Computer-Mediated Security Threats into the Web 2.0 Society

Bogdan Nadolu
Department of Sociology, West University of Timisoara, Blvd. V. Parvan 4, Timisoara 300223, Romania
bogdan.nadolu@e-uvt.ro

Delia Nadolu
Department of Sociology, West University of Timisoara, Blvd. V. Parvan 4, Timisoara 300223, Romania

Abstract

This paper is focused on a contemporary very complex and controversial issue related to the ICT using: should the Internet be censured, or not? The promise of the 4 of A – Anyone to be able to send Anything, Anywhere, Anytime is almost achieved. Into the digital universe we can find plenty of useful information for positive or negative actions. The global info-sphere has developed a distinct chapter of dark and deep web, where the tracking of information and users is blocked, and thus contents over the laws limits can be easily accessed.

1. Introduction

The general profile of the Internet remains a quasi-anarchic one, with various alternative connections between any two terminals, with a high level of control on the defining of the own identity (and thus with a high potential of anonymity, usually on the principle *I am what I am write*), with a special definition of *to be in virtual space*, based on *to act* and that in almost all situation means *to write*. Significantly, with the absence of power resources that are usually present in any face to face interaction, and thus the self-censure and social distance are more volatile, in the virtual space is easier to access unknown people because they literally are only *virtually* close to you, they cannot reach you directly. More than half of the Earth's population is already on-line and thus *social media*, as an important component of the Internet generates a huge challenge for the public security planning. Traditionally, security planning was far more territorial, limited by rules, laws, and principles of one particular jurisdiction, which is comparatively outdated when the promise and reach of the internet is Anyone (sending) Anything, Anywhere, Anytime.

2. State of the Art

Social media has already been used in events which threaten security, such as the uprising in the Arab Spring across North Africa, and in the London and Manchester riots in the UK (ACPO 2013). It is certain that social media will have an increasing role in any other similar events. Often the first news (and that which is most likely to be influential) is received by the public from social media and not from the usual news channels via television or print media. The disruptive elements in society may also use social media to plan, organize and control such events. However, given the emerging pattern of using social media to promote terrorism, there are efforts reported in the news (Workman, Bommer, & Straub: 2008) to include security measures in social media. Another main problem is that Internet and social media are borderless and not constrained by the laws and regulations of a single country, making it difficult for any country to impose its laws and maintain its national security effectively when a threat is generated on social media.

Social media can generate new kinds of risks, creating vulnerability to attack, and stimulating threats and dangerous activities. It is obvious that the Internet and social media usually cannot be shut down (only on a limited area, under the totalitarian regime), as there is a lack of centralized control over both entities. It is also obvious that it is almost impossible to guard against the musing conventional approaches when confronted by virtual behavior and computer-based manifestations of terrorism. The virtual social networking can be used for anticipating various collective behaviors (i.e. the advancing of a current of public opinion, or the manifestation of some trend for or against a subject etc.) It is also important to monitor the social media in order to identify the current agenda (the most relevant topic discussed into the public virtual space). Social networking tools can be used for getting insights, to establish potential threats, to identify perpetrators, to discover threatening organization topologies, identifying potential escalations, and also heeding expressed community fears and expectations. Also, social media may be used to predict possible security threats. Open data is available for this kind of investigation, as there is no privacy restriction, and also this leads to greater security in society. Private data shall be used only according to the privacy policies and laws of the country/territories where such predictions are made. (Zevenbergen, 2015)

During the Romanian presidential election in November 2014, on the 2nd tour, social media had a central role in generating a so-called social tsunami, changing the prediction of any sociological poll, by motivating and bringing to vote up to 1 million people (in only one day of inefficient organized vote abroad, with plenty of small videos shared on Facebook[12]). When access to social media is relatively easy, it can simply be used to quickly spread any kind of content, which can create an emotional impact that, in turn, can generate a strong social movement.

The extremist movement (including here the terrorist's activities) can expose their cruelty via social media to expose their doctrines and to convert those who will do the same. Security planning is not bound by legal and ethical implications when using open data from social media, as this is, by nature, open and public. When it comes to private data, the procedures should respect the existing and new regulations from the country/territory where it is used. When new regulations are done, there should be taken into account the international regulations that exist, such as the fundamental human rights (Article 8, ECHR). On the other hand, with very few restrictions, any communication on the social media is a public one. If the information is not in a direct peer-to-peer message then any kind of post, share, like, or other manifestation would be considered public and can be monitored, recorded, analyzed without any explicit permission from the owner as the public nature of his or her message is implicit.

New criminal trends have emerged, with people committing crimes in cyberspace that they would not otherwise commit: the anonymity of the Internet utilization, its quasi-anarchic structure and the possibility of adopting flexible identities can be incentives for criminal behavior. Criminals can gain access to large numbers of targets through online services such as banking, shopping, and social networking. Global connectivity also means criminals can learn from each other, even if they never meet. Online criminal "social networking" can provide forms of criminal "outreach", and links between criminal groups. A false impression of social acceptability of criminal acts such as child sexual exploitation can be created by online communities.

There are many ways information and communication technologies are driving new and emerging crimes. Consumer financial fraud has become transnational with the now-commonplace use of online payments. Global incitement to violence and terrorism through social media has widened the reach and influence of previously localized radical and terrorist groups. Illicit drugs and other products can be bought online, paid for with anonymous virtual currencies[13]. Criminal groups operate in new ways, hiring specialists to perform tasks that are not covered by their existing knowledge and skills. This trend of a more transient and less structured organization may be how serious crime will be perpetrated in the future. The use of modern technology in criminal activity is

[12] More details about this event http://www.telegraph.co.uk/news/worldnews/europe/romania/11249449/Romanian-presidential-election-does-Klaus-Iohanniss-victory-prove-social-media-can-win-an-election.html which helped me to rephrase the paragraph to this: During the first round of the Romanian Presidential elections in November 2014, social media had a central role in generating a social tsunami, in which the Romanian diaspora around Europe voiced their discontent at the way in which the elections had been handled. The government's difficulties in dealing with the election had been exposed and claims of undermining democracy had been shared, between Romanians, across Europe using hashtags.

[13] According with http://gjis.journals.yorku.ca/index.php/gjis/article/view/38935

doubtless increasing, but established methods such as bribery and corruption continue to be important in the way these new crimes are carried out, particularly for illicit cross-border trafficking and movement.

The digital environment is deeply affecting the meaning and use of media and information. The social media provides opportunities and challenges at all the levels of society. Continuous technological developments create and publicize an ever-growing amount of content and information as well as new online spaces. They introduce new issues, challenges, and possibilities, as the Internet scenario goes mobile, ubiquitous, and multiplatform. Individuals gain more control over their roles as media creators and critics, and not only consumers. Social media and social network sites take on added relevance, as they serve as references to new forms of social interaction, as well as new rights and participation models such as global citizenship in a digital age on one hand, and polarization on the other. We are constantly witnessing the blurring of ground democracy. The cyber world is creating new unmanned and intensely webbed societies. This does pose a security threat, as conducting a country under law and order takes on a new dimension in the cyber-sphere of lawlessness. The digital universe is developing with a considerable speed. The web 2.0 has made a deep change of the paradigm concerning the internet users' behavior, by shifting the status from passive consumer to active user content generator. It is expected that in the further web 3.0 level will be implemented applications of AI that will produce self-generated web content which is quasi-independent from the human implications. In this perspective, any control of the information, produced and circulated into the Internet, will be almost impossible.

Easy availability of information sharing apps and mobile technologies generally increases awareness amongst populations, even amongst the rural populations which are otherwise ill informed. This is a positive development which brings with it the risk of uprisings, unrest, and disorder. Like Arab springs more uprisings can be expected as populations become more informed and have the ability to communicate their concerns. Realization of massive disparities will come (have come) in front to compare notes and exchange views. Divides of "have" and "have not" will dangerously expand - and this will result to resentment, discontentment, and violence, of course. Crime persists, and those who carry out criminal activities – such as drug lords and terrorists – will be further enabled with the development of social media and technology. Social media has also privatized violence. The criminal net-warriors increasingly employ information operations to add to their barbarization and high order violence. The brutal campaign of the Islamic State carving its way across Iraq and Syria reflects a decade-long trend in world politics – the intensifying privatization of violence at a faster speed due to social media tools.

The very tools of social media, which is causing widespread unrest in the world, must be utilized in a way that becomes a tool for security. This does not mean to abandon traditional practices of the law enforcement community, but to use social media as an enhancer and enabler of the traditional techniques. By 2020 there will be 50 billion networked devices; such connectivity will increasingly become part of our everyday life. The mobile phone was already declared in 2012 by the World Bank the technology with the highest impact on short time over humanity (in 2012 ¾ have had access to a mobile phone). The data from these devices is and will increasingly shape our societies and economies and our view of the world. We already have a continuing quick increasing info-sphere and also a very consistent cyber-sphere with very complex consequences concerning the human behavior and its strengths and weak points. Facebook has a 5,000 friends limit that any single user can add, but it has now been proven that our brains themselves are only capable of managing a maximum of 150 intimate friendships ones that are reciprocal and based around general obligations of trust reciprocity (Dunbar, 2010)[14].

Another piece of research has shown that hyperconnectivity produces "memoryless" individuals where the activation process is driven by social reinforcement at neighborhood level.

[14] This is due to evidence based finding by Oxford University Professor Robin Dunbar, in which he asserts that the part of the brain used for conscious thought and language development; the neo-cortex limits us to managing an average of 150 close friendships, no matter how social we are.

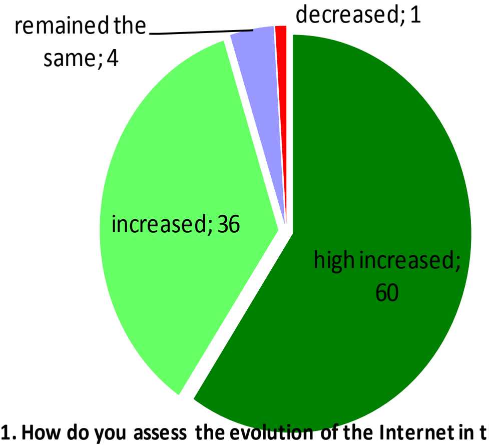
The active (or non-active) states of his or her social neighbors at each time step act as a "topological memory", causing the individual to be activated with a larger probability example: if most of an individual's friends are tweeting and re-tweeting a rumor repeatedly in time. High connectivity also reduces critical thinking, posing a greater challenge in terms of security, be it individual or collective. Terrorist radicalization and recruitment of youth to violent extremism and terrorism appear, in many instances, based on social bonding rather than ideological grounds. Young people may initially turn to violent extremist groups to find a sense of recognition, fellowship, and identity (McCauley & Segal, 1987; Russell & Miller, 1977; Silke, 2008; LaFree & Ackerman, 2009). Youngsters may also join these groups because they offer forms of support that meet their material and socio-psychological needs, e.g., money, protection, and solidarity. The disproportionate impact of the economic crises faced by many young people in terms of poverty and unemployment may increase the youngsters' vulnerability.

3. Methodology

On the base of these assumptions (developed into a collaborative group effort for an EU project application[15]) we have designed and applied a very quick on-line sociological research concerning the dangers that can be assured to the Internet utilization. Thus, between the 21st – 28th October, 2015 we promoted an on-line Google form short questionnaire that has collected answers from 421 subjects. Even if this volume can be reasonable for a statistical representation of the recorded results, the technique of selection, by snow-ball approach (friends of the friends of the friends etc) produced a slightly limitation for generalization of the data. Anyway, the results can be considered relevant for educated urban Romanian Internet users. The sample was free, formed mostly of women (70%), and has an average age of 24 years (from 14 to 63 years old). A distinct question was dedicated to the self-evaluation of the self-competence into the Internet using, and the median had the value of 8. Although it is a mere subjective self-evaluation, it is quite sure that the users who answered to the questionnaire are not novices in the Internet and social media utilization.

4. Results

The first question of the on-line questionnaire was dedicated to a general evaluation of the Internet evolution in the last 5 years:



Q1. How do you assess the evolution of the Internet in the last 5 years?

[15] Parts of these theoretical description were developed into a H2020 application in 2014 related by Social Media and Terrorism with a significant (but not exclusive) contributions of: Nicolae Goga (University of Groningen, Nl), Nuno Garcia, Pedro Inacio (University of Beira Interior, Pt) Yori Gidron (University of Brussels), Clare Frances Moran, Maria O'Neill(Auberty Unviersity, UK) Rupali Jeswal, Joseph Marchese, Dorin Muresan, Florin Lobont and Bogdan Nadolu (West University of Timisoara).

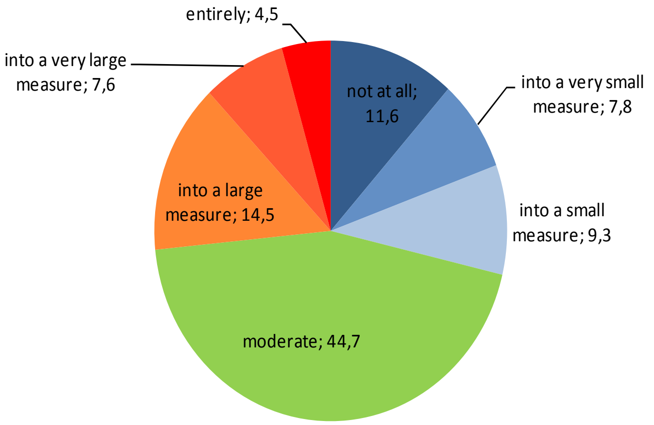
The answers at this question indicated a quasi-total trend of increasing into the evolution of the Internet during the last 5 years (96% for "increased" and "high increased") with a median value of 5 (corresponding to "high increased"). This public perception is strictly related to the current developing of the Internet applications, utilizations and related behaviors. In accordance with the above theoretical framework can be expected that this extensive evolution will include soon or later various antisocial content and negative manifestation. This is not a compulsory trend but only a natural extension, after the digitalization of almost all regular domains (education, mass-media, transportation, health, public administration, government, culture and so on) the areas of human manifestations that are at the law limits or beyond these will become on-line. At this moment the extension of the Internet is a quite solid fact.

Another question has included several statements that the subjects had to evaluate (from total agree to total disagree):

Q2. How did you evaluate the following statements?	Totally agree	Agree	Undecided	Disagree	Totally disagree
On the Internet can be found any information…	**37.5**	**48.7**	5.5	6.9	1.4
The quality of the information from the Internet is doubtful…	4.8	**40.6**	**30.4**	20.7	3.6
Some information shouldn't be found on the Internet…	**24.7**	**33.3**	14.7	17.8	9.5
A lot of information from the Internet are contradictories	**21.9**	**51.5**	16.2	8.1	2.4

Following these results we can conclude that 86.2% of the subjects consider that on the Internet can be found any information, but half of them (45.4%) are not so sure on the quality of this information, and this mostly because *a lot of information from the Internet is contradictory* for 73.4% from subjects. It is very interesting that, despite this high informative profile of the Internet, a quite high level of users (73.4%) appreciate that *some information shouldn't be found on the Internet*. Without getting into details, from distributions can be extracted a soft conclusion, that too much information can be used for negative behaviors and actions. Even if they are posted with a non-violent intention, some contents can be used for various dangerous acts, mainly because of their inconsequence toward reality. Nowadays, there are quite few key words that do not generate into the search engine booth type of answers, pros and cons. From buying electronic gadgets to various politicians, public figures or health care, it is very easy to find contradictory information about them. Thus it remains on the experience of the user and on him/her capacity to discern the true from all these irrelevant contents.

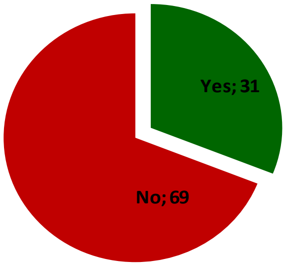
Another question was focused on a more sensible topic related to the censuring of the information on the Internet (%):



Q3. To what extent that information from the Internet should be censored?

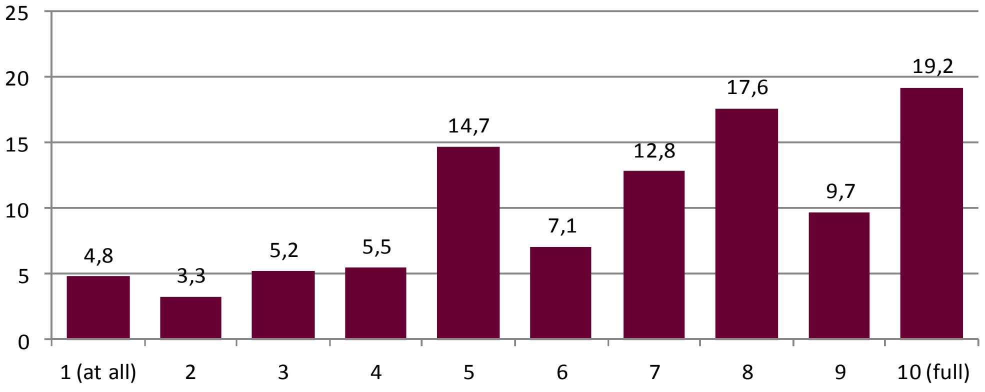
Following this distribution, we can observe that a large part of the subjects (44,7%) consider that the information from the internet should be moderately censored (against various risks and social dangerous). Beside them, 26.6% evaluate that this process should be wider, and 28.7% think it should be lower. These two almost equal groups consolidate the central trend, and reflect a quite important worry concerning this perspective. The Internet has begun as an almost totally free of control medium, a quasi-anarchic structure, a symbol for the freedom of expression for any users. In time, it has become more and more accessible, and a large amount of information has become available inside the Info-sphere. Now, due to some negative consequences, it looks like starting to censure some information is not a prohibitive idea anymore, but rather a desirable one. We want to stress on the fact that the sample was formed by regular users that are not experts in security issues and thus, the recognizing of the importance of having a moderate censuring onto the Internet is a very significant conclusion. With an indirect connection to the previous item, the next question has directly approached a special topic related to the user's knowledge about the dark web and/or deep web. These represent a quite particularly topic among the Internet users, and represent an area where the IP tracking is difficult or not-possible. Into this kind of sites and applications any user can remain anonymous, no matter what he/she does, posts or accesses.

The distribution of answers to this question is the following:



Q4. Have you heard about dark/deep web?

Around two thirds of the respondents have not heard about dark/deep web. This is not necessary unusual, since the dark/web is usually associated with illicit activities, and is not regularly promoted into the virtual space. On one hand, the lack of information concerning this sensible topic can expose innocent users to various risks related to their presence, identity, private life, all exposed on the Internet. On the other hand, the dark/deep web trend is to cumulate all negative persons, contents, actions, and applications against the personal and public security. If a regular user does not know about these potential risks, he/her might become more vulnerable to the direct threats. Thus, directly related to this, the following question has tried to identify the users' perceptions about how dangerous be the Internet be:


Q5. Do you believe that the internet can be used with antisocial purpose?

With a median value of 7 it is obvious that a large part of the sample consider that the Internet can be used in a consistent manner for various antisocial purposes (59.3% evaluated this risk above 7). Even if this is a subjective evaluation, the focusing of answers on the high part of the scale confirms the relevance of this topic. Once again, without a direct experience in the security issues, the users that have answered to the questionnaire recognize that in the digital world can be infiltrated people, contents, information, actions, and applications with less ethical intentions. Finally, the last question was dedicated to an explicit problem: the recruitment of adepts by terrorist groups with the help of the Internet (%):

very small measure	4.8
small measure	12.4
moderate measure	21.4
large measure	**38.5**
very large measure	23

Again a significant volume of users (61.5%) estimate that the terrorist groups can recruit adepts from the Internet without serious difficulties.

5. Conclusion

We have thus a quite coherent picture on the negative part of the internet: dangerous information, deep/dark web, and computer-mediated recruitment for the extremist movements. Even these are just some consequences of the natural evolution of the Internet, and it is quite sure that it cannot remain beyond any action, control, or at least attention. It is a very consistent chapter of the Internet, and surely it is not a positive one. The direct risks that can be associated with this chapter can generate very complex consequences into the effective social space. The recent results from the epigenetic research conclude that the trauma can be inherited, and, thus, the undefined hate can go across generations. It is very important not to delay any adequate and proper measures, because the Internet must keep its promise of the 4 of A: anyone to be able to send Anything, Anytime, Anywhere, and all this without becoming a public threat.

References

Dunbar, R. (2012). Social cognition on the internet: testing constraints on social network size. Philosophical Transactions of the Royal Society, London, 367B: 2192-2201

LaFree, Gary, & Ackerman, Gary, (2009). The Empirical Study of Terrorism: Socil and Legal Research. *Annu. Rev. Law. Soc. Sci.* 5. 347-74.

McCauley, C & Segal, M. (1987). Social Psychology of Terrorist Groups, In Hendrick, C. (ed) *Review of Personality and Social Psychology*, Beverly Hills, CA: Sage.

Russell, CA and Miller, BH.(1977). Profile of a Terrorist. *Military Rev*. 57: 21-24.

Silke, A. (1998). Cheshire-Cat Logic: the recurring theme of terrorist abnormality in psychological research. *Psychol. Crime Law*. 4(1): 51-69.

UK ACPO; Guidelines for the Safe Use of the Internet and Social Media by Police Officers and Police Staff, Association of Chief Police Officers (England and Wales) 2013, available online at http://library.college.police.uk/docs/ACPO/safe-use-of-the-Internet-Feb-2013.pdf.

Zevenbergen, B. (2015). *Ethical privacy guidelines for mobile connectivity measurements*
blog available at http://blogs.oii.ox.ac.uk/policy/ethical-privacy-guidelines-for-mobile-connectivity-measurements/ last accessed on the 15th of August 2015.

Workman, Bommer, & Straub (2008). Security lapses and omissions of information security measures: A threat control model and empirical test. Computers in Human Behaviour, 24(6), pp. 2799-2816. (Available on Science Direct).

*** Social Media in Jihad and Counterterrorism – special number of Combater Terrorism Exchange electronic journal, no 4/2012 available at https://globalecco.org/documents/10180/605826/CTXVol2No4.pdf/8701f69a-ec4a-4f7a-b08d-c8a793e3fc27

*** The use of the Internet for terrorist purposes – United Nations Office on Drugs and Crime – electronic document available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf last accessed December 2014.