations with directions relating cyberspace. The committee's report was annexed to a recommendation (No. (89)9) which urged all governments to renew national provisions. The Union's greater contribution, though, was the 'Cyber-crime Convention'. The convention was open to signature, since 2001 and since then it has been signed by 34 out of the 46 members of the Union. This convention is an instrument greeted for its content, something which was virtually expressed by the fact that four non EU members took part in its composition. The United States of America, South Africa, Canada and Japan participated in this convention and also signed it. Other non-members states have respectively signed and ratified the convention.

The complexity of creating a legal framework for cyberspace has been completely understood by policy makers. For that reason, they have applied a series of mechanisms, so to



facilitate data security. Another conflict related to the same issue, is that cyberspace and the internet are new phenomena in people's lives, not yet well understood and comprehended. Adopting measures on such a domain is a dangerous challenge, since the activities that have to be criminalized cannot be fully approached. After having studied the existing legislative texts it comes out that there are four major principles, the keys according to which cyber crime is addressed. There is the '*active nationality principle*', which deals with the nationality of the criminal. There is also the '*passive nationality principle*', focusing on the nationality of the victim. The '*universality principle*' is applicable when a crime is recognized as a crime against humanity (ex. terrorism). Last but not least, the '*protective principle*' is a compromise between cyber crime's universal function and the national interests of the states.

According to Antonio Cassese the major principle of international criminal law is that "a crime committed within a state's territory may be tried there, although the territoriality of criminal law does not coincide with territorial sovereignty". It has to be appended, though, that in developed countries where there are national legislatures on cyber crime, there are many difficulties regarding law enforcement, since the process of investigating in the criminal activities and prosecuting the criminals is a vague task when it comes to be put into practice by the police.³⁷

Cyberspace and national sovereignty – the crime of expanding viruses

"The healthy functioning of cyberspace is essential to our economy and our national security". This is the official statement of the American government in 2003, when the 'National Strategy to Secure Cyberspace' was adopted. Cyberspace conceals many dangers for national sovereignty and integrity. Since many crimes committed through cyberspace are targeted to national cyber systems, and most specifically after the 11/9, when the war against terrorism was launched there is an urgent need for states to secure their systems.

³⁷ Ian Walden, "Crime and Security in Cyberspace", Vol.18, No.1, Cambridge Review of International Affairs, (Cambridge: Routledge Publishing Ltd.) (2005), 51-68.



Nowadays, one of the easier ways so as to violate national security (people's collective right to security) and consequently the individual right to personal security is to create viruses. New viral strains are everyday created and compared to military threats to member-states. Computer viruses are more or less like the biological ones, which use their hosts' reproductive material, in order for them to survive and copy themselves. If the hackers, the viruses' creators, are attempting to violate the systems of individuals, then the responsibility for protection relies upon the users themselves. Cyberspace ethics are once again close to the Western observation of law, where the individual cares for his own protection.

Individuals, when using the internet, have theoretically decided to enter into a contractual relation with the internet system itself and afterwards with all the other users. In the case that the viruses are made to violate national computer systems the situation becomes more complex. According to recent statistics, the number of systems infected by viruses is doubling every year. Hackers, whether they act individually or in teams, break into networks and cause great damages. Sometimes they claim to act in favor of their political views, by demonstrating the weaknesses of the systems. Hobsbawm, in 1965, has characterized them as "primitive rebels". It has been recorded that there is an emerging nonwhite class of hackers. People of a Latin origin or black-skinned create hacking groups and in this way they show their frustration for the discriminations they face in their everyday life. Hacking can be also originating from unemployment. The National Security Association for the United States reported in 1999, that Bulgaria had originated 76 viruses in a year. After studying the statistics, it has been submitted that in Bulgaria there was a significant number of well-trained but unemployed programmers, who unfortunately found the creation of viruses as one of the ways so as to express their creativity.

The states have the responsibility to protect their nationals (expression of the social contract idea) by securing data of state interest. The last few years, viruses are often mentioned as 'communications' terrorism', which raise wide protection. On the other hand, the idea of using viruses as national military tools is emerging rapidly these days. For example, in 1987, the Hebrew University library network in Jerusalem, reported the existence of a virus in its systems. It has been found out that the virus was put so to delete and destroy all the files as a protest on



13th May 1988, which was the 40th anniversary of the last day that Palestine has been recognized as a subject in the international legal order. This example obviously shows that viruses are employed for political uses, from the very beginning of cyberspace's birth.

The one and sole solution that has been found till now in 'the war against viruses' is the quick adaptation of the operating systems to technology progress. Diversion and flexibility are the two elements that can tackle viruses; they form the so-called "Adaptive Security Management".³⁸

Cyberspace and the United Nations³⁹

On November 13th to November 15th, the United Nations organized in Rio de Janeiro a forum dealing with several aspects regarding cyberspace. The 'United Nations Internet Governance Forum', hosted at about 1,700 participants, who represented member-states, the private sector, the media, non-governmental organizations and civil societies. One of the issues to be discussed was that developing countries' need to achieve access to the internet. It has been submitted that despite the progress that has been made during the last years, there are still many things to be done, since the inequalities between the people of developed and developing countries continue to exist. High costs of international connections and expensive access prices are the boundaries that do not allow developing countries to use the internet.

The Brazilian Minister of Communications has stated that there is an urgent need to bring most people online and to achieve low prices along with services of good quality. It has also been reported, though, that Latin America has increased through a variety of mechanisms its access to the web. The Pacific Islands Telecommunications Association has asked for the impediment of the European and American domination on the Internet Exchange Points (IEPs), which provokes developing countries of using the internet.

³⁸ Stefan Helmreich, "Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism", Vol.25, No.4, Science, Technology & Human Values, (2000), 472-491.

³⁹ Ahmad Kamal, "The Law of Cyber-Space", United Nations Institute for Training and Research (UNITAR), (Geneva: 2005).



Another topic that has been thoroughly put under discussion is that of achieving diversity and multiculturalism in cyberspace. The Brazilian Minister of Culture expressed his fears that there are several barriers on cyberspace which disfavor multiple cultures and diverse positions to be established through the internet. One of the Indian representatives, on the other hand, stated that cyberspace is one of the most powerful social actors, as it has helped people of different castes to communicate and create relationships between each other.

The Thailand Association for the Blind mentioned that cyberspace remains a place not accessible for people with disabilities and he said that diversity equals indeed to disability. Last but not least, the International Development Research Centre has presented its program for localizing the internet and creating a new digital content in 35 local languages in Asia and Africa respectively and by promoting the use of free software.

The second day, the forum dealt with balance between property rights and internet freedom. There is a clash between the ideas of the free movement of information and intellectual property law. Fortunately, many of the participants were optimistic enough so as to support the fact that freedom of information can exist alongside with effective regulations. Most of these participants were signatories in the European Convention for cyberspace.

Some of the conflicting areas that have been touched upon were the prohibitions that have to be implemented to web casters, since the International Association of Broadcasters said that there is not a sense of balance between the traditional and the web-based media. Amnesty International has made some of the most vital comments. Focusing on the protection of human rights, the organization stated that governments do not care about the protection of human rights and pay attention only to crimes, such as child pornography or terrorism. At the same time, many internet users have been the victims of censorship and there are many occasions where activists have been punished for actions that were fully legitimate and legal. Special attention was also given to the protection of personal data, especially after the example of a country in Latin-America, which made available for everyone to see the names of all those infected with HIV/AIDS, in the name of transparency.

The last day of the forum the podium belonged to the civil libertarians and all the skeptics who examine systematically cyberspace's future. There were many discussions regarding the



democratic transformations that should be taking place through the internet and they unfortunately do not function properly, thus belittling the importance of political participation and common life. The so-called “global internet law” was another topic where many different opinions were expressed. Many did not hesitate to compare internet law with the law of the sea, which was an area of clash for a large number of countries, a fact that led to many years of endless negotiations.

The minimum consensus that was reached was that there is a necessity to move towards a well-governed ‘topos’, which will provide its users with safety. Last but not least, those representing civil societies called for infrastructure and state capacity, which will enable citizens to have access to the internet and will at the same time improve the networks, helping to save energy for the sake of the environmental climate change.⁴⁰

Propositions – Solutions

Truth be told, that the international community needs to move on with radical and specific measures, so as to combat the aforementioned conflicting areas. Not only the United Nation’s member-states but also all the actors of the international legal system have to cooperate and adopt initiatives for the improvement of the present case. The United Nations has recently organized a world forum which discussed cyberspace and reached many different aspects of the topic. The problem, though, is that cyberspace and the human rights abuses that it may come out of its use are not on top of the United Nations’ agenda.

The UN has created mechanisms which allow it to act on a basis of autonomy, thus enhancing the organism’s negotiating capacity. In the time being, there are many points of clash between the member-states which pose a halt to the procedures of decision-making. Members-states do not share policies regarding cyberspace and they obviously try to satisfy their own interests. Most of the developed countries do not share technology information with the

⁴⁰ <http://www.un.org/News/Press/docs//2007/pi1814.doc.htm>



developing ones and in this way there is no chance for the latter to build secure and safe networks not only for national purposes but also for their citizens. Computer technology has to be shared between the members-states, and, the United Nations need to provide their “weaker” members with the opportunity to access the world web. During the last years, many countries in Africa, Latin America and Asia have improved their position on this domain. The problem that continues to exist, though, and influences the citizens more than the states’ administrations is that access to the internet is not really permitted to people, since the prices of both hardware and software are very high.

There are very few multinational corporations that own computer technology and they offer it on high prices, which makes it almost impossible for the developing countries to afford. There is more or less a kind of monopoly regarding computers and especially the services which are necessary for accessing the internet. The United Nations needs to deal with the existing conditions and create a system which will offer to its members equal opportunities regarding cyberspace, or otherwise, the gap between the developed and the developing countries will become wider. Cyberspace is not a luxury for people and its necessity has to do mostly with knowledge and information.

The next step that has to be dealt with is that of legislation and its unification. There are many difficulties arising, something which is more or less expected due to the fact that cyberspace is legally approached for the first time by the international community. It has to be seen as a “terra nullia” which has to be well and effectively governed by its users, who are citizens from all over the world, nationals of every country. The United Nations should carefully examine all the diverse views that appear and work on a convention which will gain wide acceptance amongst its members-states. The codification and maybe the criminalization of all the illegal actions which are conducted through the internet is of capital importance, as it will help not only the individuals, but also the governments, by providing them with a strong shield against criminals.

Attempts towards the creation and implementation of an international instrument which will be dealing with all the areas that are related to cyberspace, have not been successful in the past years. Some states adopt a more libertarian position which stands against the above idea. It



is only under the auspices of the United Nations that a solution can be possibly reached' a solution which will be reflecting a minimum consensus between the states.

Last but not least, it has to be mentioned that other actors, except from the members of the UN have to be participating in every forum on cyberspace. Non governmental organizations, like Amnesty International and Human Rights' Watch have long experience on the protection of human rights and can offer available information and great assistance in almost every sub-topic on cyberspace and human rights. The private actor has also to cooperate in all possible ways, as it plays a fundamental role, regarding the technological aspects of the topic.

Mutual understanding and negotiation and compromise are the keys, so as to deal with the case and conclude to a specific legal frame which will be protecting the international community both vertically and horizontally.

Conclusions

Cyberspace, the new and exciting reality, touches almost upon everyone. It is the centre of information and the means to reach the world. It is the technology which makes it easier to dream of a global community and build a world where states are not of paramount importance for the procedure of decision-making. Pluralism, multicultural, polyphony, democracy and other notions find cyberspace as a promising reality which will ease down the existing international disputes, by building mutual understanding and by being the major expression of globalization's advantages. The problems which follow cyberspace's existence are many though, due to the legal vacuums that need to be covered fast.

Human rights are in the heart of all the above mentioned, as cyberspace is created in order to help people's communications and to provide them with infinite knowledge and information. Individual and collective rights have to be protected and this is the reason why states are involved in this process. It is high time that the United Nations took action on this field, heading to the establishment of a "place", where good governance will be finally attained and achieved.



Index of authorities

A. BOOKS AND TREATISES

Brunn, *Towards an Understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning*, Geopolitics, (Cambridge: Routledge), (2000),

Cohen, *Terrorism and Cyberspace*, Managing Network Security,

Dunn, *Cyber-Threats and Countermeasures, Towards an Analytical Framework for Explaining Threat Politics in the Information Age*, 5th Pan-European IR Conference, SGIR (Hague: 2004),

Geist, *Global Internet Jurisdiction: Highlights of the ABA/ICC Survey*, Committee on Law of Cyberspace (“Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet”), (2000),

Kamal Ahmad, *The Law of Cyber-Space*, UNITAR, (Geneva: 2005),

Perri 6, Global “Digital Communications and the Prospects for Transnational Regulation” in David Held & Anthony McGrew eds., *Governing Globalization*, (Cambridge: Blackwell Publishing Company) (2002) 145,

Rundle, *Beyond Internet Governance: The Emerging International Framework for Governing the Networked World*, Research Publication No.2005-16 (2005),

Rundle, *International Personal Data Protection and Digital Identity Management Tools*, Identity Mashup Conference (Harvard Law School: Berkman Center for Internet and Society), (2006);



B. PERIODICALS

Adams, *Network Topologies and Virtual Place*, Vol.88, No.1, *Annals of the Association of American Geographers*, (1998),

Beckles, *Black Liberation and the Internet: A Strategic Analysis*, Vol.31, No.3, *Journal of Black Studies*, Special Issue: Africa: New Realities and Hopes (2001),

Beeson, *Top Ten Threats to Civil Liberties in Cyberspace*, Vol.23, No.2, *Human Rights*, (1996),

Black Higher Education on the World Wide Web, No.14, *The Journal of Blacks Higher Education*, (1996-1997),

DiMaggio; Hargittai; Neuman; Robinson, *Social Implications of the Internet*, Vol.27, *Annual Review of Sociology*, (2001),

Fandy, *CyberResistance: Saudi Opposition between Globalization and Localization*, Vol.41, No.1, *Comparative Studies in Society and History* (1999),

Gilbreth; Otero, *Democratization in Mexico: The Zapatista Uprising and Civil Society*, Vol.28, No.4, *Latin American Perspectives*, Mexico in the 1990's: Economic Crisis, Social Polarization, and Class Struggle, (2001),

Helmreich, *Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism*, Vol.25, No.4, *Science, Technology & Human Values*, (2000),

Hurwitz, *Who Needs Politics? Who Needs People? The Ironies of Democracy in Cyberspace*, Vol.28, No.6, *Contemporary Sociology*, (1999),



Juviler; Stroschein, *Missing Boundaries of Comparison: The Political Community*, Vol.114, No.3, *Political Science Quarterly*, (1999),

Leiwei Li, *Introduction: Globalization and the Humanities*, Vol.53, No.4, *Comparative Literature*, (2001),

Rodan, *The Internet and Political Control in Singapore*, Vol.113, No.1, *Political Quarterly*, (1998),

Sharpe, *Racialized Fantasies on the Internet*, Vol.24, No.4, *Institutions, Regulation and Social Control* (1999),

Shu, *Information Technologies, the U.S. Nation-State, and Asian American Subjectivities*, No.40, *The Futures of American Studies*, (1998),

Sussman, *Urban Congregations of Capital and Communications: Redesigning Social and Spatial Boundaries*, No.60, *Globalization?*, (1999),

Walden, *Crime and Security in Cyberspace*, Vol.18, No.1, *Cambridge Review of International Affairs*, (Cambridge: Routledge Publishing Ltd.) (2005),

Wellman; Salaff; Dimitrova; Garton; Gulia; Haythornthwaite; *Computer Networks as Social Networks: Collaborative Work, Telework, and Virtual Community*, Vol.22, *Annual Review of Sociology* (1996),

Yang, *The Co-Evolution of the Internet and Civil Society in China*, Vol.43, No. 3, *Asian Survey*, (2003).



THESSISMUN 2008



C. WEBSITES

<http://www.un.org/News/Press/docs//2007/pi1814.doc.htm>