Aleksandre Glonti
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
Giorgi Alavidze
John Jay College of Criminal Justice, New York, USA

EXPLOITATION OF CYBERSPACE FOR PURPOSES OF RETALIATION IN COUNTRIES WITH ECONOMIC AND POLITICAL TRANSITION ON THE EXAMPLE OF GEORGIA

Abstract

This thesis investigates acts of retaliation and deterrence conducted through internet that are specific to post-Soviet Union countries.

In modern world, acts of retaliation partly transcended from real to cyber world, reaching its highest levels. On one hand, this is influenced by the lack of legislative statutes that encompass discussed field, on the other, rapid advancement of digital technology has triggered various new methods of retributive justice.

Nowadays, retaliation using the internet is a well spread phenomenon. Active social players realized that implicit benefits of cyberspace, eventually, equipped them with high anonymity, fast proliferation of the information, and deficiency of the legislative acts related to cybercrime. Therefore collaboration of abovementioned three factors provides interested parties with an ultimate weapon for retaliation.

Key words: Cyberspace; Cyber crime; Cyber Retaliation; Cyber Warfare

An analysis of preliminary data, gathered in Georgia reflects that recent acts of retaliation through means of cyber space exploitation have significantly increased. In fact, high number of cases involving cyber retaliation substantively grew in the beginning of the second decade of the 21st century. Emergence of stated is relatively bind in a context with a political turmoil, economic instability and rapid social change.

Ultimately, contemporary acts of cyber retaliation include inciting religious hatred, agitation of massive reprisals against sexual minorities, using internet to spread violent ideas for political causes, suppressing rights of media and freedom of speech by the high-level officials, imposing terrorist threats, and finally, initiating quarrels among the members of the different internet communities that overgrow into grave conflicts in real life.

Remarkably, consequences of cyber-retaliation are civil unrest in the country, disregard of the articles stated in the Human Rights and Constitution, and protraction of growth of the democratic community.

Following sections attempt to frame the issue of specification of cyber-retaliation, namely problems stated in paragraph 5, in post-Soviet Union and other countries on the example of Georgia. Followed by historical overview, authors will provide an insight on theoretical fundaments, key assumptions, and conclusions.

1. Historical Overview

To some extent, all member countries of the former Soviet Union underwent a complex process of redevelopment in the end of the 20th century. The collapse of the union left many countries in an economic recession and political turmoil. While generally former member countries built their legislative, judicial and executive power systems on the example of the former Soviet system, Georgia, on the contrary, chose to implement variety of legislations typical for western countries, following the 2003 Rose Revolution.

Rapid transition from the Soviet to Western system has taken its toll, leaving the Georgian people with mentality and traditions often attributable to the former Soviet Union countries, while implementation of new laws and procedures dragged them into a more pro-western stylized legal system. Combination of both, traditions and rapid reformation negatively affected Georgian people. New types of crime patterns emerged, combining "eastern" and "western" manner of committing them.

In Georgia, traditional acts of retaliation were commonly historical. Over the past millennium, Georgians preferred to revenge against each other, rather than allow law enforcers to deal with the criminals. Blood feud and vendetta, though in decreased frequency, is still in existence in certain regions of country.

Over the second half of the past century, members of a well-known organized crime syndicate, thieves-in-law committed various acts of retributive justice, mainly based on the "eye for an eye" principle. Corruption and failure to combat organized crime gave thieves-in-law overwhelming power to impose cruel and unofficial laws and a mentality which ruled public for the upcoming decades. After their supremacy on the streets became non-negotiable, leaders of organized criminal groups started to penetrate government offices. These deviant government officials, in varying degrees, used means of retaliation for enforcing their will. After the 2003 Rose Revolution a new political party, "The United National Movement" took over government and started the reformation of the country's infrastructure. Together with a majority of other law codes, criminal law code and criminal procedure law codes were also renewed. Georgian society practically encountered the new legal approaches towards the thieves-in-law. These new legislative implementations generally focused on the combat against organized crime and corruption. With accusation of being corrupted, 16.000 policemen were fired instantly from their working places and replaced by new staff members. Newly recruited police officers underwent specialized trainings provided by joint cooperation of MIA police academy of Georgia, USA

Embassy and Bureau of International Narcotics and Law Enforcement. As a result of new legislative implementations, along with the "zero-tolerance" policing adopted by the government of that time, the organized criminal activities in Georgia were remarkably reduced. Traditional acts of retaliation, principally committed by members of organized criminal groups, almost seized to exist. However, abolishment of the traditional types of retaliation gave birth to novel methods of technological retribution.

2. Statement of Problem and Case Studies

One of the examples of such newly born types of retaliation is "cyber retaliation". It emerged after vast popularization of electronic computers and computerized gadgets. In case of Georgia, massive establishment of "cyber dimension" began in the beginning of the 21st century. This sudden shift formed new sources of delivering information to the public. While usually people use cyber space to communicate, interact, share information and work, there are societies that misuse this valuable source to their own advantage. Cyberspace is there for everyone to use – or to abuse [1].

The following paragraph will shortly frame, describe and introduce the recent examples of specific cyber-retaliation cases from Georgia, as well as from the former Soviet Union countries.

Acts of retaliation are believed to be more spread in countries that are in a transitional phase in terms of politics and economics. Sudden changes in the course of mentality are bound to have a negative effect on public obeying newly imposed laws and customs. Regarding Georgia, transition was fast, leaving the society confused about newly imposed lifestyle and behavior. The reformation of legislative and judicial systems caused, *inter alia*, misunderstanding between the government and the people that eventually led to massive protests and public meetings. As the cyber space became a primary source of information, leaders of opposing parties started to exploit it as a driving mechanism for their ideas and beliefs.

Since judicial system isn't yet well trusted, some groups prefer use of acts of retaliation, rather than mediation or punishment. While traditional retaliation is strictly prosecuted in Georgia, unpleased members of society started to use newly emerged possibility – namely cyber retaliation. Legislative background against cyber retaliation is still full of square brackets. In practice, existing statutes do not fully encompass cybercrime therefore it became one of the favorite instruments for adversaries.

A) Religion and Cyber Retaliation

Religious disputes caused acts of retaliation many times throughout the course of history. Up to the present time, countless number of wars was fought by representatives of various religious groups and denominations. Today this tendency still remains, however, strengthened by the new means of dissemination of the information - the internet. It has brought people from all over the world together, thus overcoming limitations of time, space and locality, and accelerating religious transnationalism and the flowing of the ideologies [4].

The rise of cyber network has a profound impact on the way conflicts are carried out and the faithful practice their religions. Nowadays, online religious communities use cyber space as an instrument to preach their beliefs, provide advices for concerning religious doctrine, answer pilgrims' questions, and otherwise spread the religion. Some websites, like www.patheos.com, also combine teachings of different religions. As pointed out by Hojsgaard and Warburg (2005a, p. 2), by 2004, the number of religious web pages had grown considerably worldwide, with up to approximately 51 million pages on religion, 65 million webpages dealing with churches, and 83 million webpages containing the word of *God*.

While the purpose of these online tools is to spread belief to the masses of people, preaching humanity and social order, sometimes these same sources become epicenters for disputes and spreading of religious hatred. This in fact, the other side of the coin, still remains to be an uphill battle for the law enforcement agencies worldwide.

Present-day religious conflicts usually start with a minor incident. These occasions are normally settled locally; nevertheless, sometimes they fall under the highlights of certain media broadcasters. Internet is one of such broadcasters, which allows its users to make their comments concerning occasions that have occurred. Since incident involves two, or more, opposing sides, supporters of each side have equal chances to express their points of view concerning what happened. Comments often include violent hate speeches and harassment of opposing side, which eventually leads to an act of retaliation from the harassed side. Finally, a small incident that would rather be forgotten in a short period of time might overgrow into severe conflict that is supported by followers of opposing groups worldwide. Unstoppable queue of the acts of cyber retaliation from both sides may ultimately result transcendence from cyber to real life retaliation.

The classic example of using cyber space as an instrument of retaliation was a massive online dispute that resulted in taking down Islamic minaret on the 26th of August 2013 in village Tchela, in Adigeni region of Georgia. Process itself caused clash of the law enforcers and the representatives of the Muslim community. Prior to the act of demolition of the minaret, Christian dwellers of the village Tchela have protested against construction of the Islamic religious symbol, which eventually grew into public unrest and altercation between opposing groups. Via internet, local disagreement became a matter of an argument in the Georgian internet domain, as well as, involving activities of the countless followers of Muslims and Christians. Acts of cyber retaliation stemming from both sides of online quarrel finally overgrew into a real life conflict.

Another example is "The Moluccan Conflict" of Eastern Indonesia. Due to their seemingly harmonious lifestyle, nobody really expected that a minor quarrel between a Christian bus driver and a Muslim passenger in Ambon town in January 1999 would end up in a bloody and enduring multidimensional conflict: hundreds of churches and mosques were destroyed, thousands of

people on both sides were killed, and hundreds of thousands had to flee - nearly one third of the Moluccan population [5].

Both abovementioned incidents were triggered by the constant acts of retaliation in the cyberspace. Both incidents occurred under the circumstances in which a dispute, in general, should have been settled down locally. However, rapid dissemination of these minor occasions via Internet has resulted in a massive aggression of members of affiliated religious groups worldwide against each other. In both cases religion itself was not the cause of the civil unrest. It was the people involved in it that very soon grouped around the religion as their prime marker of identity.

B) Sexual Orientation and Cyber Retaliation

Social minorities, in particular, often become victims of hate speeches and hate crimes. Information-communication technologies act as a force amplifier, enhancing power and enabling social actors to raise their weight and attain a reach and influence pro or against these minorities. Preliminary analyses show that together with the popularization of the internet, as a source of mass media, acts of harassment, humiliation and retaliation against minorities have seemingly increased in number. While both, traditional and internet based retaliation acts, have a number of similarities, latter has taken severity of humiliation and abuse to its highest levels. Among other groups of social minorities, members of lesbian, gay, bisexual and transgender (LGBT) communities are one of the most target groups on the worldwide web.

In Georgia obvious acts of cyber retaliation against LGBT persons began in the second quarter of 2012, following an incident of 17th of May - International day against homophobia, biphobia and transphobia. A sudden appearance of the members of the *Pride* parade in the center of Tbilisi led to a minor conflict involving demonstrators and random bystanders. While law enforcers were successful in suppressing the aggression, this incident had a wide discussion on the web, accompanied by many hate speeches and agitations of violence against LGBT persons. This first attempt to put the issue of LGBT rights on stage in Georgia was soon forgotten.

Police forces, however, experienced real difficulties during *Pride* parade held on the same day, next year. This time both sides of conflict, the LGBT demonstrators and the opposing groups, were well prepared. Georgian cyberspace was filled with advertisements prior to the planned parade, encouraging members of sexual minorities to participate in an organized march in the center of the capital city. These advertisements were not ignored by the opposing groups. First spark that later ignited huge fire was lit on the internet and the media. Prior to the International day against homophobia, biphobia and transphobia, adversary parties retaliated against one another using the internet. Local news broadcasting websites and social networks became a whirlpool consisting of hate speeches, agitation toward aggression, and calls of uniting against demonstration planned by the LGBT persons. As expected, many thousands of people gathered to oppose the *Pride* parade. To disallow physical violence LGBT parade participators were safely

removed by the police forces. Official sources confirm dozens of protestors got injured. Acts of traditional and cyber retaliations lasted for months after the failed parade itself.

Analyses of both cases clearly show that it was the internet that played a major role in the second encounter. In 2012, few to none advertisements of the planned pride parade took place. General public wasn't aware of gathering of the LGBT individuals, thus there were no means to alter it. Nevertheless, many acts of cyber retaliation were initiated against the demonstrators afterwards. In second case, internet broadcasted planned parade prior to the date. Discussions over LGBT gathering literally flooded news, blogs, forums and social networks. There, radicals expressed their hostile attitude towards organizers of the *Pride* parade, banned celebration of the international day against homophobia, biphobia and transphobia in Georgia, and called for the reinforcements of accomplices to massacre demonstrators.

Relatively similar incident was witnessed on the 17th of May of 2013 in Moscow, Russia. Leaders of LGBT societies trying to organize a parade for supporting rights of sexual minorities were attacked by members of the nationalist group. A physical encounter between opposing parties forced the police to take confrontational measures and arrest aggressive radicals from the both sides. Prior to the planned parade, a huge wave of advertisements of *Pride* parade was published in the Russian cyber space, resulting relatively same consequences as there were in case of Georgia.

It is clear that internet has increasingly become the battleground for the fight for recognition. If certain preventive measures will not be enacted, it might be only a tip of an iceberg that has been encountered so far. Nevertheless, some former Soviet Union countries were successful in taking first steps toward the recognition of LGBT rights. Same march has succeeded in Ukraine, while still encountering problems from opposing groups.

C) Cyber Retaliation as an Element of Cyber Warfare

Cyber warfare occurs when one country perpetrates a cyber-attack against another country that would to the reasonable person constitute a state act of war [13]. Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare [16]. Richard A. Clarke defines cyber warfare as "actions by nation-state to penetrate another nation's computers or networks for the purposes of causing damage disruption" [3]. Similarly, former NSA and CIA director Michael Hayden referred to cyber warfare as the "deliberate attempt to disable or destroy another country's computer networks" [14].

While definition of cyber warfare has been, more or less, coined, causes of cyber warfare apparently are in need of further criminological research. Needless to say, that defining cause of a certain problem is usually a key to enacting effective means of preventing, ultimately, solving it. This article isn't intended to enumerate or investigate causes of cyber warfare, but rather point out one of the potential causes – the cyber retaliation.

Analyses of facts gathered clearly show that cyber retaliation is usually a hostile answer to a prior belligerent action and/or a cyber-attack. Yet, cyber-attack is defined as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions" [2]. It can be assumed that cyber retaliation is an act of cyber-attack from defending side motivated by previous cyber or other attack made by offending side.

While term cyber-attack may sound, more or less, harmless, consequences may result scenarios ranging from virus that scrambles financial records or incapacitates the stock market, to a false message that causes nuclear reactor to shut off, or dam to open, to a blackout of air traffic control system that results airplane crashes – anticipate severe and widespread economic or physical damage [11]. While none of the enumerated scenarios have thus far occurred, numerous cyber-incidents occur regularly.

Cyber warfare initiated by Russia against Georgia in beginning of August of 2008 may be referred to as an act of cyber retaliation, following Georgia's military campaign against South Ossetia. On 9th August part of Georgian cyber space was compromised. An official websites of ministry of foreign affairs and parliament of Georgia along with commercial and financial institutions were "defaced" [17] and compromised with the distributed denials of service attacks. In fact, hackers replaced original content of webpages with images that expressed visual similarities of the former president of Georgia Mikheil Saakashvili and Adolf Hitler. Officially not confirmed, yet number of facts point out to a blackout of the communication systems in Georgia, thus leaving the military forces without means of communicating with each other. The Russian side of the mentioned conflict blames Georgia of an act of cyber retaliation against Russian internet news broadcasters.

Similar scenario took place in Estonia in the spring of 2007. Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyber-attacks, which led to a massive shutting down of websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters [19]. According to the Guardian reports the cyber-attacks began in late April, coinciding with Estonia's decision to move a Soviet World War II memorial, the Bronze Soldier, from a central location in Tallinn, the Baltic nation's capital.

Further example of cyber-attack is Iran's nuclear program grounded to a halt, the subject of sophisticated cyber-attack that sent centrifuges spinning widely out of control. It was not a tangible weapon that caused this. "Stuxnet", a computer "worm" [18] that appears to have many authors from around the world, targeted Siemens industrial control systems compromising its normal operation. This cyber-attack is believed, yet not confirmed, to be conducted by United States and Israel joint cooperation as an act of cyber retaliation against Iran's political course.

Landmark examples above demonstrate three acts of cyber retaliation, hence not officially named so. In all three cases, a cyber-attack followed certain acts conducted by defending sides, opposing interests of offending side. While enumerated incidents haven't caused severe damage, incident with "Stuxnet" malware could have resulted irreparable wrong.

D) Government using Cyber Retaliation and Deterrence against Media

Freedom of expression is a fundamental human right as stated in the Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" [15].

United Nations declare freedom of media and press a worldwide priority. Free, independent and pluralistic media is considered as an example of good governance in both, young and old democracies. Such media ensures transparency, accountability and rule of law; it promotes participation in public and political discourse; finally it contributes its toll to the fight against poverty.

Media, to some extent, is unofficially referred to as fourth branch of power, after traditional *trias politica*, which occasionally is accepted in many countries. It can be a powerful tool to control government and prosperity of democracy in the country. Hence, main responsibility of the media is delivering of objective information to the general public, sometimes it falls victim of suppression from the representatives of other three major power branches, resulting skewing of the delivered information. Essentially, these are the same powers that deter the representatives of the media groups, forcing them to inform general public with certain information that is advantageous for their own purposes. This is, perhaps time worn accusation, however outcome of it is usually an act of underreporting of the actual situation, eventually leading to a serious protraction of advancement in a country.

Case studies show that the suppression of the rights of the media through deterrence is a somewhat of an often occasion worldwide. Usually, a whole broadcaster, or sometimes, individual journalists are being targeted by certain government officials or political party in order to skew information, or neglect some acts, to their own advantage. Since, there are no legal means for officials to force media to underreport certain acts, they usually use means of threatening and sometimes acts of retaliation. Nowadays, cyber technologies opened a new boundary for acts of retaliation – the cyber retaliation.

Meanwhile, absolute majority of the acts of deterrence against representatives of the media remain in secrecy, one scandalous incident that took place in Georgia on May of 2013 led to a disclosure of obvious fact of cyber retaliation. On 5th of May of 2013 ministry of internal affairs of Georgia initiated an investigation of criminal case envisaged by first part of article № 157 of Georgian criminal law code – namely "intrusion of privacy of the citizen of Georgia" [7]. Case involved a journalist and a former deputy minister of internal affairs. According to the case

details, latter used internet to disclose secret surveillance video materials, captured by special team of operators from the former department of constitutional security department of the ministry of internal affairs of Georgia, uncovering certain details of journalists' sexual orientation. Prior to dissemination of videos via internet, journalist wrote an article in a newspaper, accusing personal adviser of prime minister of Georgia, deputy of the chief prosecutor of Georgia, and former deputy minister of foreign affairs of illegally overtaking a certain business company. As victim claims, there has been a sequence of threats against him before publishing mentioned article. Journalist neglected acts of deterrence against him, and soon became victim of cyber retaliation. On 12th of May of 2013 former deputy minister of internal affairs was found guilty of criminal act envisaged by the second part of article № 157 of criminal law code of Georgia [8].

Above mentioned incident brought another disturbing fact to the surface. Now former minister of internal affairs, Irakli Gharibashvili announced that ministry of internal affairs of Georgia possesses more than 25 000 hidden audio and video materials, whereas some of them may contain data that depicts private life. According to official statement of Irakli Gharibashvili, on 5th of September of 2013 hidden materials contained on 110 storage disks were destroyed [9]. Remaining materials will be overlooked by a special commission which is obliged to determine if they contain data on private life.

Case study shows that mentioned hidden audio and video data was used as compromising materials against individuals by acting members of the government. Main purpose of these materials was to deter certain social actors, thus forcing them to unwilling cooperation with representatives of certain government agencies.

Present officials of ministry of internal affairs of Georgia admit that certain people from former government had an access to these hidden materials, therefore it is hard, if not impossible, to determine how many copies have been made and/or who possesses these materials now. Assumption is however obvious. These data may still be used by the unknown possessors to deter or retaliate against social actors that are, so to say, unwilling actors these materials.

E) Political Cyber Retaliation

Throughout the course of history, politicians often used different sophisticated schemes to compete for the power. In the politics, campaign advertising is considered as one of the most important means to emphasize the political activities. Internet, with its endless informational capabilities, recently became a strategic/operational "center of gravity" of an advertisement of the political campaigns. Moreover, today internet's features and possibilities challenge the traditional patterns of authority in the "Information Age".

While cyber space is sometimes used as a driving mechanism of political advertisement, its "other side of the coin" may be using of it as a powerful instrument of anti-advertisement. Politicians are well aware of this tactic and are widely using it nowadays. "War has rules, mud wrestling has

rules - politics has no rules" [14]. Having similar quotes and thoughts in mind, some politicians or political parties neglect the articles imposed in law and engage in political arena without recognizing certain unwritten principles. While legislation has arguably a narrow scope on cyber space, internet has become a favorite tool for political backdoor activity. It provides these social actors with unlimited variations of schemes they may utilize against their adversaries.

However, the idea of cyber space as an "offshore" propaganda tool is fast spreading. If one political party started using it, opposing political party might use it as well. With existing legislation acts, cyber space provides almost no limitations to the members of a political arena to take part in an "electronic battle for power", thus leaving the general public aside as spectator of the ongoing clash. Although,"Du choc des opinions jaillit la vérité[1]", sometimes "electronic political battlefield" turns into a place of cyber retaliation.

Theoretically, it can be assumed that both opposing political actors have same proportion of power to compete in for their causes. Everything seems legit – equality is granted to both sides of competition. However, general public, here assumed as spectator of ongoing political collision, may sometimes fall as a victim of the endless cyber retaliation acts of this ongoing opposition.

An incident that took place in Georgia in June 2013 has all its bonds tied to the cyber space. An unknown user of popular video portal Youtube has uploaded clip named "Taliban Jihad against Georgian Troops in Afghanistan" under the nickname of "Hammad Zaman". Video presented a clear threatening message to the members of Georgian armed forces serving in an ISAF mission in Afghanistan. It showed pictures of killed Georgian soldiers with audio accompaniment which stated that "same fate awaits all remaining Georgian troops participating in *crusade* against Afghanistan." This message also included a threat of retaliation against former president of Georgia and all the Georgians, finalized with a statement: "we will punish you!"

The investigation body concluded that uploader of the mentioned video is a citizen of Kyrgyzstan, Samar Chokutaev who currently lives in *de facto* republic of Abkhazia [10]. According to an official statement of the spokesperson for the ministry of internal affairs of Georgia, Chokutaev was found guilty by the decision of the Tbilisi city court in a criminal act - "publicly disseminating information on encouraging commitment of the terrorist act that creates threat for committing of such crime" envisaged by article 330[1] of criminal law code of Georgia".

Discussed incident provides food for thought for criminologists, sociologists and/or representatives of other scientific fields. On one hand, what was driving force, a motive, of this conduct, on the other hand - who has benefitted from it? Meanwhile, aim of this article is not investigation of the abovementioned case; it can arguably be assumed that mentioned act is closely tied with political anti-advertisement or, perhaps, an act of cyber retaliation against certain political party.

[1] "From the clash of opinions emerges the truth"

Due to certain characteristics, described incident may be accounted as new way of cyber retaliation in post-Soviet countries. Although beneficiary of this act is not clear, one fact remains certain – Video "Taliban Jihad against Georgian Troops in Afghanistan" caused serious moral panic in Georgia (spectators), especially after *coincidence* that after two hours from the upload of the mentioned video 3 more Georgian soldiers were killed in Afghanistan.

3. Conclusion, Theories, and Key Assumptions

Statement of problem and case studies clearly show that cyber retaliation has become a considerable issue in Georgia and in the modern world. Research shows that the legal framework overall is not yet compatible to encompass cyber retaliation phenomenon, thus neglecting certain types of deviant acts that participators may commit against each other, or against society.

An act of deterrence may be considered another key assumption that usually takes place prior to an act of cyber retaliation. Deterrence itself may be committed using cyber instruments, or without. Nevertheless, as described in paragraph (D) of second article of this article, fearing an act of retaliation in the cyber space victim of deterrence may be seriously limited in own fundamental rights granted by the Constitution and The Human Rights. Ministry of internal affairs of Georgia has once already failed to secure all the hidden audio/video materials. This fact may only strengthen fear of being retaliated against. Since up to now, there is no clue concerning individuals who currently possess discussed hidden audio/video materials, it is logical to assume that freedom of expression and/or other fundamental rights of Georgian people are severely strained.

Why is cyber retaliation so popular? In particular, several theories can be applied.

Firstly, cyber space became primary instrument of the “information highway”. With the amount of users growing each day, more and more spectators join “international goggles” of observation. Paragraph (A) of second article of this proposal demonstrates how may a petty local incident, strengthened by the cyber retaliation instruments, transcend into a massacre.

Secondly, speed of dissemination of the information in the cyber space leaves no doubts that facts will reach targeted society swiftly. Nowadays, Internet provides its users with information 24 hours a day. Facts that were once uploaded to the internet will eventually remain there, thus leaving almost “non-washable stains”. Cases described in paragraphs (B) and (C) of second article of this proposal show how rapid could effects of cyber retaliation occur. In fact, cyber-attack launched by Russia against Georgia paralyzed Georgia cyber space in the matter of two days. Same is true in case of Estonia. Sequence of messages spread on forums, social networks and other sources of information on the internet instantly gathered thousands of people in the center of Tbilisi.

Finally, internet may guarantee an individual with anonymity which sometimes is impossible to trace and/or uncover. In majority of cyber related criminal incidents, it is infeasible to identify

the criminal. Hence criminal has been identified; legislation which only partly covers cybercrime isn't usually capable of encompassing certain deviant acts. Live example of this assumption is occasion described in paragraph (E) of the second article of this article. According to official declaration of spokesperson of ministry of internal affairs of Georgia, uploader of the indicated video was found guilty by decision of the court in the criminal act - "publicly disseminating information on encouraging commitment of the terrorist act that creates threat for committing of such crime" envisaged by article 330[1] of the criminal law code of Georgia." Theoretically, author did publicly disseminated information with threatening of commitment of the terrorist act. However, nor author, nor the act itself possessed threat to Georgia or its citizens. Discussed fact clearly points out that legislation is yet several steps behind of the technological progress.

Overall discussion is aimed to emphasize the fact that cyber retaliation issue has to be put on the agenda. Ignoring it may create substantial obstacles and cause disruption if it remains outside of limits of the power of the legislation. In terms of cybercrime, we are already starting with a handicap of decades. Criminologists, sociologists, and experts of the field should work in cooperation with legislators and responsible government bodies, combining theoretical and empirical studies. A further research must be carried out to measure true extent of deviant conducts related to cybercrime and cyber retaliation. Establishing a credible source of quantitative data and properly carried out fieldwork will, eventually, provide a good lode from which to mine insights and hunches.

References

1. Adler F., Mueller G.O.W., Laufer W. S. *Criminology 7th Edition.*
2. Gen. Cartwright J. E. Nov. 2011. Chiefs of the Military Services. Commanders of the Combatant Commands, Dirs. Of Joint Staff Directories. *Joint Terminology for Cyberspace Operations 5.*
3. Clarke & Kanke. Aug. 2011. *More than Firewalls: Three Challenges to American Cyber Security, Asymmetric Threat.*
4. Eickelman.1997. *The Middle East and Central Asia: An Anthropological Approach.*
5. Eckert J. 2007. *Citizenship Studies.*Volume 11, Issue 4.
6. Miller & Slater. 2000. *The Internet: An Ethnographic Approach.*
7. Ministry of Internal Affairs of Georgia - *http://police.ge/ge/shinagan-saqmeta-saministros-gantskhadeba/279*
8. Ministry of Internal Affairs of Georgia - *http://police.ge/en/shinagan-saqmeta-saministros-gantskhadeba/4673*
9. Ministry of Internal Affairs of Georgia - *http://police.ge/en/shinagan-saqmeta-saministros-gantskhadeba/5451*
10. Ministry of Internal Affairs of Georgia - *http://police.ge/ge/terorizmis-shesakheb-muqaris-ets-djihadis-videos-saqme-gakhsnilia/5598*
11. Hathaway O. A. Collective of Authors, Yale Law School - *Law of Cyber-Attack.*

12. Ross Perrot Quote.
13. Dycus S. S. *Congress's Role in Cyber Warfare.*
14. Gjelten T. *Extending the Law on War to Cyberspace.*
15. United Nations Website - *http://www.un.org/en/events/pressfreedomday/background.shtml*
16. Wikipedia - *http://en.wikipedia.org/wiki/Cyberwarfare*
17. Wikipedia - *http://en.wikipedia.org/wiki/Website_defacement*
18. Wikipedia - *http://en.wikipedia.org/wiki/Computer_worm*
19. Christian Science Monitor - *http://www.csmonitor.com/2007/0517/p99s01-du*