ГЛОБАЛНА НЕЕДНАКВОСТ, ИНДИВИДУАЛНА ТРАУМА – ДЕВИЈАЦИЈА

Драган СТЕФАНОВСКИ

Апстракт: Крајот на XX век е исполнет со исклучителни динамични промени во современото општество, предизвикани главно од процесот на глобализација инволвиран во секој сегмент на општеството. Мешањето на процесите на глобализација, транзицијата, како и приватизацијата во постсоцијалистичките земји доведе до значителен пораст на општествената нееднаквост, манифестирана преку значително зголемениот број сиромашни луѓе. Се разбира дека глобалните промени водат кон турбуленции на општествениот систем и дека се насочени кон интензификација на сиромаштијата, општествената и економската поларизација и распад на општествената кохезија и солидарноста. Во натамошниот дел од текстот ќе се фокусираме на врската помеѓу сиромаштијата и одредени типови девијации, имајќи предвид дека поединецот како индивидуа е навикнат на промени, но секој од нас различно реагира на општествената траума. Одговорот што го бараме е, дали постои брз и креативен начин за надминување на овие трауми предизвикани од брзите и неочекувани глобални промени и дали тој лежи во надминувањето на економските разлики.

Клучни зборови: општествена траума, општествена нееднаквост, модерно општество, сиромаштија, девијации.

UDK 316. 325. 063. 24:004] – 027. 511
Short Scientific Aartcle

GLOBAL COMPUTER NETWORK AND SOCIAL TRAUMA[1]

Ljupcho Cvetkovski[2]

Abstract: The global computer network has a significant contribution to the ongoing globalization process that integrates societies in every aspect. At the same time, it brings challenges to the world that need to be solved. These challenges present threats that can cause social traumas. Computer network technology and intellectual property laws are not well known and understood by everyone. The presence of fear can be confirmed by the survey I have conducted in 2013 among global computer network users in Republic of Macedonia. The survey shows that users are not against the existence of the laws and are willing to pay for the services, although they have different opinions on the rules and payment methods. The more important information from the survey is that users are afraid of security and privacy threats. Their fear is not stated directly, but it can be inferred from their answers. My overall conclusion is that all people should be more engaged in the process of globalization in order to overcome social traumas. Every person from all around the world is a social being and should contribute to the global society.

Keywords: network, threat, trauma, survey, globalization

1. Introduction

The greatest achievement of the globalization process on a political scale is the foundation of the United Nations. Globalization would not be felt by people around the world if there were not technology advances that contribute to it. One of the greatest technology advances that have significant contribution to the ongoing globalization process is the global computer network. The United Nations and the global computer network are themselves products of social traumas experienced during the Second World War. The United Nations were founded as an international organization primarily to maintain peace and security among the nations. The global computer network was born of a defense project that intended to create a computer network safe from interruptions. That would be made possible by having no central authority and using packet switching technology. The first connected computers acted as peers in a distributed computer network. Peer-to-peer computer networks are distributed networks of peer computers. They are best known for file sharing among their users. The

[1] Paper presented at International Scientific Conference *Facing Social Traumas: A Challenge for Sociological Research*, Faculty of Philosophy, within Ss. Cyril and Methodius University in Skopje, Skopje 23-24 April, 2015.

[2]e-mail: cvetkovski_ljupco@yahoo.com

growth of the global computer network introduced threats that can cause traumas to its users. Such are security and privacy threats. The users of peer-to-peer file sharing applications face the same threats. Presence of fear among the users can be inferred from the results of the survey research I conducted in 2013 in Republic of Macedonia.

2. Peer-to-Peer File Sharing in Global Computer Network

On 29 October 1969 a group of scientists made the first data transmission through the computer network built for the project funded by the United States Department of Defense Advanced Research Projects Agency (Ryan 2010:30-31). By December 1969 the initial network connected four computer nodes from different locations in the United States (Ryan 2010:30). This computer network was demonstrated at the International Conference on Computer Communication in Washington in October 1972 (Ryan 2010:30). A group of researchers formed the International Network Working Group (Ryan 2010:95). The first international connection of this network was established in 1973 (Ryan 2010:95). In 1974 the term "Internet" was used for the first time in Request for Comments (Cerf, Dalal and Sunshine 1974). The Internet protocol suite was introduced in 1981 (Postel 1981). It was fully implemented on the network in 1983 (Ryan 2010:91).

The growth of computer and Internet usage in every part of the world can be confirmed by the reports of the International Telecommunication Union. It was estimated that almost 3 billion people would use Internet at the end of 2014 (ITU 2014:174).

People could use the global computer network to cooperate, but at the same time, to commit crimes as well. Malware can cause damages to computer hardware and software. In 1988, Robert Tappan Morris, a graduate student at Cornell University, released a computer worm that caused failure of computers at universities and research institutions throughout the United States (Hafner and Markoff 1991:220). Around six thousand computers were infected with the Morris worm (Hafner and Markoff 1991:321). His father was a computer security expert and chief scientist at the National Computer Security Center (Hafner and Markoff 1991:261).

A massive data theft was announced by Sony in April 2011 (Kelly and Baker 2011). Someone obtained personal data from 77 million user accounts through Sony's online video game network (Kelly and Baker 2011). The unknown person obtained usernames, passwords, and possibly credit card data (Kelly and Baker 2011).

Social networks are very useful for criminals to acquire personal data and even arrange meetings with the victims. Some people use false profiles to set up a blind date with persons they know just to make fun of them. Anyone can go to an Internet café where nobody asks for an identity document and create a social network profile of someone he knows and use it with criminal intent. One can

either use false pictures or even downloaded pictures of the right persons to create their profiles and establish contacts with people without them knowing how their personality is introduced. The military intelligence officers use false profiles to track the activities of military employees on the social networks. Privacy protection groups have complained for Facebook putting their personal data at risk (Kirk 2010). Facebook enables users to set restrictions for access to their profiles, but in 2013 they admitted that an unexpected fault had exposed the contact information of 6 million users (Bosker 2013). Austrian law student Max Schrems was surprised when he received 1,222 pages of information upon his request of his personal data recorded by Facebook (Guillard 2011). Schrems said: "When you delete something from Facebook, all you are doing is hiding it from yourself" (Guillard 2011).

Peer-to-peer computer network is a distributed network of interconnected computers that act as equals (Buford and Yu 2010:6). In a peer-to-peer network every computer can act as a server and client simultaneously. There is no single point of failure. The number of computers joining or leaving the network can change at any time without negative consequences. All the computers contribute to the network.

The applications used in peer-to-peer networks can belong to these groups:

- Content delivery: file sharing (Napster, KaZaA, iMesh, LimeWire, Shareaza, eMule, BitTorrent, BitComet, BitTornado, µTorrent, Transmission, Yet Another BitTorrent Client, Vuze, Deluge, FrostWire, qBittorrent, rTorrent), audio and video streaming (PPStream, PPLive, TVUPlayer, Joost, CoolStreaming), news (Usenet), web portals (Osiris);
- Resource sharing: processing power (SETI@home), cache (Dalesa);
- Collaboration (Collanos Workplace, BestPeer, Windows Meeting Space, Microsoft SharePoint Workspace);
- Real-time communication: audio, video, and text messaging (Skype, Qnext);
- Content search: search engine (YaCy, FAROO), web crawler (Apoidea);
- Trade: marketplace (Tradepal, Fiverr), payment system (Bitcoins), exchange (Mt.Gox, Bitcoin-Central, Bitstamp, Intersango) (Cvetkovski 2013:38-39).

File sharing applications are the most popular among peer-to-peer network users. According to the Sandvine Global Internet Phenomena Report for the first half of 2014, BitTorrent is a world leading upstream application in peak period traffic in fixed access networks (Sandvine 2014). The share of network upstream traffic with other applications during peak period by regions is: North America 24.53%, Europe 33.20%, Latin America 19.83%, Asia-Pacific 45.74%, and Africa 23.02% (Sandvine 2014).

Peer-to-peer file sharing applications were the focus of my master's thesis research in 2012 and 2013. From 4 April to 5 June 2013 I conducted an anonymous survey among global computer network users in Republic of Macedonia (Cvetkovski 2013:88). The survey was intended for users aged 18 to 74. There were 425 respondents. The sample size satisfied the criteria for confidence interval of 95% and margin of error of 5%. Out of 22 questions, 21 questions were semi-closed and 1 question was open-ended. Semi-closed questions offered a list of answers with a possibility for the respondent to give his own answer that was not on the list. The number of answers that were given by respondents for each of the semi-closed questions did not surpass 3% of the total number of answers. The small number of other answers confirmed the quality of the possible answers offered.

The answers of the question on the most often used way of downloading files from the Internet were: Peer-to-Peer File Sharing Applications 32.7%, World Wide Web 24.9%, Free Download Manager 15%, File Hosting Service 10.4%, Web Browser Add-on 5.9%, Instant Messaging 5.9%, electronic mail 4%, Remote Connection 0.7% (Cvetkovski 2013:90-91). In 2013, peer-to-peer file sharing applications were the most often used applications for downloading files among global computer network users in Republic of Macedonia. On the question of how often they used peer-to-peer file sharing applications, 38% of them answered they used them often (Cvetkovski 2013:91). Even the users that did not use them most often for downloading files used them often.

The users of peer-to-peer file sharing networks face the same threats as the global computer network, such as security and privacy breaches.

3. Security in Peer-to-Peer File Sharing Networks

There are many scientific papers that explore the security in peer-to-peer file sharing networks. Scientists offer different solutions to overcome the security threats, but many users do not understand and cannot implement them if they are not already implemented. Much of the implementation of security solutions demands users to have knowledge and skills to modify the applications. Those demands can cause trauma to the users who are not knowledgeable and skilled. Even the creators of peer-to-peer file sharing applications face security problems they cannot solve without the help of computer security experts. The best way of protection against security breaches is using security software developed by the best companies in the field. Even the best security software cannot detect all the security threats and defend the computers from all possible attacks. That can also cause trauma to the users.

In order to compare the behavior of different antivirus software I performed a simple test on 24 and 25 August 2012 (Cvetkovski 2013:53). On a Samsung lap top with an Intel i5 M480 processor and 4 Gigabytes of random-access memory I used VMware Workstation 7.0.0 to create two virtual machines. I installed Microsoft Windows XP Professional Service Pack 2 on one of the

machines and Microsoft Windows XP Professional Service Pack 3 on the other machine. Then I connected the two machines in a virtual network, as well as to the Internet through a Speedport W 503V router. I used portable µTorrent 3.2 and its built-in tracker to create torrent file representing a folder named Great Stuff. The machine with Microsoft Windows XP Professional Service Pack 2 shared the folder. It acted as a sender while the other machine acted as a receiver of the folder. I used the snapshot manager to take snapshots of the machines. I installed antivirus software on the receiving machine. Each time after downloading had finished, I took a snapshot of the receiving machine, activated the first snapshot, installed other antivirus software, and started downloading the folder. At the end, I compared all the snapshots of the receiving machine.

The folder Great Stuff contained files that cause unwanted behavior of the computer:

- script Screen flash.bat makes the screen flashing;
- script Notepad.bat continuously opens the text editor Notepad;
- scripts Shutdown.bat, Shutdown2.bat, and Shutdown3.bat cause the computer to shut down;
- script Folders.vbs creates a lot of folders in drive C;
- script CD Drive.vbs continuously pops out the Compact Disk Drive;
- script Backspace.vbs continuously executes the user's previous commands while typing or opening windows;
- script You are deceived.vbs continuously writes "You are deceived" while typing;
- script Enter.vbs continuously presses the Enter button on the keyboard;
- script Caps Lock.vbs continuously toggles the Caps Lock button;
- macro in a Microsoft Office Word 2003 document deletes hal.dll and causes a computer failure when restarting it;
- executable file Proba.exe was created by ZIP 2 Secure EXE 14.4.0 from WinRAR 4.20 archive containing a picture Chrysanthemum.jpg and the script Folders.vbs;
- executable file Program.exe was created by Beast 2.07 by joining HJ-Split 3.0 and the script Folders.vbs;
- executable file Program 2.exe was created by Beast 2.07 by joining FastStone Capture 5.3 and the script Shutdown2.bat;
- executable file FCTBSetup.exe was created by IExpress 2.0 by joining FCTBSetup.exe and the script Shutdown3.bat (Cvetkovski 2013:53-56).

All the scripts were created with the standard Windows text editor Notepad. They can all be found on the global computer network. Executable files

were created to automatically execute scripts along with the execution of the joined applications.

The choice of antivirus software was based on popularity, awards, test results, and my own past experience: Bitdefender Antivirus Plus 2013, ESET Smart Security 5, AVG Internet Security 2012, McAfee All Access Internet Security 2012, Avira Antivirus Premium 2012, avast! Internet Security 7, Norton Internet Security 2012, and Kaspersky Anti-Virus 2013 (Cvetkovski 2013:56). Threats detected by the chosen antivirus software were:

- Bitdefender Antivirus Plus 2013: CD Drive.vbs, Program.exe, Program 2.exe, and Shutdown2.bat;
- ESET Smart Security 5: Program.exe, Program 2.exe, FCTBSetup.exe, Shutdown2.bat, and Shutdown3.bat;
- AVG Internet Security 2012: Program.exe, Program 2.exe, FCTBSetup.exe, and Shutdown3.bat;
- McAfee All Access Internet Security 2012: CD Drive.vbs, Program.exe, Program 2.exe, and Shutdown3.bat;
- Avira Antivirus Premium 2012: Screen flash.bat, Enter.vbs, Caps Lock.vbs, Program.exe, Program 2.exe, FCTBSetup.exe, Shutdown2.bat, and Shutdown3.bat;
- avast! Internet Security 7: Caps Lock.vbs, Program.exe, Program 2.exe, FCTBSetup.exe, Shutdown2.bat, and Shutdown3.bat;
- Norton Internet Security 2012: Program.exe, Program 2.exe, Shutdown2.bat, and Shutdown3.bat;
- Kaspersky Anti-Virus 2013: Caps Lock.vbs, Program.exe, Program 2.exe, and Shutdown2.bat (Cvetkovski 2013:56).

The detection of security threats started immediately after the folder Great Stuff had been downloaded. The folder had a capacity of 10.2 megabytes (Cvetkovski 2013:57). Different antivirus software detected different security threats. The Word macro was the worst threat of all, but it was not detected by any of the antivirus software. The script Folders.vbs did not represent a security threat and was not detected separately, but it was detected as such in Program.exe. AVG Internet Security 2012 and McAfee All Access Internet Security 2012 detected Shutdown2.bat as a threat in Program 2.exe, but not separately. Shutdown.bat was not detected as a threat even when both Shutdown2.bat and Shutdown3.bat were detected. When scripts that were not detected as threats were executed, the unwanted computer behavior they caused was not stopped by any of the antivirus software. The presence of antivirus software does not guarantee protection of the computer.

The survey research implicitly shows that the users of file sharing applications are afraid of security threats. The fear can cause traumas. The users' fear is obvious, though is not stated directly. It can be inferred from their

answers. Users were mostly disturbed by: viruses and other malicious software 36%, not downloading the whole file 23%, lacking of needed files 17%, legal problems 15%, forced contribution to the network by uploading pieces of the files that users are downloading 7% (Cvetkovski 2013:93).

Only 29% of the global computer network users in Republic of Macedonia shopped online. The users did not shop online mostly because of concerns with: security of payment systems 25%, complexity of the whole system 19%, possibility of not receiving the paid product or service 13%, unfeasibility of online shopping for the desired products and services 11% (Cvetkovski 2013:96).

The users preferred to pay for audio, video, software applications, electronic books, and other files in brick-and-mortar stores (Cvetkovski 2013:97).

A total of 75% considered there should be Internet regulations that would require liability for bad behavior (Cvetkovski 2013:95). Most of them (31%) agreed that all the people with bad behavior on the global computer network should be held liable.

4. Privacy in Peer-to-Peer File Sharing Networks

One way to secure the peer-to-peer file sharing networks is through building trust and reputation among the peers. It is hard to build such a system without revealing the identity of the peers. Anonymity of peers is one of the main demands of peer-to-peer file sharing networks. It protects the users' privacy. At the same time, it encourages some people to break the laws and put others at risk for helping them unknowingly.

The users of peer-to-peer file sharing applications are often held liable for breaking the intellectual property laws. The World Intellectual Property Organization is a specialized agency of the United Nations since 1974 (Cvetkovski 2013:63). As of May 2013, the founding convention was signed by 186 members, its Copyright Treaty had 90 contracting parties, its Performances and Phonograms Treaty had 91 contracting parties, Paris Convention for the Protection of Industrial Property was signed by 174 members, and Berne Convention for the Protection of Literary and Artistic Works was signed by 166 members (Cvetkovski 2013:63).

These laws were intended to provide international protection of the intellectual property. The owners of the intellectual property pay the government for protection. The government protects their properties. The owners are motivated to continue inventing. These laws promote development by disclosing the intellectual properties and protecting them from stealing. The owners could exploit their intellectual properties to get rich and hinder competition. The government encourages competition through separate competition laws. The

competition laws prevent anti-competitive behavior of the intellectual property owners.

Recording Industry Association of America sued Napster in 1999 for breaking the intellectual property laws and eventually won the lawsuit (Cvetkovski 2013:80). The recording companies filed a lawsuit against Aimster in 2001 and won it again (Cvetkovski 2013:80). Napster and Aimster were shut down. Despite the problems Napster and Aimster faced with their services allowing users to illegally share files, in 2001 a company in Netherlands started peer-to-peer file sharing system named KaZaA (Cvetkovski 2013:20). The same year the Caribbean company Grokster offered peer-to-peer file sharing application to global computer network users (Cvetkovski 2013:80). Recording companies filed lawsuits against both of them. The company in Netherlands sold the KaZaA system to the Australian company Sharman Networks incorporated in Vanuatu (Cvetkovski 2013:21). When in 2003 both were relieved from convictions, the recording companies started filing lawsuits against individual users illegally sharing files (Cvetkovski 2013:80). Sharman Networks in response filed a lawsuit against the recording companies for unauthorized use of its software (Cvetkovski 2013:80). In 2005, the United States Supreme Court unanimously decided that Grokster was liable for breaking the intellectual property laws and Grokster shut itself down (Cvetkovski 2013:81). The decision could be read on Grokster's website along with the public Internet protocol address of the logged computer warning that nobody was anonymous (Cvetkovski 2013:81). In 2005, Patricia Santangelo claimed she was not using KaZaA on her computer and after her case had been dismissed by the court in 2007, recording companies filed lawsuits against two of her children (Cvetkovski 2013:81). Her daughter Michelle asked to testify against KaZaA's owners because they did not warn their users of the possibility of breaking the laws (Cvetkovski 2013:81).

The German company ipoque, which provides network traffic management and analysis by using technology of deep packet inspection, said the creators of peer-to-peer file sharing applications justified encryption and obfuscation as means to protect privacy (Cvetkovski 2013:85). Encryption and obfuscation could be used either to circumvent bandwidth limitations imposed by Internet service providers or to hide the illegal activities on the network from the authorities.

In 2006, the German record company Peppermint Jam Records used the services of the Swiss company Logistep to search for users who were sharing its records through peer-to-peer file sharing applications (Cvetkovski 2013:73). Most of the alleged infringers were from Italy where a trial court ordered the Internet service providers to disclose their identity, but the Appellate court reversed the order to protect their personal data (Cvetkovski 2013:74).

In 2007, the American Internet service provider Comcast blocked the BitTorrent protocol in accordance with its traffic management policy, but the two non-profit organizations Free Press and Public Knowledge filed a complaint

against it because the policy did not conformed to the network neutrality policy of the Federal Communication Commission (Cvetkovski 2013:84). Comcast appealed the initial decision and the Appellate court ruled in its favor (Cvetkovski 2013:84).

The legal cases show the presence of privacy threats on the peer-to-peer file sharing networks. In 2013, 49% of peer-to-peer network users in Republic of Macedonia accepted file sharing through their computers, but just for the users they knew (Cvetkovski 2013:98). The reasons that most of the users did not want to share files were privacy (22%) and security (13%) (Cvetkovski 2013:98).

There are many organizations and individuals that promote freedom on the global computer network. Security and privacy threats can cause traumas that increase the desire for freedom. But unrestricted freedom on the global computer network means freedom even for the users that can destroy the network. There have to be some regulations. According to the survey research, users think that: everybody should be held liable for bad behavior on the network (31.1%), Internet service providers should be held liable for letting users with bad behavior to impact other users (25.4%), Internet should be free of regulations (24.7%), and end users should be held liable for bad behavior (18.3%) (Cvetkovski 2013:95).

People must pay to own computers and to have access to the global computer network. The prices are still high. That could be one of the reasons that 33% of the users wanted downloading files through peer-to-peer networks to be free of charge (Cvetkovski 2013:97). Still, 66% of the users accepted paying for the files, but in different ways: if it was included in internet subscriptions (29%), if the price was low (21%), if all the users were paying (9%), and if they got paid for the files others were downloading from them (7%) (Cvetkovski 2013:97).

5. Peer-to-Peer File Sharing and Globalization Process

Peer-to-peer file sharing networks connect people from all around the world. More connected people mean faster downloads. Globalization process has a positive impact on peer-to-peer file sharing in many ways. Prices of desired products and services could become lower. Globalization could establish a legal system for the whole world. Network users would not feel afraid of not knowing all the laws from different parts of the world. Laws could protect their security and privacy. At the same time, they could stop the inventors to hide in countries that allow businesses forbidden in their homelands.

We are still far away from a globalized world. The biggest obstacle for its achievement is the power of the nation states. Governments of several nation states rule the world. Until they feel they represent their homelands in international relations and have the power to rule the world, the globalized world will just be a fiction. Politicians usually come to power from their homelands and

protect national interests. They cannot bear the burden to rule the whole world and protect the interests of mankind.

The United Nations was founded in 1945 and currently is made up of 193 Member States (United Nations 2015). The organization promotes human rights, but is not efficient in protecting them. The wars fought inside and among its members after its foundation are proofs of its inefficiency.

Yugoslav Wars were fought among the Yugoslav republics. Eventually all of them became democratic countries and made the decision to become members of the European Union. That makes wars illogical.

The armed conflict in Republic of Macedonia in 2001 happened at the time when the country's name was not recognized by the international community. Macedonians felt a threat to the territorial integrity and sovereignty of the state and their national identity. Albanians fought for improved rights in the state, such as declaring their language as second official language. Though they were a minority, they wanted Republic of Macedonia to be constituted as bi-national state (Iseini 2008:12). Even the Council of the European Union suggested to the Macedonian government that Republic of Macedonia should be re-constituted as a multinational state (Veljovski 2010:45).

The best way to stop the armed conflicts is to develop a collective consciousness of the people towards living in a society with citizenship as a core value (Matevski 2009). The political parties in the United States of America speak to the citizens, not to ethnical or religious groups. But even there, the politics of fear promotes everyone as a potential victim that needs to be protected from criminals and terrorists (Altheide 2009:55). Terrorists are presented as people without goals, except to kill and terrify, and criminals are called terrorists because they spread terror, like the serial killers that kill at random (Altheide 2009:63, 66).

The sense of powerlessness initiates the foundation of civic organizations, but even they promote fear. In June 2001, a charitable organization issued a report which disputed the claim that child abduction was a serious risk and warned that the risk for the child was greatest at home (Furedi 2002:173). It just moved the risk from one place to another.

There are different views on global culture. One view is that cultures will preserve their differences (Giddens 2009:146). Another view is that cultural diversity will be undermined (Robinson 2007:140). The first view for some cultures means they cannot assimilate other cultures. The second view for some cultures means they cannot protect their cultures from assimilation.

There is no homogenous culture that is completely isolated from other cultures. Differences exist among people in every nation state. Globalized world does not mean that differences will stop existing. It means that everyone will act as a human, not as someone that is an inhabitant of a part of the world. In the past, tribes grew into nations, but today there are still some tribes. Cities grew into empires, but they still exist. They are parts of the nation states. Inside the

state, people identify themselves by the city, the district, the street, and even the building they live in. That does not mean they do not belong to the nation. For everyone, belonging to the nation should not mean that one is neither a human belonging to mankind nor a social being belonging to a global society. The nation state borders should be like municipality borders. People elect mayors and members of Parliament. There should be a world government elected from the global citizens, not from national governments. The state government, not the mayors, creates the state politics. The world government, not national governments, should create the world politics. In the world political institutions, the politicians should represent world interests, not national.

6. Conclusion

In the world we live in, there are many preconditions for social traumas. The global computer network, specifically peer-to-peer file sharing network, presents threats that cause fears among its users. Users are afraid of the security and privacy breaches. Some people say the global computer network should be free, but total freedom brings chaos. We are all humans. We are limited by our intelligence, emotions, and instincts. Limitations make us people. We are not free from breathing, drinking, eating, and sleeping. Everybody should be aware that there have to be laws that bring order. The proper order can improve security. Privacy protection could not relieve people from liability. The problem is that the laws are not clear enough for the people to know how exactly they are expected to behave. Even the companies that legally registered their businesses faced legal problems afterwards. The biggest problem in making regulations for the global computer network is that it connects the users from all around the world, but different states have different laws in effect. To overcome this issue, the globalization process could help. The effect of the globalization could be increased by the engagement of all people. Every person from all around the world should contribute to the process.

REFERENCES

Altheide, David L. 2009. "Terrorism and the Politics of Fear". Pp. 54-69 in *Cultures of Fear: A Critical Reader,* edited by Uli Linke and Danielle Taana Smith. London, UK and New York, USA: Pluto Press.

Bosker, B. 2013. "How Facebook Explains User Data Bug That Leaked 6 Million People's Information". *The Huffington Post.* Retrieved March 28, 2015 (http://www.huffingtonpost.com/2013/06/25/facebook-user-data-bug_n_3492889.html)

Buford, John F. and Yu H. 2010. "Peer-to-Peer Networking and Applications: Synopsis and Research Directions". Pp. 3-45 in *Handbook of Peer-to-Peer Networking,* edited by Xuemin Shen, Heather Yu, John Buford, and Mursalin Akon. New York, USA: Springer.

Cerf, V., Dalal Y., and Sunshine C. 1974. "Specification of Internet Transmission Control Program". *Request for Comments 675.* Retrieved March 28, 2015 (https://www.ietf.org/rfc/rfc675.txt.pdf).

Cvetkovski, Lj. 2013. "Analysis of the Trend of Using Peer-to-Peer File Sharing Applications Among the Population of the Republic of Macedonia". Master's Thesis, Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University. Skopje, Republic of Macedonia.

Furedi, F. 2002. *Culture of Fear: Risk-taking and the Morality of Low Expectation.* Revised Edition. London, UK and New York, USA: Continuum.

Giddens, A. 2009. *Sociology.* 6th ed. Cambridge, UK and Malden, USA: Polity Press.

Guillard, S. 2011. "Austrian student sues Facebook for keeping 'deleted' data". InterAksyon. Retrieved March 28, 2015 (http://www.interaksyon.com/article/17218/austrian-student-sues-facebook-for-keeping-deleted-data).

Hafner, K. and Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* New York, USA: Simon & Schuster.

Iseini, M. 2008. "Truth about Albanian-Macedonian Conflict". Selection of Texts about the Conflict in 2001. Skopje, Republic of Macedonia: Foundation Institute Open Society.

ITU. 2014. *Measuring the Information Society Report 2014.* Geneva, Switzerland: ITU.

Kelly, T. and Baker, Liana B. 2011. "Massive data theft: 77 million users exposed in Sony's PlayStation security breach". *The Globe and Mail.* Retrieved March 28, 2015 (http://www.theglobeandmail.com/technology/gaming/gaming-news/massive-data-theft-77-million-users-exposed-in-sonys-playstation-security-breach/article577882/)

Kirk, J. 2010. "Facebook privacy slammed by European data protection officials". *ComputerworldUK.* Retrieved March 28, 2015 (http://www.computerworlduk.com/news/it-business/20269/facebook-privacy-slammed-by-european-data-protection-officials/?intcmp=in_article;related)

Matevski, Z. 2009. "Religious Tolerance in Republic of Macedonia – Are the National Interests Stronger Than Ecumenical Conscience?" in *Religion in Modern Society.* Skopje, Republic of Macedonia: Faculty of Philosophy.

Postel, J. 1981. "Internet Protocol". *Request for Comments 791.* Retrieved March 28, 2015 (http://tools.ietf.org/pdf/rfc791.pdf).

Robinson, William I. 2007. "Theories of Globalization". Pp. 125-143 in *The Blackwell Companion to Globalization,* edited by George Ritzer. Oxford, UK: Blackwell Publishing.

Ryan, J. 2010. *A History of the Internet and the Digital Future.* London, UK: Reaktion Books.

Sandvine. 2014. *Global Internet Phenomena Report 1H 2014.* Retrieved March 28, 2015 (https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf)

United Nations. 2015. "UN at a Glance". Retrieved March 29, 2015 (http://www.un.org/en/aboutun/).

Veljovski, Gj. 2010. "The Effectiveness of the Counterinsurgency Operations during the Macedonian Conflict in 2001". Master's Thesis, Faculty of the U.S. Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

ГЛОБАЛНАТА КОМПЈУТЕРСКА МРЕЖА И ОПШТЕСТВЕНАТА ТРАУМА

Љупчо ЦВЕТКОВСКИ

Апстракт: Глобалната компјутерска мрежа има значаен придонес кон постоечкиот процес на глобализација што ги интегрира општествата во секој аспект. Истовремено, таа носи предизвици во светот кои треба да бидат решени. Овие предизвици претставуваат опасност што може да предизвика општествени трауми. Компјутерската мрежна технологија и законите за интелектуална сопственост не се доволно познати за и разбрани од сите. Присуството на страв може да се потврди со анкетата што ја спроведов во 2013 година меѓу компјутерските корисници во Република Македонија. Анкетата покажува дека корисниците не се против постоењето на законите и дека се подготвени да платат за услугите, иако имаат различни мислења за правилата и начините на плаќање. Најважната информација од анкетата е дека корисниците се плашат од опасностите по безбедноста и приватноста. Нивниот страв не е искажан директно, но може да биде екстрахиран од нивните одговори. Мојот генерален заклучок е дека сите луѓе треба да бидат повклучени во процесот на глобализација за да ги надминат општествените трауми. Секоја личност од светот е општествено суштество и треба да придонесува во глобалното општество.

Клучни зборови: мрежа, закана, траума, анкета, глобализација.